NIST Special Publication 800-53

# Recommended Security Controls for Federal Information Systems


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



**Ron Ross**
**Gary Stoneburner**
**Stuart Katzke**
**Arnold Johnson**
**Marianne Swanson**




## INFORMATION SECURITY

**INITIAL PUBLIC DRAFT**


Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930



***October 2003***




**U.S. Department of Commerce**
*Donald L. Evans, Secretary*

**Technology Administration**
*Phillip J. Bond, Under Secretary of Commerce for Technology*

**National Institute of Standards and Technology**
*Arden L. Bement, Jr., Director*

## 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 non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Authority

The National Institute of Standards and Technology (NIST) has developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict 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.

**National Institute of Standards and Technology Special Publication 800-53, 238 pages (October 2003) 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 the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.



THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT BEGINS ON 1 NOVEMBER, 2003 AND ENDS ON 31 JANUARY 2004. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV

OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

## Acknowledgements

The authors, Ron Ross, Gary Stoneburner, Stuart Katzke, Arnold Johnson and Marianne Swanson of the National Institute of Standards and Technology (NIST) wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

## Note to Reviewers

NIST Special Publication 800-53 may be used by organizations in conjunction with an emerging family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Pre-publication final), December 2003;
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second public draft), June 2003;
- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems* (Initial public draft), Spring 2004;
- NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*, August 2003; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels* (Initial public draft), Fall 2003.
- FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*, (Projected for publication, Fall 2005) [1]

The series of seven documents, when completed, is intended to provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in Federal information systems—and thus, make a significant contribution toward satisfying the requirements of the Federal Information Security Management Act (FISMA) of 2002. We regret that all seven publications could not be released simultaneously. However, due to the current international climate and high priority of information security for the Federal government, we have decided to release the individual publications as they are completed. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another.

Reviewers will notice that the security controls for the high baseline (i.e., those controls for the protection of information systems designated as FIPS Publication 199 security category of high) have not been identified in the first public draft of Special Publication 800-53. These security controls will be provided in subsequent drafts of this special publication. The breadth and depth of the security controls required to protect the most critical/sensitive information systems within the Federal government is substantial. The selection of appropriate security controls for the three baselines in moving from low to moderate to high does not increase in a linear manner, but rather exponentially. Thus, for the high baseline, the number of security controls will increase significantly as will the content of the associated controls (i.e., control robustness). Based on the final selection of security controls for the high baseline, an estimated threat coverage will be determined. NIST plans to hold a public workshop on March 8, 2004 in Gaithersburg, MD, to address the issues associated with constructing the security controls for the high baseline as well as the development of appropriate security controls for that baseline. Obtaining feedback from the first public comment period on Special Publication 800-53 (specifically on the technical content and applicability of the security controls in the catalog) is a prerequisite for taking on this next important task in security control development. Consult the NIST project web site at http://csrc.nist.gov/sec-cert for additional details on the upcoming workshop.

[1] FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*, when published in 2005, will replace NIST Special Publication 800-53 and become a mandatory standard for Federal agencies in accordance with the Federal Information Security Management Act (FISMA) of 2002.

It should be noted that this initial draft of Special Publication 800-53 is preliminary in nature. The security controls described in the catalog and associated control baselines have been incorporated from many different sources, and as such, will require several iterations of review, comment, and subsequent modification to achieve consistency in terminology, structure, and content. While it is important to retain the identity of the source security controls (which we have attempted to do with a detailed mapping notation), it is equally important to move toward a standardized language and expression for those controls. The importance of security controls in the protection of Federal information systems demands early exposure to the community who will be employing those controls and thus, motivated the release of this document as the earliest opportunity.

Reviewers are encouraged to provide comments on any aspect of this special publication. Of particular interest are comments on: (i) the content of the security controls listed in the control catalog (including consistency of terminology); (ii) the choice of the minimum security controls assigned to the security control baselines; (iii) the estimated threat coverage for the respective security control baselines; (iv) the overall process of initial security control selection and tailoring based on an organization's assessment of risk; and (v) understandability and usability of the security controls. Finally, it is the authors' intention that the security controls and baselines will be periodically updated to reflect feedback from use and changes in the state-of-the-art and generally accepted security practices.

Your feedback during the public comment period is essential to the document development process and is greatly appreciated.

-- RON ROSS, PROJECT LEADER

# Table of Contents

# List of Tables

# List of Figures

CHAPTER ONE 1

# INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION SYSTEMS

*It is estimated that ninety-nine percent of all reported intrusions result through exploitation of known vulnerabilities or configuration errors, for which safeguards and countermeasures were available…NIST*

The selection of appropriate *security controls* for an information system[2] is an important task that can have major implications on the operations and assets of an organization. Security controls are the management, operational, and technical safeguards and countermeasures prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. There are three important questions that should be answered by organization officials when addressing the security considerations for their information and information system:

- What security controls are needed to adequately protect the information and information system that supports the operations and assets of the organization in order to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired level of assurance, (i.e., grounds for confidence), that the selected security controls, as implemented, are effective in their application?

The answers to these questions cannot be given in isolation. They must be given in the context of an information security program for the organization that identifies, controls, and mitigates risks to its information and information systems.[3] The security controls defined in Special Publication 800-53 and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined information security program. An effective information security program should include—

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system;
- Security plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;[4]

[2] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[3] The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets.

[4] NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, provides guidance and recommendations on the format and content of security plans.

- Security awareness training to inform personnel of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency depending on risk, but no less than annually;[5]
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the organization and its information systems;
- Procedures for detecting, reporting, and responding to security incidents;[6] and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.[7]

It is of paramount importance that responsible individuals within the organization understand the risks and other factors that could adversely affect their operations and assets. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

## 1.1 PURPOSE AND APPLICABILITY

The purpose of this special publication is to provide guidelines for selecting and specifying security controls for information systems. These guidelines have been developed to help achieve more secure information systems by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for baseline (minimum) security controls for information systems categorized in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- Promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and
- Creating a foundation for the development of verification techniques and procedures for determining security control effectiveness.

[5] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second public draft), June 2003, provides guidance for certifying and accrediting information systems.

[6] NIST Special Publication 800-61, *Computer Security Incident Handling Guide* (Initial public draft), September 2003, provides guidance for detecting, reporting, and responding to security incidents associated with information systems.

[7] NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002, provides guidance for contingency planning and continuity of operations.

The guidelines provided in Special Publication 800-53 are applicable to all Federal information systems[8] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[9] The guidelines have been broadly developed from a technical perspective to complement similar guidelines issued by agencies and offices operating or exercising control over national security systems. This publication is intended to provide guidance to Federal agencies until the publication of FIPS Publication 200, *Minimum Security Controls for Federal Information Systems* (Projected for publication, Fall 2005). State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are encouraged to consider the use of these guidelines as appropriate.

## 1.2 RELATIONSHIP TO OTHER SECURITY CONTROLS AND STANDARDS

In an attempt to create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations.[10] The objective of NIST Special Publication 800-53 is to provide a sufficiently rich set of security controls that satisfy the breadth and depth of security requirements[11] for information systems and that are consistent with and complementary to other established security standards.[12]

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of the respective organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security control objectives and control descriptions within the catalog facilitate the development of verification techniques and procedures that can be employed during testing and evaluation to demonstrate control effectiveness in a

[8] A Federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[9] A national security system is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Agencies should consult NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*, for guidance on determining the status of their information systems.

[10] For example, security controls from the audit, defense, healthcare, intelligence, and standards communities have been defined in the following publications: (i) General Accounting Office, *Federal Information System Controls Audit Manual*; (ii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive (DCID) Manual 6/3, *Protecting Sensitive Compartmented Information within Information Systems*; (v) NIST Special Publication 800-26, *Security Self Assessment Guide for Information Technology Systems*; and (vi) International Standard ISO/IEC 17799, *Code of Practice for Information Security Management*.

[11] Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

[12] For example, ISO/IEC 15408, *Common Criteria for Information Technology Security Evaluation*, provides a more detailed framework for defining security requirements for information technology products and systems.

consistent and repeatable manner—thus, contributing to the organization's confidence that there is ongoing compliance with security requirements.

## 1.3 ORGANIZATIONAL RESPONSIBILITIES

It is recommended that organizations use FIPS Publication 199 standards to define security categories for their information systems. The recommendations for baseline (minimum) security controls from Special Publication 800-53 can subsequently be used as a starting point for and input to the organization's risk assessment processes[13] and the development of security plans for those information systems. While the FIPS Publication 199 security categorization associates the operation of the information system with a "worst-case" impact on an organization's operations and assets (providing an upper bound on risk), the incorporation of refined threat and vulnerability information during the risk assessment process facilitates the tailoring of the baseline security controls to address organizational needs and tolerance for risk. Deviations from the recommended baseline security controls should be documented (along with supporting rationale) in the security plan for the information system. The use of security controls from Special Publication 800-53 and the incorporation of baseline (minimum) controls as a starting point in the control selection process, facilitates a more consistent level of security in an organizational information system—and, at the same time offers the needed flexibility to fine tune and adjust the controls based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

It is important to keep a proper perspective when addressing the topic of security controls for information systems. Building secure systems is a multi-faceted undertaking that involves the employment and use of: (i) well defined system-level security requirements and security specifications; (ii) well designed information technology component products; (iii) sound systems/security engineering principles and practices to effectively and securely integrate component products into an information system; (iv) appropriate metrics for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management. From a systems engineering viewpoint, security is another required capability for an organization's information system—a capability that must be funded by the organization throughout the life cycle of the system. Realistically assessing the risks to the organization's operations and assets by placing the information system into operation or continuing its operation is of utmost importance. Addressing the security requirements for the information system must be accomplished with full consideration of the risk tolerance of the organization *and* the cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system. In general, there may not be sufficient resources to satisfy all security, cost, schedule, and performance objectives for the information sys-

[13] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. The assessment of risk is a process that should be incorporated into the system development life cycle and the process should be reasonable for the organization concerned. For example, at the requirements definition stage, the organization may conduct a high-level risk assessment to supporting investment analysis and budget determination. This initial risk assessment is typically very abstract and conceptual. The next iteration of risk assessment may be performed by the organization as part of requirements determination. This risk assessment is based on more tangible information, perhaps an information system architecture or design, but prior to actual implementation. And finally, there may be an assessment of risk by the organization during the process of security control verification (security certification) and system authorization (security accreditation). This risk assessment focuses on the implemented and fielded information system—and the risk to the organization's operations and assets resulting from the operation of that system. At a minimum, documentation should be produced that describes the process employed and describes the results obtained. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides recommendations on conducting risk assessments.

tem. Management should allocate resources appropriately in accordance with agreed upon priorities and document the resource allocation decisions.

## 1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

This special publication contains three main chapters and ten supporting appendices. Chapter 1 introduces the concept of security controls in the context of FISMA and OMB-related requirements and includes the purpose and applicability of the special publication. Chapter 2 describes the fundamental concepts associated with security control selection and specification to include: (i) the properties of security controls; (ii) the organization and structure of security controls; (iii) baseline or minimum security controls for information systems; and (iv) revising and extending security controls in the control catalog to meet changing security requirements and technologies. Chapter 3 provides an overview of the security control selection and specification process and includes recommendations for: (i) selecting an initial set of baseline security controls for an information system; (ii) tailoring the initial set of security controls based on an assessment of risk and organizational inputs; and (iii) documenting the final agreed upon set of security controls in the security plan for the information system. The supporting appendices provide more detailed information to include: (i) references; (ii) definitions and terms; (iii) acronyms; (iv) a description of information security program activities; (v) threat descriptions; (vi) recommended sets of baseline security controls in accordance with FIPS Publication 199 impact levels; (vii) a comparative summary of security controls within baselines; and (viii) a catalog of security controls.

CHAPTER TWO

# 2

# THE FUNDAMENTALS

SECURITY CONTROL PROPERTIES, STRUCTURE, BASELINES, AND EXTENSIBILITY

*Assurance is the basis for confidence that the security controls in an organization's information system work as intended to protect the system and the information it processes, stores, and transmits…NIST*

This chapter describes the fundamental concepts associated with security control selection including: (i) the properties of security controls; (ii) the organization and structure of security controls; (iii) baseline security controls and estimated threat coverage; and (iv) revising and extending security controls to meet changing security requirements and technologies. These fundamental concepts will be applied during the actual security control selection and specification process described in the next chapter.

## 2.1 PROPERTIES OF SECURITY CONTROLS

Security controls possess two important properties—*robustness* and *flexibility*. The robustness property allows security controls to be defined with varying strengths of function and with varying degrees of assurance regarding the effectiveness of implementation. The flexibility property allows organizations to tailor security controls to satisfy organizational security policies and to meet specific operational needs. The properties of robustness and flexibility ensure that organizations can select the most appropriate security controls to protect their information systems and do so in a manner that is consistent with the organization's mission and resource constraints.

### *Security Control Robustness*

Security controls applied to an information system can be based on mechanisms (e.g., identification and authentication mechanisms, physical access control devices to facilities, cryptographic mechanisms) or documentation (e.g., policies, plans, procedures, memorandums of understanding or agreement). Whether mechanism-based or documentation-based, every security control has a particular robustness level associated with it when implemented. Security control robustness is determined by two key factors: (i) the strength of function associated with the control; and (ii) the assurance, or grounds for confidence, in the effectiveness of the control. The strength of function associated with a particular security control is a relative measure of the effort (or cost) required to defeat a correctly implemented control and is not necessarily related to the cost of implementing such a control.[14] Assurance in the effectiveness of a security control is a function of the control's strength of function as well as the design of the control, the methodology used to construct the control (including the maturity of the processes employed during development), and the context in which the control is used. Assurance is based on these factors and the sophistication and degree of rigor applied during the security control verification process (pre-deployment and post-deployment).[15] Three levels of security control robustness are defined in this special publication: (i) basic; (ii) enhanced; and (iii) strong.

[14] The term work factor is also used by some organizations to define the level of effort required to defeat security controls in information systems.

[15] Verification is the process used to confirm or establish by testing, evaluation, examination, investigation, or competent evidence, the effectiveness of the security controls in an information system. Ongoing security control verification (continuous monitoring) supports the information system authorization process. Testing and evaluation procedures used to verify the effectiveness of security controls can be found in NIST Special Publication 800-53A, *Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems* (Initial public draft), Spring 2004.

***Security Control Flexibility***

In addition to robustness levels, some security controls have sections that are variable in nature, providing a means for organizations to instantiate certain values within the control. The variable section of a security control is clearly identified by the keywords *assignment* or *selection* indicating the type of operation permitted. The assignment operation permits the specification of a parameter to be filled in when the security control is used. For example, the requirements for conducting information backup operations within an organization may vary widely. The assignment operation for information backups permits organizations to specify how often backups are to be conducted but provides a minimum period which is at least monthly. Where assignment operations are allowed, there is typically a lower bound (minimum value) or upper bound (maximum value) established for the variable portion of the security control. The selection operation permits the specification of items that are to be selected from a list given in the security control. For example, organizations may be asked to specify the type of alternate communications services that will be available on a contingency basis by selecting from a list of available options (i.e., long haul, short haul). An example that illustrates both the assignment operation and selection operation in the same security control is provided below:

"…When the maximum number of unsuccessful attempts is exceeded the information system automatically [Selection: locks the account/node until released by an administrator, locks the account/node for an [Assignment: time period (e.g., fifteen minutes)], delays next login prompt according to [Assignment: delay algorithm (e.g., the standard Unix algorithm that accomplishes successively longer delays with each subsequent failure)]…"

## 2.2 STRUCTURE AND ORGANIZATION

There are many different types of security controls that can be employed within an information system to help protect the assets and operations of an organization. The security controls in Appendix J (Catalog of Security Controls) of Special Publication 800-53 have a well-defined structure that consists of three key components: (i) a *control objective* section; (ii) a *control mapping* section; and (iii) a *control description* section. As the name implies, the control objective section provides the overall objective for the particular security control when applied to an information system. The control mapping section lists source documents considered during the development of the control catalog that have similar security controls.[16] The control description section provides the specific control requirements and details of each control. A single control objective may have up to three security control versions associated with it reflecting the basic, enhanced, and strong levels of robustness (if so defined).

The security controls are also organized into *classes* and *families* within a control catalog for ease of use. There are three general classes of security controls (i.e., management, operational, and technical), which correspond to the major sections of a security plan. Management controls typically involve those safeguards and countermeasures employed by an organization to manage the security of the information system and the associated risk to the organization's assets and operations. There are five families within the management class of security controls that address: (i) risk assessment; (ii) security planning; (iii) acquisition of information systems and services; (iv) review of security controls; and (v) authorization for processing (also termed security accreditation by some organizations).

[16] The list of source documents and associated item identifiers believed to contain similar security controls included in SP 800-53 is provided for those organizations interested in seeing a mapping to those source documents. For example, organizations completing an ISO 17799 assessment can find the related security controls in Special Publication 800-53 by examining the control mapping section of each control. Mapping of security controls among various source documents facilitates reuse of assessment evidence and prevents unnecessary duplication of effort during the control verification process.

Operational controls are those safeguards and countermeasures employed by an organization to support the management and technical security controls in the information system. In contrast to technical controls that are primarily executed by the information system, operational controls are typically executed by people that support the system. There are nine families within the operational class of security controls that address: (i) personnel security; (ii) physical and environmental protection; (iii) contingency planning and operations; (iv) configuration management, (v) hardware and software maintenance; (vi) system and information integrity; (vii) media protection; (viii) incident response; and (ix) security awareness and training.

Technical controls are those safeguards and countermeasures (typically described as security mechanisms) employed within the information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. There are four families within the technical class of security controls that address: (i) identification and authentication; (ii) logical access control; (iii) accountability (including audit); and (iv) system and communications protection. Occasionally, the control catalog is modified to place security controls together according to purpose rather than type, enhancing the usefulness of the control catalog and resulting in a few management and technical controls appearing in other sections.

Within the catalog of security controls described above, a standardized naming convention is adopted to uniquely identify each control—that is, a two-character identifier indicating the respective family where the control resides and a numeric identifier indicating the number of the control within the family. Table 1 summarizes the classes and families in the security control catalog and the two-character family identifiers.

| CLASS | FAMILY NAME | IDENTIFIER |
|---|---|---|
| Management | Risk Assessment | RA |
| Management | Security Planning | PL |
| Management | System and Services Acquisition | SA |
| Management | Security Control Review | CR |
| Management | Processing Authorization | PA |
| Operational | Personnel Security | PS |
| Operational | Physical and Environmental Protection | PE |
| Operational | Contingency Planning and Operations | CP |
| Operational | Configuration Management | CM |
| Operational | Hardware and Software Maintenance | MA |
| Operational | System and Information Integrity | SI |
| Operational | Media Protection | MP |
| Operational | Incident Response | IR |
| Operational | Security Awareness and Training | AT |
| Technical | Identification and Authentication | IA |
| Technical | Logical Access Control | AC |
| Technical | Accountability (Including Audit Trails) | AU |
| Technical | System and Communications Protection | SP |

**TABLE 1: CLASSES AND FAMILIES OF SECURITY CONTROLS**

In addition to the family and numeric identifiers, there is also an identifier addressing the robustness level of the security control. Robustness levels indicate a basic (b), enhanced (e), or strong (s) version of the security control with regard to strength of function and assurance of effectiveness. To illustrate a few examples of the security control naming convention, CP-4.b would uniquely identify the fourth security control in the Contingency Planning and Operations family with a basic level of robustness; PS-6.e would uniquely identify the sixth security control in the Personnel Security family with an enhanced level of robustness; and finally, IA-8.s would uniquely identify the eighth security control in the Identification and Authentication family with a strong level of robustness.

## 2.3 BASELINE SECURITY CONTROLS

Organizations, including *communities of interest*,[17] may find it useful to employ security controls applicable to their respective areas of responsibility. These security controls could be used to support meeting security requirements as typically defined by laws, Executive Orders, directives, policies, or regulations (e.g., the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Financial Services Modernization Act, or Department of Defense Instruction 8500.2, Information Assurance Implementation). The challenge for organizations is to determine the appropriate set of security controls, which if implemented and verified effective in their application, would comply with the stated security requirements. Selecting the right security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task—a task that demonstrates the organization's due diligence with regard to security and the protection of the confidentiality, integrity, and availability of their information and information systems.

To assist organizations in making the appropriate selection of security controls for their information systems, the concept of *baseline* controls is introduced in Special Publication 800-53. Baseline security controls are the minimum controls recommended for an information system based on the system's security categorization established in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Prepublication final, December 2003).[18] FIPS Publication 199 security categories are typically considered during the risk assessment process to help guide the initial selection of security controls for an information system. The risk assessment process provides useful information and a procedural approach to examining the important factors that ultimately determine which security controls are necessary to protect the organization's operations and assets. The baseline security controls from Special Publication 800-53 associated with the security categories of FIPS Publication 199 serve as a starting point for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. The baseline security controls can be tailored or adjusted based on the results of the risk assessments conducted by the organiza-

[17] For purposes of this special publication, a *community of interest* is defined as any group or organization within the public or private sectors that must comply with specific security requirements. A community of interest is typically concerned with a particular area of interest (e.g., healthcare, banking and finance, defense, environment, law enforcement, education).

[18] FIPS Publication 199 security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. FIPS Publication 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions takes place within the context of each organization and the overall national interest.

tion. Modifications to the baseline controls should be documented (with supporting rationale for the changes) in the security plan for the information system.

A catalog of security controls for information systems is provided in Appendix J. This catalog represents the entire set of security controls (defined at this time) covering the three principal classes of controls (i.e., management, operational, and technical). From the control catalog, three sets of baseline (minimum) security controls have been identified corresponding to the low, moderate, and high impact levels defined in the security categorization process in FIPS Publication 199. Appendices F, G, and H, respectively, provide a listing of the baseline security controls associated with each of the FIPS Publication 199 impact levels. Each of the three baselines provides a minimum set of security controls (or floor) for a particular impact level associated with a security category. (See Chapter 3 for additional information on how to use security categories to select the appropriate set of baseline security controls.)

The security controls in any of the three baselines contain a mix of controls from the three levels of robustness in the control catalog. For example, the low baseline contains security controls at the basic level of robustness. For the moderate baseline, there is a mix of security controls at the basic and enhanced levels of robustness. And finally, for the high baseline, there is a mix of security controls at the basic, enhanced, and strong levels of robustness. ***There is no direct relationship between the three levels of security control robustness and the three security control baselines.*** The appropriate security controls are selected for the appropriate baselines. For example, a security control at the basic level of robustness control may first appear in the high baseline or the control may never appear in any baseline and be available only as an option for organizations to supplement their control set.

The security control baselines are intended to provide coverage for certain potential threats described in Appendix E. The security controls selected for each baseline are at the recommended level of robustness to achieve the estimated threat coverage. In cases where the baselines do not provide sufficient coverage against certain types of threats, additional security controls may be needed if the organization determines that the likelihood of particular threats exploiting known vulnerabilities in their information system is sufficiently high. A summary and comparison table of the security control baselines is provided in Appendix I. This comparison table can assist organizations in understanding the relative increases in security control robustness required in moving from baseline to baseline.

Organizations may wish to document the association of specific security requirements to particular security controls defined in Special Publication 800-53. This can be accomplished by using what is commonly referred to as a Requirements Traceability Matrix (RTM). The organization starts with the specific security requirements for which there must be compliance. Each security requirement is mapped to an appropriate security control within the selected baseline of controls. The mapping of requirements to controls can be: (i) one-to-one (i.e., a single security requirement is satisfied by a single security control); (ii) one-to-many (i.e., a single security requirement is satisfied by more than one security control); (iii) many-to-one (i.e., a group of security requirements is satisfied by a single security control); or (iv) many-to-many (i.e., a group of security requirements is satisfied by a group of security controls). Table 2 illustrates a simple example of a partial RTM and associated mappings of a set of hypothetical security requirements to set of security controls from Special Publication 800-53.

| SECURITY REQUIREMENTS | MAPPING | NEEDED SECURITY CONTROLS |
|---|---|---|
| Security Requirement No. 1 | 1 TO 1 | PS-1.b |
| Security Requirement No. 2 | 1 TO MANY | PE-2.b, PE-3.b, PE-6.e, PE-7.b |
| Security Requirement No. 3<br>Security Requirement No. 4 | MANY TO 1 | CM-2.e |
| Security Requirement No. 5<br>Security Requirement No. 6 | MANY TO MANY | IA-1.e, IA-2.e, IA-4.b |

**TABLE 2: SAMPLE REQUIREMENTS TRACEABILITY MATRIX**

## 2.4 REVISING AND EXTENDING THE SET OF SECURITY CONTROLS

The set of security controls listed in the control catalog represents the current state-of-the-practice safeguards and countermeasures for information systems. The security controls will be revised and extended to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; and (iii) new security technologies that may be available. The controls populating the various families are expected to change over time, as controls are eliminated or revised and new controls are added. The proposed additions, deletions, or modifications to the catalog of security controls will go through a rigorous, public vetting and review process to obtain government and private sector feedback and to build consensus for the changes. The current set of baseline (minimum) security controls defined in Appendices F, G, and H will change over time as well—as the level of security and due diligence for mitigating risks within organizations increases. A dynamic, flexible, and technically rigorous set of security controls will be maintained in the control catalog to allow organizations and communities of interest to continue to be able to select the appropriate controls for their respective needs in a cost effective manner.

CHAPTER THREE

# 3

# THE SECURITY CONTROL SELECTION PROCESS

SELECTING BASELINE SECURITY CONTROLS AND TAILORING THE CONTROL SET

*Confidence in information systems security can be gained through the careful selection and implementation of appropriately defined security controls…NIST*

The process of selecting the appropriate security controls for an information system should, ideally, be accomplished during the early stages of the system development phase of the life cycle (i.e., prior to solicitation) and be a part of and guided by the organization's assessment of risk. The previous chapter described the fundamental concepts associated with the security control selection process. This chapter demonstrates how the fundamental concepts are applied by organizations to: (i) select an initial set of baseline security controls in accordance with the FIPS Publication 199; (ii) tailor the baseline security controls as needed; and (iii) document the final set of security controls in the security plan for the information system. The process described above provides *controlled flexibility* for organizations in the security controls selection process—that is: (i) establishing common baselines of security controls in accordance with FIPS Publication 199; and (ii) incorporating specific information from the organization to adjust and tailor the control set giving needed flexibility to provide adequate security within the system life cycle constraints of cost, schedule, and performance.

## 3.1 SELECTING BASELINE SECURITY CONTROLS

The first step in selecting an appropriate set of baseline security controls for an information system is to establish the FIPS Publication 199 security category of the system. The security category of the information system is represented as a triple of the associated potential impacts for confidentiality, integrity, and availability. The generalized format for expressing the security category, SC, of an information system is:

**SC** = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.[19]

After the organization has established the security category of its information system, the maximum value (or high water mark) of the potential impacts is noted. It is a straightforward task to select an initial baseline set of security controls for the information system from the appropriate Appendix in Special Publication 800-53 based on the highest value of the potential impacts defined in the FIPS Publication 199 security category. That is: (i) if the highest potential impact is LOW, select the LOW baseline of security controls; (ii) if the highest potential impact is MODERATE, select the MODERATE baseline of security controls; and (iii) if the highest potential impact is HIGH, select the HIGH baseline of security controls. For example, the security category, SC, for an information system supporting an organization's acquisition process is expressed as:

$\mathbf{SC}_{\text{acquisition system}}$ = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}.

The maximum value (or high water mark) of the potential impacts for the acquisition system is MODERATE and, therefore, the MODERATE baseline of security controls is selected.

[19] The definitions of low, moderate, and high potential impact can found in FIPS Publication 199.

The minimum security controls listed in the low, moderate, and high baselines are a recommended starting point for organizations in selecting the actual security controls that may be necessary to protect their information systems. The initial set of baseline security controls provides a foundation of controls that may be augmented with additional controls, if necessary. Each baseline, in addition to being associated with the high water mark of potential impacts in the initial FIPS Publication 199 security categorization of the information system, provides a threat coverage estimate described in the tables in Appendix E.

## 3.2 TAILORING THE BASELINE SET OF SECURITY CONTROLS

After selecting the initial set of baseline security controls, the organization can now tailor the controls to meet organization and information system-specific needs. There are two steps that should be followed in tailoring the baseline security controls to meet organization and system-specific needs: (i) adjusting the baseline security controls based on the results of organizational risk assessments (either formal or informal); and (ii) assigning organization-defined values to security controls where indicated by assignment and selection operations. These steps are described in greater detail below.

### *Adjusting the Baseline Security Controls Based on an Assessment of Risk*

The organization's assessment of risk plays an important part in the security control selection process. Since the recommended baseline security controls from Special Publication 800-53 represent a starting point in the selection process, an adjustment of the control set may be required based on the specific information derived from the organization's risk assessments. It is during the risk assessment process that the planned or actual security controls (depending on whether the information system is in development or operational) are examined in light of the expected threats to and vulnerabilities in the system and the anticipated impact should there be a threat of exploitation of the identified vulnerabilities. The initial baseline of security controls selected by the organization is an initial response to the FIPS Publication 199 security categorization of the organization's information system. The estimated threat coverage provided by the baseline security controls should be used in conjunction with the risk assessments to answer two important questions.

- For those threats that are not covered in the threat tables in Appendix E, should additional security controls be added to reduce or eliminate vulnerabilities?
- Has the organization determined that the likelihood of threat exploitation of known vulnerabilities is sufficiently low to justify the decision to eliminate certain security controls or to refrain from adding controls?

Ultimately, management may make a risk-based decision to substitute equivalent controls or enhance the recommended security controls for an information system. For example, when deemed appropriate (typically for operational or technical reasons), management may approve the substitution of security controls in the baseline with other equivalent controls. Alternatively, there may be times when management determines that more stringent security controls are needed than are contained in the sets of baseline controls described in Special Publication 800-53.

### *Assigning Organization-defined Values to Security Controls*

There are certain security controls within the catalog of controls that can be tailored to specific organization needs by specifying organization-defined values for the explicitly identified parameters. The variable sections of these types of security controls (typically identified by italicized text and the keywords *assignment* and *selection*) are filled in to reflect the organization and system-specific security requirements and the results of the risk assessments. This is the final step in the

security control tailoring process. The following examples illustrate the assignment and selection operations on two security controls from the control catalog:

EXAMPLE 1: Enforcement of Physical Access to Information System Facilities

**PE-3 PHYSICAL ACCESS ENFORCEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply physical access controls at designated physical entry points within sensitive facilities and restricted/controlled areas containing information systems.

**PE-3.e** ENHANCED CONTROL: Physical security perimeters are defined by the organization. Sensitive facilities and restricted/controlled areas are prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that control access. The main entrance to sensitive facilities and restricted areas is controlled/manned. Secondary entrances have cameras and/or electronic entry detection devices (e.g., card keys), to monitor access. Apparent security violations or suspicious physical access activities are investigated and remedial actions taken. Every physical access point to sensitive facilities or restricted areas housing information systems that process or display information is controlled during working hours and guarded or locked during non-work hours. Identification badges are worn. Access authorization is verified before granting physical access. Unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations, etc.). The organization controls access to non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) as appropriate in accordance with the organization's assessment of risk. **The [*Assignment: list of physical access points*] physical access points are controlled twenty-four hours per day, seven days per week through the use of entry devices such as key cards or biometrics. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

A hypothetical example of the completed assignment is: " …The front door facing Elm Avenue, two side doors facing 25th Street, and back door facing the employee parking lot are controlled twenty-four hours per day, seven days per week through the use of physical access devices such as key cards or biometrics…"

EXAMPLE 2: Mechanisms Employed to Back Up Information Systems

**CP-7 BACKUP MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable backing up information and the information system state.

**CP-7.b** BASIC CONTROL: Mechanisms provide for sufficient backup storage capability. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time. A capability to conduct the following types of backup exists: (i) full (complete backup); and (ii) [*Selection of one or more: incremental (changes since last incremental) | differential (changes since last full)*].

A hypothetical example of the completed selection is: "…A capability to conduct the following types of backup exists: (i) full (complete backup); and (ii) incremental (changes since last incremental)…"

## 3.3 DOCUMENTING SECURITY CONTROLS IN THE SECURITY PLAN

The security plan for an information system documents the results of the security control selection and specification process. The plan goes through various stages of development—but in the end, contains all of the security controls either planned or in place for the information system. It is important that the final security controls selected for or identified in the information system are documented in the security plan as the plan provides the foundation for conducting the subsequent security control verification (security certification) and security authorization (security accreditation). The security plan should contain all of the justification and rationale for the final security controls selected. The security plan and the results of the security control verification and security authorization play a key role in deciding if the planned or actual connection of the information system to systems outside the authorization boundary can be accomplished in a manner that maintains the degree of security that is acceptable to the organization. The security plan should include rationale (with pointers to supporting documentation) explaining why the security controls meet the organization's security requirements.

## APPENDIX A

# REFERENCES

LAWS, POLICIES, REGULATIONS, STANDARDS, AND SPECIAL PUBLICATIONS


1. Department of Defense Instruction 8500.2, Information Assurance Implementation, February 2002.
2. Director of Central Intelligence Directive (DCID) Manual 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.
3. E-Government Act of 2002 (Public Law 107-347), December 2002.
4. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Pre-publication final), December 2003.
5. Federal Information Security Management Act of 2002, Title III, (Public Law 107-347), December 2002.
6. International Standard, ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation, October 1999.
7. International Standard, ISO/IEC 17799, *Code of Practice for Information Security Management*, December 2000.
8. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.
9. NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
10. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
11. NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second public draft), June 2003.
12. NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (Initial public draft), Projected for publication, Spring 2004.
13. NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.
14. NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels* (Initial public draft), Projected for publication, Fall 2003.
15. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, February 1996.
16. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Security Requirements*, Attachment A, Rev. 3.1, March 2003.
17. United States General Accounting Office *Federal Information System Controls Audit Manual*, January 1999.

## APPENDIX B

# GLOSSARY

COMMON TERMS ASSOCIATED WITH SECURITY CONTROL SELECTION AND SPECIFICATION

The terms and definitions in this special publication and have been obtained from Congressional legislation, Executive Orders, OMB policies, and commonly accepted glossaries of security terminology. Where terms and definitions in this glossary conflict within the terms and definitions used in other publications, readers should defer to the usage in this publication.

| | |
|---|---|
| Adequate Security | Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that information systems and applications used by the organization operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, operational, and technical controls. |
| Agency | See Executive Agency. |
| Availability<br>[44 U.S.C., SEC. 3542] | Ensuring timely and reliable access to and use of information. |
| Baseline Security Controls | The minimum security controls recommended for an information system based on the system's security categorization established in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Prepublication final), December 2003. |
| Confidentiality<br>[44 U.S.C., SEC. 3542] | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. |
| Countermeasures | Synonymous with security controls and safeguards. |
| Executive Agency<br>[41 U.S.C., SEC. 403] | An executive department specified in 5 U.S.C., Section 101; a military department specified in 5 U.S.C., Section 102; an independent establishment as defined in 5 U.S.C., Section 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. |
| Executive Departments<br>[5 U.S.C., SEC.101] | Department of State, Department of the Treasury, Department of Defense, Department of Justice, Department of the Interior, Department of Agriculture, Department of Commerce, Department of Labor, Department of Health and Human Services, Department of Housing and Urban Development, Department of Transportation, Department of Energy, Department of Education, Department of Veterans Affairs, Department of Homeland Security. |

| | |
|---|---|
| Federal Information System [40 U.S.C., SEC. 11331] | An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. |
| Information Resources [44 U.S.C., SEC. 3502] | Information and related resources, such as personnel, equipment, funds, and information technology. |
| Information Security [44 U.S.C., SEC. 3542] | The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. |
| Information System [44 U.S.C., SEC. 3502] | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. |
| Information Technology [40 U.S.C., SEC. 1401] | Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is used by an 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 which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. |
| Integrity [44 U.S.C., Sec. 3542] | Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. |
| Management Controls | The security controls (i.e., safeguards and countermeasures) applied to an information system that focus on the management of risk and the management of the information security system. Actions that are performed primarily to support management decisions with regard to information system security. |
| Military Departments [5 U.S.C., SEC. 102] | Department of the Army, Department of the Navy, and Department of the Air Force. |
| National Security Information | Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status. |

| | |
|---|---|
| National Security System [44 U.S.C., SEC. 3542] | Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. |
| Operational Controls | The security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by people (as opposed to the information system). |
| Safeguards | Synonymous with security controls and countermeasures. |
| Security | See Information Security. |
| Security Controls | The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, adequately protect the confidentiality, integrity, and availability of the system and its information. |
| Security Plan | Formal document that provides an overview of the security requirements of the information system and describes the security controls in place or planned for meeting those requirements. |
| Security Control Robustness | The strength of function of a security control and the assurance that the control is effective in its operation. |
| Security Requirements | Requirements levied on an information system derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. |
| Sensitive Facility | An area, room, or group of rooms within an organization, containing hardware, software, or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment) that must be relied upon for the correct enforcement of the security policy of the information system. |

| | |
|---|---|
| Technical Controls | The security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. |
| Threat | Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability. |
| Verification | The process used by an independent agent to confirm or establish by testing, evaluation, examination, investigation, or competent evidence, the effectiveness of the security controls in an information system. |
| Vulnerability | A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an organization's operations or assets through a loss of confidentiality, integrity, or availability. |

## APPENDIX C

# ACRONYMS

SHORTHAND NOTATIONS FOR COMMONLY USED TERMS

| | |
|---|---|
| CMS | Centers for Medicare and Medicaid Services |
| COTS | Commercial Off The Shelf |
| DCID | Director of Central Intelligence Directive |
| FIPS | Federal Information Processing Standards |
| FISCAM | Federal Information System Controls Audit Manual |
| FISMA | Federal Information Security Management Act |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISO | International Standards Organization |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| U.S.C. | United States Code |

## APPENDIX D

# INFORMATION SECURITY PROGRAM ACTIVITIES

INTEGRATING THE SECURITY CONTROL SELECTION AND SPECIFICATION PROCESS

The following sections describe some of the key activities in an organizational information security program. These activities, including security control selection and specification, are typically conducted within the system development life cycle. The activities do not necessarily need to be conducted in a sequential manner—they can, in fact, be conducted multiple times during various phases of the life cycle.

### *Security Categorization*

Security categorization standards establish three impact levels (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing information systems. The security standards are based on the potential impact that the loss of confidentiality, integrity, or availability would have on an organization's operations or assets. The standards provide organizations with a means of selecting baseline (minimum) security controls for their information systems as a starting point in the control selection process. The control selection process is refined through the employment of one or more risk assessments. Organizations should consult FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Pre-publication final), December 2003, for guidance on categorizing information systems.

### *Risk Assessments*

Periodic assessments of risk to an organization's operations or assets resulting from the operation of an information system are an important activity required by FISMA. These risk assessments bring together important information for organization officials with regard to the protection of the information system and generate essential information required for the security plan. Risk assessments typically include: (i) the identification of threats to and vulnerabilities in the information system; (ii) the potential impact that a loss of confidentiality, integrity, or availability would have on an organization's operations or assets should there be a breach in security; and (iii) the identification and analysis of security controls for the information system. Organizations should consult NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, or other similar publications for guidance on conducting risk assessments.

### *Security Planning*

In accordance with the provisions of FISMA, information security programs are required to have plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate. The preparation of a security plan for an information system ensures that agreed upon security controls planned or in place are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the organization's information security program (e.g., risk assessments, security test and evaluation results, plan of action and milestones,[20] configuration management plan, contingency plan, incident response plan, secu-

[20] The results of security testing and evaluation may uncover deficiencies in the security controls employed to protect an information system. A detailed plan of action and milestones is required to document the planned corrective measures needed to increase the effectiveness of the security controls and provide the requisite security for the information system prior to security authorization. The authorizing official normally reviews and must approve the plan of action and milestones prior to authorizing operation of the information system.

rity awareness and training plan, rules of behavior, system interconnection agreements, and security authorizations/accreditations). Organizations should consult NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, or other similar publications for guidance on creating security plans.

### *Security Control Development*

For new information systems, the security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development or integration of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective. This activity typically takes place during the acquisition/development phase of the system development life cycle.

### *Developmental Security Test and Evaluation*

The security controls developed for a new information system must be tested and evaluated prior to deployment to ensure that the controls are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed—these controls are typically management and operation level controls. For those security controls that can be assessed prior to deployment, a security test and evaluation plan is developed. This plan guides the developmental security testing and evaluation of the security controls and provides important feedback to information system developers and integrators. This activity typically takes place during the acquisition/development phase of the system development life cycle.

### *Security Control Integration*

The integration of security controls occurs at the operational site where the information system is to be deployed for operation. Integration and acceptance testing occurs after delivery and installation of the information system. Security control settings and switches are enabled in accordance with manufacturer instructions and available security implementation guidance. This activity typically takes place during the implementation phase of the system development life cycle.

### *Security Control Verification*

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required to ensure that the controls are effectively implemented. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures (also known as security certification) is a critical activity conducted by the organization or by an independent third party on behalf of the organization to give organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. In addition to security control effectiveness, security control verification also uncovers and describes the actual vulnerabilities in the information system. The determination of security control effectiveness and information system vulnerabilities provides essential information to authorizing officials to facilitate credible, risk-based, security authorization (accreditation) decisions. Organizations should consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (Initial public draft), Spring 2004, or other similar publications for guidance on the evaluation of security controls.

### *Security Authorization*

In accordance with the provisions of OMB Circular A-130, the security authorization of an information system to process, store, or transmit information is required.[21] This authorization (also known as security accreditation), granted by a senior organization official, is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified risk to an organization's operations or assets. The security authorization decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An authorizing official relies primarily on: (i) the completed security plan; (ii) the security test and evaluation results; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities, in making the decision on whether to authorize operation of the information system and to explicitly accept the risk to an organization's operations or assets.

### *Configuration Management and Control*

Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security authorization. Ensuring adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment requires an effective configuration management and control policy and associated procedures. Configuration management procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

### *Ongoing Monitoring*

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required on an ongoing basis to ensure that the controls continue to be effective in their application. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate organization officials is an essential activity of a comprehensive information security program. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits. Organizations should consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems* (Initial public draft), Spring 2004, or other similar publications for guidance on the ongoing monitoring of security controls.

[21] Security authorization is typically only one factor that ultimately goes into the organizational decision to place an information system into operation. All required functionality within the information system, (both security related and non-security related) must be installed and working properly before the final approval to operate is given by the organization's authorizing official.

Figure 1 illustrates key information security program activities and the impact of those activities on the organization's information systems.

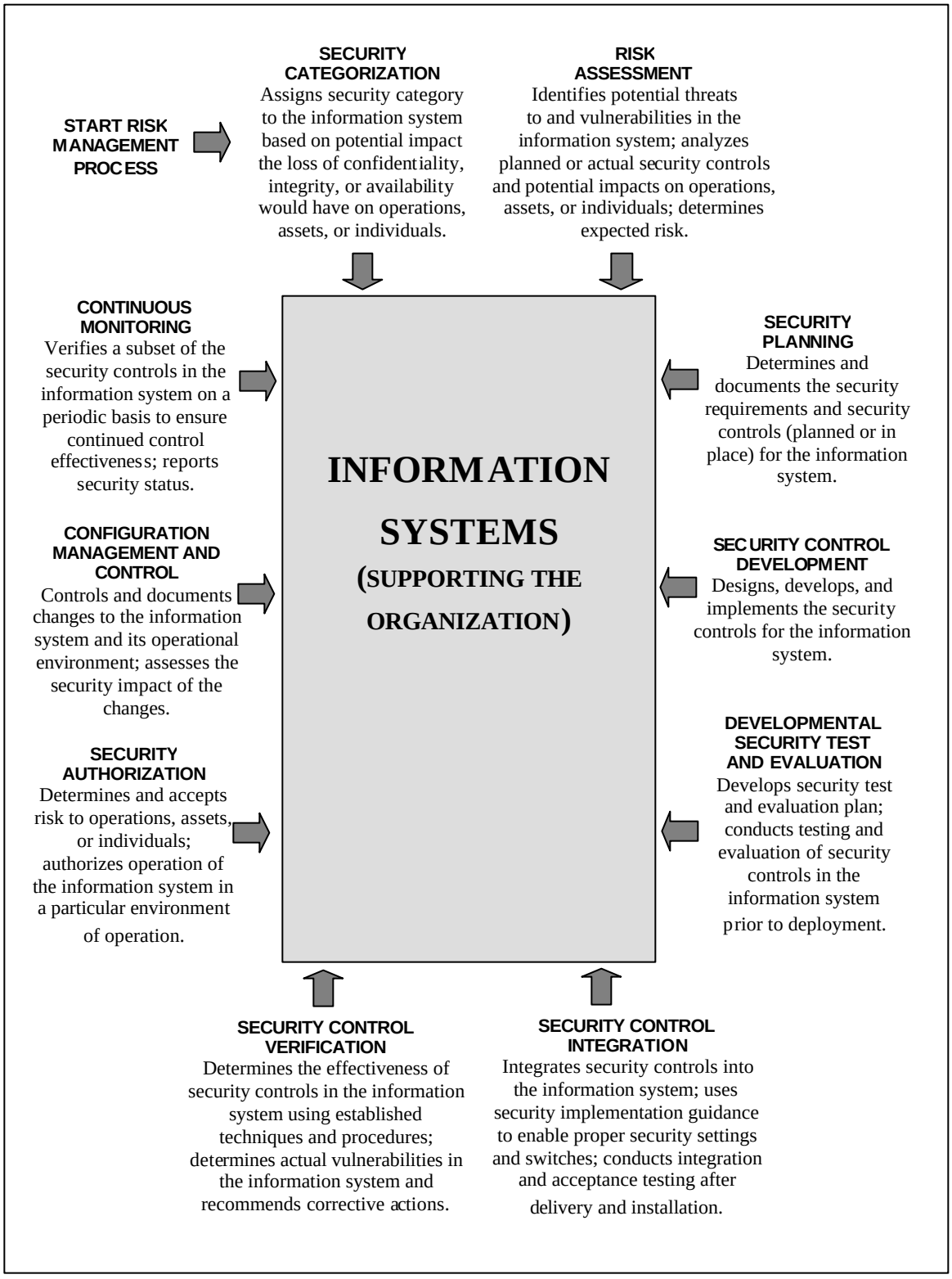


**FIGURE 1: INFORMATION SECURITY PROGRAM ACTIVITIES**

## APPENDIX E

# DESCRIPTION OF THREAT SOURCES

CHARACTERIZING THE THREAT BY TYPE, CAPABILITIES, RESOURCES, AND INTENTIONS

To understand the breadth and depth of threat coverage obtained by the application of security controls to an information system, it is important to show which potential threats are intended to be countered by the selected controls and which potential threats are not intended to be countered. In that regard, it is helpful to be able to characterize the potential threats to information systems by describing the key characteristics of those threats. Threat sources can be categorized as errors, events of nature, or intentional attacks. Errors, caused by humans or machines, can impact an information system in a variety of ways from a minor degradation in performance to a complete loss of system capability. Events of nature (e.g., fires, floods, hurricanes, and earthquakes) can also result in damage or disruption to an information system depending on the severity of the event and the extent of the geographic area affected. And finally, intentional attacks on an information system, usually (but not always) conducted with malicious intent and with varying degrees of intensity, can be the source of potential damage to the system and to the operations or assets of the organization.

Intentional attacks are usually characterized by: (i) the type of attack; (ii) the capability of the attacker; (iii) the intent of the attacker; and (iv) the resources available to the attacker. The type of attack is either local or remote. In some cases, intentional attacks on information systems require the physical presence of the attacker at the site where the system resides. In other cases, the attacker can launch the attack remotely via the network. The capability of the attacker is typically described by the sophistication of the attack and the availability of access to the information system. The sophistication of the attack is based on two factors: (i) the knowledge and skills of the attacker; and (ii) the availability and use of sophisticated attack tools.[22] In examining the accessibility of the information system to the attacker, consideration is given as to whether the attacker is a member of the organization or is an outsider. If the attacker is an insider, further consideration is given as to whether the attacker is a non-privileged user, a privileged user, or a non-user of the information system being attacked. Further consideration is also given for outsiders with the possibilities being non-user and public-user. The attacker's status determines typical access rights to the information system under routine conditions.

The intentions of the attacker can be widely varied on a continuum ranging from non-malicious and harmless to malicious with intent to do grave damage to the organization. On the non-malicious side, curious hackers may find intellectual challenges in breaking into information systems and web sites without any intent to cause harm to the organization. In some cases, the attacker just intends to annoy the organization and takes great pleasure in letting the organization know that the system has been compromised. There are other attackers whose intentions are not so benign. Attackers that are part of a loosely affiliated group or an organized group (small, mid-size, or nation-state level) with a political, military, or economic motivation can attack an organization's information system in a coordinated or unstructured manner with the specific intent to inflict damage on the organization. This malicious intent, coupled with a sophisticated attack ca-

[22] It should be noted that the sophistication of the attack may have very little to do with the knowledge and skills of the attacker. Sophisticated attack tools are now widely available from public sources (e.g., Internet web sites). Individuals with common IT skills and knowledge can launch very sophisticated attacks using low cost, powerful computing platforms. The use of sophisticated attack tools becomes even more dangerous when individuals launching the attack have significant IT skills and knowledge.

pability and adequate resources (as discussed in the next section) is the most dangerous scenario faced by the organization.

Resource considerations address both the nature of the attacker and the cost of initiating and completing the attack. Attackers can be: (i) self-directed and self-motivated (e.g., individuals or small groups operating independently without outside influences, direction, or guidance); (ii) part of an organized effort not involving a nation-state (e.g., a company engaged in commercial espionage or an entity engaged in criminal or terrorist activity); or (iii) part of an organized effort involving a nation-state (e.g., a country engaged in intelligence gathering activities, information warfare, or state-sponsored terrorism). It is assumed that as the nature of the attacker changes from an individual, self-directed/self-motivated mode to a more organized and directed mode with the involvement of organizations (including nation-states), there will be a commensurate increase in the level of effort applied to the attack and the resources available for the attack. In the case of self-directed/self-motivated individuals or small groups, it is assumed that attacks will be carried out with minimal resources (typically less than one million dollars). For groups other than nation-states with some direction and organization, it is assumed that attacks will be carried out with moderate resources (typically less than ten million dollars). And lastly, for groups or organizations funded and supported by nation-states, it is assumed that attacks will be carried out with substantial resources (typically greater than ten million dollars and including national intelligence and cyber warfare assets). Table 3 summarizes the definitions for the various threat characteristics.

| | |
|---|---|
| **TYPE OF ATTACK** | |
| | **Local:** The physical presence of the attacker is required at the site of the attack where the information system resides. |
| | **Network:** The physical presence of the attacker is not required at the site of the attack where the information system resides; rather the attacker initiates the attack from the network. |
| **CAPABILITY OF THE ATTACKER** | |
| | **SOPHISICATION OF THE ATTACK** |
| | **Low:** The attacker has common IT skills and limited knowledge about the information system being attacked and does not use attack tools. |
| | **High:** Either (or both) of the following: (i) the attacker uses sophisticated attack tools (includes publicly available tools); or (ii) the attacker uses advanced IT attack skills. |
| | **ACCESS TO THE INFORMATION SYSTEM** |
| | **Insider:** The attacker is a non-user of the information system, a non-privileged user of the information system or a privileged user of the information system. |
| | **Outsider:** The attacker is either a non-user of the information system or a public user of the information system. |
| **INTENT OF THE ATTACKER** | |
| | **Non-malicious:** The attacker has no intent to do damage to the information system or to cause harm to the organization but pursues the attack due to curiosity, boredom, or for the intellectual challenge. |
| | **Malicious:** The attacker has clear intent to do damage to the information system and to cause harm to the organization adversely affecting the organization's operations or assets. |
| **RESOURCES OF THE ATTACKER** | |
| | **Minimal:** The attacker is: (i) self-directed and self-motivated; (ii) operates independently (as an individual or in a small group) without outside influences, direction, or guidance; and (iii) carries out attack with minimal resources (typically less than one million dollars). |
| | **Moderate:** The attacker is: (i) part of a group or organization not involving a nation-state (e.g., a company engaged in commercial espionage or an entity engaged in criminal or terrorist activity); (ii) operates with significant direction and guidance from the leadership of the group or organization and is subject to the influences of the group or organization; and (iii) carries out attack with moderate resources (typically less than ten million dollars). |
| | **Substantial:** The attacker is: (i) part of a group or organization involving a nation-state (e.g., a country engaged in intelligence gathering activities, information warfare, or state-sponsored terrorism); (ii) operates with significant direction and guidance from the leadership of the group or organization and is under the direct authority of the group or organization; and (iii) carries out attack with substantial resources (typically greater than ten million dollars). |

**TABLE 3: DEFINITIONS FOR THREAT CHARACTERISTICS**

Threat coverage is based on two factors: (i) an estimate of the effectiveness of the baseline security controls against the stated threats; and (ii) the situation or context in which the controls are employed. The situation or context in which the controls are employed can be a source of risk mitigation. Several potential risk mitigation factors have been identified to include: (i) the level of maximum potential impact to the organization should there be a breach in security (in accordance with FIPS Publication 199); (ii) the attacker's intent (malicious or non-malicious); (iii) whether the attack requires the physical presence of the attacker; (iv) the resources applied to the attack; and (v) the purposefulness and directed focus of the attacker. For example, a significant portion of threat coverage may come from the fact that the maximum impact of loss to the organization is low (e.g., lower value assets may be less appealing targets than higher value assets), there is a lack of malicious intent on the part of the attacker making that attack less threatening, the attack lacks sufficient resources making it less likely to succeed, or there is a lack of direction and focus on the part of the attacker decreasing the likelihood of pursuing the attack to completion in lieu of moving to another target.

Tables 4, 5, and 6 provide an estimate of threat coverage and supporting rationale for the three security control baselines—that is, which threats are expected to be countered by the respective baseline controls when applied to an information system and which threats can be expected to remain unchecked. The estimate of threat coverage indicates one of three conditions: (i) the security controls in the selected baseline provide adequate security and coverage for the stated threats (indicated by a ✓ symbol); (ii) the combination of the security controls in the selected baseline and the situation and context in which the controls are employed including any general risk mitigation factors provide adequate security and coverage for the stated threats (indicated by a ✓- symbol); and (iii) the security controls in the selected baseline do not provide adequate security and coverage for the stated threats (indicated by an **X** symbol). Organizations should employ risk assessments during the system development life cycle to tailor the security controls in the baseline, as appropriate. If the estimated threat coverage appears to be inadequate, security controls may be strengthened (increasing the robustness level) or additional controls may be added. The organization's judgment as to the likelihood of threat sources exploiting identified vulnerabilities in their information systems and the organization's tolerance for risk to its operations and assets should guide the security control selection process.

| THREAT CHARACTERISTICS | *BASELINE SECURITY CONTROL COVERAGE ESTIMATE* | | |
|---|---|---|---|
| | **LOW** | **MODERATE** | **HIGH** |
| **ERRORS** (MACHINE OR HUMAN) | ✓- | ✓- | TBD |
| **EVENTS OF NATURE** | | | |
| DISRUPTION | ✓- | ✓ | TBD |
| DISASTER (LOCAL) | **X** | ✓ | TBD |
| DISASTER (REGIONAL) | **X** | **X** | TBD |

| **LEGEND** | | |
|---|---|---|
| | ✓ | The security controls in the selected baseline provide adequate security and coverage for the stated threats. |
| | ✓- | The combination of the security controls in the selected baseline and the situation and context in which the controls are employed including any general risk mitigation factors provide adequate security and coverage for the stated threats. |
| | **X** | The security controls in the selected baseline do not provide adequate security and coverage for the stated threats. |

**TABLE 4: BASELINE COVERAGE ESTIMATE FOR ERRORS / EVENTS OF NATURE**

| THREAT CHARACTERISTICS | | | | BASELINE SECURITY CONTROL COVERAGE ESTIMATE | | |
|---|---|---|---|---|---|---|
| | | | | LOW | MODERATE | HIGH |
| **INTENTIONAL ATTACK:** LOCAL (Physical presence of attacker required at the site of attack) | | | | | | |
| | **ATTACK SOPHISTICATION:** LOW | | | ✓ | ✓ | TBD |
| | **ATTACK SOPHISTICATION:** HIGH | | | | | |
| | | **ATTACKER INTENT:** NON-MALICIOUS | | | | |
| | | | **ATTACKER RESOURCES :** ALL LEVELS (MINIMAL, MODERATE, SUBSTANTIAL) | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓ | ✓ | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | ✓- | TBD |
| | | **ATTACKER INTENT:** MALICIOUS | | | | |
| | | | **ATTACKER RESOURCES :** MINIMAL | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓ | ✓ | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | ✓- | TBD |
| | | | **ATTACKER RESOURCES :** MODERATE | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓ | ✓ | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | **X** | TBD |
| | | | **ATTACKER RESOURCES :** SUBSTANTIAL | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓ | ✓ | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | **X** | TBD |

| LEGEND | | |
|---|---|---|
| | ✓ | The security controls in the selected baseline provide adequate security and coverage for the stated threats. |
| | ✓- | The combination of the security controls in the selected baseline and the situation and context in which the controls are employed including any general risk mitigation factors provide adequate security and coverage for the stated threats. |
| | **X** | The security controls in the selected baseline do not provide adequate security and coverage for the stated threats. |

**TABLE 5: BASELINE COVERAGE ESTIMATE FOR LOCAL ATTACKS**

| THREAT CHARACTERISTICS | | | | BASELINE SECURITY CONTROL COVERAGE ESTIMATE | | |
|---|---|---|---|---|---|---|
| | | | | LOW | MODERATE | HIGH |
| **INTENTIONAL ATTACK:** NETWORK (Physical presence of attacker not required at the site of attack) | | | | | | |
| | **ATTACK SOPHISTICATION:** LOW | | | ✓ | ✓ | TBD |
| | **ATTACK SOPHISTICATION:** HIGH | | | | | |
| | | **ATTACKER INTENT:** NON-MALICIOUS | | | | |
| | | | **ATTACKER RESOURCES :** ALL LEVELS (MINIMAL, MODERATE, SUBSTANTIAL) | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓- | ✓- | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | ✓- | TBD |
| | | **ATTACKER INTENT:** MALICIOUS | | | | |
| | | | **ATTACKER RESOURCES :** MINIMAL | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓- | X | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | ✓- | X | TBD |
| | | | **ATTACKER RESOURCES :** MODERATE | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | ✓- | X | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | X | X | TBD |
| | | | **ATTACKER RESOURCES :** SUBSTANTIAL | | | |
| | | | **ATTACKER ACCESS:** OUTSIDER | X | X | TBD |
| | | | **ATTACKER ACCESS:** INSIDER | X | X | TBD |

| LEGEND | | |
|---|---|---|
| | ✓ | The security controls in the selected baseline provide adequate security and coverage for the stated threats. |
| | ✓- | The combination of the security controls in the selected baseline and the situation and context in which the controls are employed including any general risk mitigation factors provide adequate security and coverage for the stated threats. |
| | X | The security controls in the selected baseline do not provide adequate security and coverage for the stated threats. |

**TABLE 6: BASELINE COVERAGE ESTIMATE FOR NETWORK-BASED ATTACKS**

## APPENDIX F

# BASELINE SECURITY CONTROLS – LOW

FIPS PUBLICATION 199 SECURITY CATEGORIZATION—LOW IMPACT

The minimum security controls listed in this baseline (which were extracted from the Catalog of Security Controls in Appendix J) are a recommended starting point for agencies in assessing the actual security controls that may be necessary to protect their information systems. The baseline is associated with the initial security categorization of the information system in accordance with FIPS Publication 199 and provides an estimated threat coverage described in the tables in Appendix E. Organizations should employ risk assessments during the system development life cycle to tailor the security controls in the baseline, as appropriate. The final agreed upon set of security controls should be documented in the security plan providing a justification and rationale for any adjustments to the initial baseline.

The baseline security controls in this Appendix consist of two key components: (i) a *control objective* section; and (ii) a *control description* section. The control objective section provides the overall objective for the particular security control when applied to an information system. The control description section provides the specific control requirements and details of each control. The security controls in the baseline are selected from the catalog in Appendix J and represent a subset of the controls in the catalog. Therefore, the numbering of the controls in the baseline may not always be consecutive.



### Table of Contents – Low Baseline

## MANAGEMENT CONTROLS

**FAMILY:** RISK ASSESSMENT (RA)

### RA-1.b SECURITY CATEGORIZATION

CONTROL OBJECTIVE: The potential impact on organizational operations and assets resulting from the operation of the information system is identified.

The information system is categorized in accordance with FIPS Publication 199 and NIST Special Publication 800-60. The security categorization is explicitly documented and approved by an appropriate senior official.

### RA-2.b RISK ASSESSMENT

CONTROL OBJECTIVE: Risks to organizational operations and assets resulting from the operation of the information system are identified.

An assessment of risk to organizational operations and assets due to the operation of the information system is performed and documented on an [*Assignment: time period which is at least annually*] and whenever there are significant changes to the system, facilities, or other conditions that may impact the security or authorization status of the system. The risk assessment (either formal or informal) is consistent with the intent of NIST Special Publication 800-30. The documented risk assessment includes the following: (i) identification of the conditions for reassessment, indicating the period for periodic reassessment and defining the level of change to the information system or environment that will cause a reassessment to occur; (ii) identification of the security authorization boundary; (iii) the current information system configuration including connections to other systems; (iv) actions that will be taken to ensure that the boundary definition is accurately updated periodically; (v) an inventory of information system assets; (vi) identification and assessment of threat sources; (vii) identification and assessment of information system vulnerabilities; and (viii) identification of risks from third party connections.

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY PLANNING (PL)

### PL-1.b RULES OF BEHAVIOR AND ACCEPTABLE USE

CONTROL OBJECTIVE: Establish information system policy for rules of behavior and acceptable use when organizational policy is not adequate to address system needs.

A set of rules that describes the security operations of the information system and clearly delineates security responsibilities and expected behavior of all system owners, users, operators, and administrators is in place. Rules include the consequences of inconsistent behavior or non-compliance. Rules include all significant aspects of information system use, including policy on use of electronic mail. Signed acknowledgement of the rules is a condition of access.

### PL-2.b ACCESS CONTROL POLICY

CONTROL OBJECTIVE: Establish an information system policy for access control when organizational policy is not adequate to address system needs.

An explicit, documented access control policy establishes the rules to be implemented to ensure that only designated individuals, under specified conditions (e.g., time of day, port of entry, type of authentication, etc.) can: (i) access the information system (i.e., logon, establish connection); (ii) activate specific system commands; (iii) execute specific programs and procedures; and (iv) create, view, or modify specific objects (programs, information, system parameters). The policy has provisions for periodic review of access authorizations. This policy covers both discretionary and non-discretionary controls. Discretionary controls are those controls established at the discretion of the information owner, usually with constraints called out in the policy. Non-discretionary controls (e.g., restrictions on the viewing of export-controlled information or personal medical information), are those controls established by organizational policy and not subject to determination by the owner of the information.

### PL-3.b GROUP IDENTIFICATION AND AUTHENTICATION POLICY

CONTROL OBJECTIVE: Establish information system policy for group identifiers and the use of those identifiers when organizational policy is not adequate to address system needs.

An explicit, documented group identification and authentication policy establishes the rules to be implemented to ensure that group authenticators are used for information system access only when explicitly authorized and in conjunction with other authenticators as appropriate.

### PL-5.b ACCOUNTABILITY POLICY

CONTROL OBJECTIVE: Establish information system policy for accountability when organizational policy is not adequate to address system needs.

An explicit, documented accountability policy establishes the rules to be implemented to ensure that information system users can be held accountable for their actions as needed. Accountability policy elements are, for example: (i) purposes for accountability (e.g., deterrent, incident forensics, etc.); (ii) required granularity for accountability (e.g., to the granularity of individual users); and (iii) time period for which accountability information must be available (e.g., five years).

### PL-6.b CONTINGENCY PLANNING AND OPERATIONS POLICY

CONTROL OBJECTIVE: Establish information system policy for contingency operations when organizational policy is not adequate to address system needs.

An explicit, documented contingency planning and operations policy addresses all critical aspects of contingency planning consistent with NIST Special Publication 800-34.

**PL-7.b CONFIGURATION MANAGEMENT POLICY**

CONTROL OBJECTIVE: Establish information system policy for configuration management and control of hardware, software and firmware assets when organizational policy is not adequate to address system needs.

An explicit, documented configuration management policy establishes the rules to be implemented to ensure that organization's track and control the hardware, software, and firmware components that comprise the information system.

**PL-8.b INCIDENT RESPONSE POLICY**

CONTROL OBJECTIVE: Establish information system policy for monitoring and responding to incidents when organizational policy is not adequate to address system needs.

An explicit, documented incident response policy addresses all critical aspects of incident handling and response consistent with NIST Special Publication 800-61.

**PL-9.b SECURITY TRAINING AND AWARENESS POLICY**

CONTROL OBJECTIVE: Establish information system policy for security training and awareness when organizational policy is not adequate to address system needs.

An explicit, documented security training and awareness policy addresses all critical aspects of security training and awareness consistent with NIST Special Publications 800-16 and 800-50.

**PL-10.b PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for physical and environmental protection when organizational policy is not adequate to address system needs.

An explicit, documented physical and environmental protection policy addresses all critical aspects of physical and environmental protection consistent with General Services Administration policies, directives, regulations, and guidelines.

**PL-11.b PERSONNEL SECURITY POLICY**

CONTROL OBJECTIVE: Establish information system policy for personnel security when organizational policy is not adequate to address system needs.

An explicit, documented personnel security policy addresses all critical aspects of personnel security consistent with Office of Personnel Management policies, directives, regulations, and guidelines.

**PL-12.b MEDIA PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for media protection when organizational policy is not adequate to address system needs.

An explicit, documented media protection policy addresses all critical aspects of media protection to include: (i) media access; (ii) media labeling; (iii) media transport; (iv) media destruction and disposal; (v) media sanitization and clearing; (vi) media storage; and (vii) disposition of media records.

**PL-13.b SYSTEM MAINTENANCE POLICY**

CONTROL OBJECTIVE: Establish information system policy for information system hardware and software maintenance when organizational policy is not adequate to address system needs.

An explicit, documented information system maintenance policy addresses all critical aspects of hardware and software maintenance to include: (i) scheduling of periodic maintenance; (ii) main-

tenance tools; (iii) remote maintenance; (iv) maintenance personnel; and (v) timeliness of maintenance.

**PL-14.b SECURITY PLANNING**

CONTROL OBJECTIVE: In accordance with organizational policy, facilitate achieving adequate security by documenting and approving a security plan for the information system.

The content of the security plan is compliant with OMB policy and consistent with the intent of NIST Special Publication 800-18. The security plan is approved by appropriate organization officials and incorporated into the information resources management strategic plan. The security plan is reviewed and updated as needed to reflect current conditions, both on a regular basis every [*Assignment: time period*] and whenever there are significant changes defined as [*Assignment: criteria for significant changes*] to the information system, facilities, or other conditions that may impact security.

## MANAGEMENT CONTROLS

**FAMILY:** SYSTEM AND SERVICES ACQUISITION (SA)

### SA-1.b ACQUISITION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the risk of acquiring ineffective security capabilities by meeting specified requirements.

A discrete line item for information security (or information assurance) is established in programming and budget documentation.

*Solicitation Documents*

The solicitation documents for the information system (e.g., Requests for Proposals), include security controls and security test and evaluation procedures. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

*Information System Specifications*

For all new information systems and major upgrades to existing systems, there are detailed system specifications prepared and reviewed by management. An organization reference document such as a security recommendation guide (SRG) or a security technical implementation guide (STIG) constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products. If organization reference documents are not available, other government guidelines or vendor literature are acceptable sources. Advice from information security specialists is used in the development of requirements, acquisition documentation, and source selection. Appropriate security controls for the information system and associated security test and evaluation procedures are developed as part of the procurement action. Additionally, a clear description is provided of the security attributes of each network service.

*Vendor or Developer Expectations*

For acquired and developed information systems, identify, as early in the life cycle as possible, the network ports, protocols, and services to be used. Design reviews are conducted on the information systems and security test and evaluation is conducted prior to placing the systems into operation. Test results for the developmental information systems are documented. Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. Vendor supplied system software is supported by the vendor.

*Use of Evaluated and Validated Products*

For acquisition of security and security-enabled commercial off-the-shelf (COTS) information technology products, when multiple products meet organizational requirements, preference is given to products that have been evaluated and validated through one or more of the following sources: (i) the NIAP Common Criteria Evaluation and Validation Scheme; (ii) the International Common Criteria Recognition Arrangement; and/or (iii) the NIST Cryptographic Module Validation Program.

### SA-2.b COPYRIGHTED AND PUBLIC DOMAIN WORKS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to comply with software license restrictions and to ensure appropriate use of software and capabilities such as peer-to-peer file trading networks.

The use of copyrighted software or shareware and personally owned software is controlled and documented. Open source software use is permitted but the software is assessed to determine its security impact prior to use. Public domain software products (excluding open source software products) are not used in organization information systems unless compelling reasons are established, the product is assessed for security impacts, and explicitly approved for use. Binary or ma-

chine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used unless they are necessary for mission accomplishment and there are no alternative solutions available. Such products are assessed for security impacts, and explicitly approved for use. Purchased software is used in accordance with contract agreements and copyright laws. Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software. Use of publicly accessible peer-to-peer file trading networks is also controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**SA-3.b SYSTEM DOCUMENTATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that adequate documentation is available for the information system.

There is adequate vendor-supplied documentation of purchased software, hardware, and firmware for the information system. There is adequate documentation for applications and for in-house developed software, hardware, and firmware.

*Administrator Guides and Manuals*

There are adequate administrator guides and/or manuals for the information system. Documentation includes guides and/or manuals for the information system's privileged users. The guides and/or manuals provide, at a minimum, information on: (i) configuring, installing, and operating the system; (ii) making optimum use of the system's security features; and (iii) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation is updated as new vulnerabilities are identified.

*User Guides and Manuals*

There is a general user's guide that describes the security mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact. Information system, administrator, and user documentation are updated to include security controls added since development and as new vulnerabilities are identified.

**SA-4.b OUTSOURCED INFORMATION SYSTEM SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks from outsourced services by explicitly addressing the need for effective security controls at the service provider.

Acquisition or outsourcing of dedicated information system security services such as: (i) incident monitoring, analysis and response; (ii) operation of information system security devices (e.g., firewalls); or (iii) key management services, are supported by a risk assessment and approved by the appropriate, designated organization official. Acquisition or outsourcing of information system services explicitly addresses government, service provider and end user security roles and responsibilities. Appropriate controls are applied to outsourced software development. Appropriate policies and procedures concerning activities of external third parties (e.g., service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for: (i) security clearances (where appropriate and required); (ii) background checks; (iii) required expertise; (iv) confidentiality agreements; (v) security roles and responsibilities; (vi) connectivity agreements; and (vii) individual accountability.

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY CONTROL REVIEW (CR)

### CR-1.b INFORMATION SYSTEM ASSESSMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to support knowledgeable, risk-based information system authorization by performing a technical assessment of the system.

Assessments of the information system are conducted to: (i) determine if security controls are correctly implemented and, as implemented, are effective in their application; (ii) ensure that security-applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines are met. Assessments of security controls are conducted: (i) prior to initial operational capability and authorization to operate; (ii) prior to each re-authorization to operate; or (iii) when a significant change to the information system occurs. Routine self-assessments are conducted every [*Assignment: time period (e.g., annually)*] to monitor the effectiveness of security controls. Management reviews of system assessment results are conducted and documented forming the basis for management decisions and action plans. Inspection reports, including self-assessment reports, corrective actions and supporting documentation are retained for a minimum [*Assignment: time period (e.g., five years)*]. Assessments are conducted in a manner to minimize disruption of operations.

### CR-2.b VULNERABILITY SCANNING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*].

## MANAGEMENT CONTROLS

**FAMILY:** PROCESSING AUTHORIZATION (PA)

### PA-1.b AUTHORIZE INFORMATION SYSTEM CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from connections to information systems by explicit authorization prior to establishing connections.

Management authorizes in writing all connections to other information systems (including systems owned and operated by another program, organization, or contractor). The connections are compliant with established organizational connection rules and approval processes. Connection agreements consistent with intent of NIST Special Publication 800-47 are in place whenever the information system is connected to systems not under the control of the same authorizing official. Trust relationships among hosts and external entities are appropriately restricted. A list is developed and maintained, along with evidence of deployment planning and coordination and exchange of connection rules and requirements for: (i) applications (on all hosting information systems, current and potential); and (ii) the information system (including all hosted applications). Criteria are defined for conditions under which information system connections are to be disabled.

### PA-2.b AUTHORIZE MOBILE CODE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from mobile code by explicit authorization prior to establishing a mobile code capability.

Deployment of mobile code is restricted based on its potential to cause damage to the information system if used maliciously. Mobile code registration, approval, and control procedures to prevent the development, acquisition, or introduction of unacceptable mobile code within the information system, are implemented. All mobile code or executable content employed is registered unless otherwise approved by the authorizing official. Uploading of mobile code or executable content from one organizational information system to another system is to be similarly authorized.

### PA-3.b AUTHORIZE REMOTE ACCESS CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from remote access (e.g., dial-up access or Internet access) by explicit authorization prior to establishing a remote access capability.

The number of users who can access the information system from remote locations (for information systems other than public web servers or systems specifically designed for public access) is limited and justification for such access is documented, monitored, and approved by a designated organization official. Dial-up lines, other than those that are protected with FIPS 140-2 validated cryptography, are not used for gaining access to an information system that processes organizational information unless the authorizing official provides specific written authorization for a system to operate in this manner. Actions such as periodic monitoring are taken to ensure that installed equipment does not include unanticipated dial-up capabilities.

### PA-4.b AUTHORIZE COLLABORATIVE COMPUTING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from collaborative computing by explicit authorization prior to establishing a collaborative computing capability.

Running collaborative computing mechanisms (e.g., the IETF standard Web-based Distributed Authoring and Versioning that enables collaborative editing and file management on remote Web servers) on information systems requires explicit authorization by the authorizing official or au-

thorizing official's designated representative. When granted, authorization is specific, identifying allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used.

**PA-5.b AUTHORIZE WIRELESS ACCESS POINT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from wireless connections by explicit authorization prior to establishing a wireless capability.

Installation of wireless access points into organizational networks is discouraged and requires explicit authorization by the authorizing official.

**PA-6.b AUTHORIZE INFORMATION SYSTEM OPERATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure explicit management authorization to operate the information system and acceptance of risks to the organization's operations and assets.

In compliance with NIST Special Publication 800-37, explicit authorization to operate the information system is received prior to placing the system into operation. If the authorization decision is an interim approval to operate, then: (i) the authorization is granted for a maximum time period (typically in accordance with the designated FIPS Publication 199 security category of the information system) of [*Assignment: time period for each security category (e.g., eighteen months, twelve months, six months)*]. An explicit plan for corrective action is in-place, being effectively implemented, and monitored by the authorizing official. Re-authorization is obtained prior to continued operation following significant information system changes. Re-authorization is obtained at least every [*Assignment: time period, a maximum of three years*].

## OPERATIONAL CONTROLS

**FAMILY:** PERSONNEL SECURITY

### PS-1.b POSITION REVIEW

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to review information system-related positions for criticality/sensitivity.

All positions within the organization are assigned a criticality/sensitivity rating (e.g., low, moderate, high) based on the information system access given to individuals filling those positions. The criticality/sensitivity rating is consistent with the FIPS Publication 199 security categories of the information systems accessible to the individuals filling the designated positions. All positions are reviewed for criticality/sensitivity rating periodically every [*Assignment: time period (e.g., five years)*].

### PS-2.b PERSONNEL SCREENING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is not granted without first verifying that the individual seeking access meets organizational personnel security requirements.

Individuals requiring access to information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access for access authorization in accordance with organizational personnel security policies. Privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls), are screened prior to access and periodically every [*Assignment: time period (e.g., two years)*]. For prospective employees, references are contacted and background checks performed, as appropriate. Periodic reinvestigations are performed every [*Assignment: time period, no more than five years*], consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management. Security agreements are required for employees and contractors assigned to work with mission information. The period during which nondisclosure requirements remain in effect is identified.

### PS-3.b TERMINATION AND TRANSFER

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is terminated upon personnel transfer or termination.

Termination and transfer procedures include: (i) exit interview procedures; (ii) return of property, keys, identification cards, passes, etc.; (iii) notification to security management; and (iv) immediately escorting employees terminated for cause out of the organization's facilities.

### PS-4.b THIRD PARTY PERSONNEL SECURITY

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that service providers and other third parties apply appropriate personnel security measures.

Personnel security measures employed by service providers and third parties (e.g., service bureaus, contractors, other organizations providing system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include, if appropriate, provisions for: (i) security clearances; (ii) background checks; (iii) required expertise; and (iv) confidentiality agreements. Personnel security measures employed by service providers and third parties are consistent with the intent of NIST Special Publication 800-35.

## OPERATIONAL CONTROLS

**FAMILY:** PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

### PE-1.b IDENTIFICATION OF SENSITIVE FACILITIES AND RESTRICTED AREAS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to identify and designate sensitive facilities and restricted areas containing information systems.

The organization identifies and designates sensitive facilities and restricted areas (i.e., areas, rooms, or groups of rooms containing information system servers, controlled interface equipment, associated peripherals or communications equipment that must be relied upon for the correct enforcement of the system security policy). The organization also identifies and designates non-sensitive facilities and non-restricted areas, (i.e., areas, rooms, or groups of rooms containing information system components not involved in security policy enforcement and possibly accessible to the general public).

### PE-2.b AUTHORIZE PHYSICAL ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage, and make available for enforcement, authorizations for physical access to sensitive facilities and restricted/controlled areas containing information systems.

A list of persons with authorized physical access to sensitive facilities and restricted/controlled areas containing information systems (i.e., access authorizations) is maintained. Access lists also show which individuals are authorized to operate the information system or supporting peripheral equipment. Access lists are documented on standard forms, maintained on file, and approved by appropriate organization officials. The list of persons with authorized physical access to sensitive facilities and restricted/controlled areas is reviewed by appropriate organization officials every [*Assignment: time period (e.g., as needed and at least annually)*].

### PE-3.b PHYSICAL ACCESS ENFORCEMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply physical access controls at designated physical entry points within sensitive facilities and restricted/controlled areas containing information systems.

Physical security perimeters are defined by the organization. Sensitive facilities and restricted/controlled areas are prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that control access. The main entrance to sensitive facilities and restricted areas is controlled/manned. Secondary entrances have cameras and/or electronic entry detection devices (e.g., card keys), to monitor access. Apparent security violations or suspicious physical access activities are investigated and remedial actions taken. Every physical access point to sensitive facilities or restricted areas housing information systems that process or display information is controlled during working hours and guarded or locked during non-work hours. Identification badges are worn. Access authorization is verified before granting physical access. Unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations, etc.). The organization controls access to non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) as appropriate in accordance with the organization's assessment of risk.

**PE-5.b VISITOR CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control visitor access to sensitive facilities and restricted/controlled areas containing information systems and system/media libraries.

Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks. Visitors, contractors, and maintenance personnel are formally signed in, escorted, and activities monitored when required. Registers are maintained and include: (i) the name; (ii) date; (iii) time of entry; (iv) time of departures; (v) purpose of visit; and (vi) person(s) visited. The register is closed out [*Assignment: time period (e.g., at the end of each month)*] and reviewed by appropriate organization officials.

**PE-7.b ROUTINE PHYSICAL SECURITY CHECKING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance physical security by periodically checking for physical security compliance.

Routine checks (e.g., end of the day security checks and unannounced security checks) are performed periodically to ensure that information is being properly handed and stored.

**PE-9.b STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to securely store information and information systems.

Documents/equipment are stored in approved containers or facilities with maintenance and accountability procedures. All restricted areas used to protect information meet criteria for secured area or security room, or provisions are made to store high value items in appropriate containers during non-working hours. Organizational information in any form is protected during non-working hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization. Mobile and portable information systems are stored securely. Organizational information is locked in cabinets or sealed in packing cartons while in transit. Organizational information remains in the custody of an authorized individual. Accountability is maintained during movement.

**PE-10.b ACCESS DEVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance physical security by using devices to control access.

Keys, combinations, or other access devices are needed to enter sensitive facilities or restricted/controlled areas that contain information or information systems unless other protective measures (e.g., guards) are in place. Keys, combinations, or other access devices are secured. Combinations and keys are changed periodically with changes occurring at least every [*Assignment: time period (e.g., annually for combinations)*]. Combinations are changed when an employee retires, transfers to another position, or is no longer an employee. An envelope containing the combination or duplicate key is secured in a container with the same or higher protections as the material the lock secures. Keys are changed as necessary to prevent or respond to compromise. Issued keys or other entry devices are regularly inventoried.

**PE-12.b IDENTIFY NATURAL DISRUPTION/DISASTER PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide an effective response to disruptions and natural disasters by explicitly indicating the intended disruption/disaster coverage.

The nature of the disruptions or natural disasters being mitigated and the extent of the expected mitigation are clearly described.

**PE-13.b PLUMBING LINES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the potential damage from plumbing leaks.

Building plumbing lines do not endanger the information system facility or, at a minimum, shut-off valves and their operating procedures exist and are known.

**PE-14.b EMERGENCY LIGHTING**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance safety and availability by providing lighting in the event of a power outage.

An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.

**PE-15.b FIRE PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to prevent, detect, and respond to fire.

Fire suppression and prevention devices and systems, (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, battery-operated or electric stand-alone smoke detectors) are installed, available, and working properly should an alarm be sounded or a fire be detected. The fire department receives an automatic notification of any activation of the smoke detection or fire suppression system. Fire suppression and prevention devices and systems are periodically checked. Fire ignition sources, such as potential failures of electronic devices or wiring, improper storage of materials, are reviewed periodically. Information system facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

**PE-16.b TEMPPERATURE AND HUMIDITY CONTROLS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control the temperature of facilities containing information systems.

Heating and air-conditioning systems are regularly maintained. Temperature and humidity are controlled automatically.

**PE-17.b POWER**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to maintain safe power for the information system.

Power cabling supporting the information system is protected from damage. A master power switch or emergency cut-off switch to information system equipment is present. It is located near the main entrance of the information system area and it is labeled and protected by a cover to prevent accidental shut-off.

**PE-20.b ENVIVONMENTAL CONTROL TRAINING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel on the use of environmental controls.

Individuals that maintain environmental controls or would use the environmental controls in the event of an emergency receive initial training in the operation of the controls. Periodic refresher training is provided every [*Assignment: time period (e.g., annually)*].

**PE-21.b EQUIPMENT DELIVERY AND REMOVAL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the flow of equipment into and out of the organization.

The organization controls the hardware, firmware, and software entering and exiting the facility, the movement of these items within the facility, and maintains appropriate records of those items. Delivery and loading areas are controlled and, if possible, isolated from information system and system/media libraries to avoid unauthorized access. Information system hardware, firmware, software, or information belonging to the organization is not removed without authorization.

## OPERATIONAL CONTROLS

**FAMILY:** CONTINGENCY PLANNING AND OPERATIONS (CP)

### CP-1.b CONTINGENCY PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, an effective response to an information system disruption is enabled by developing a system contingency plan.

A contingency plan is produced for the information system that is compliant with OMB policy and consistent with the intent of NIST SP 800-34. In addition, key affected parties approve the contingency plan for the system. The plan is reviewed once a year, reassessed, tested and, if appropriate, revised to reflect changes in hardware, software and personnel.

### CP-2.b CONTINGENCY PLAN TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel in their contingency roles and responsibilities.

Operational and support personnel (including managers and users of the information system) have received training in contingency operations and understand their emergency roles and responsibilities. Personnel receive periodic training in emergency fire, water, and alarm incident procedures.

### CP-3.b CONTINGENCY PLAN EXERCISES AND DRILLS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically test contingency plans and response capabilities.

Contingency plans [*Selection: in their entirety | [Assignment: portions*]] are exercised [*Assignment: time period (e.g., annually, quarterly, or semi-annually)*]. Test results are documented and provided to appropriate organizational officials for review.

### CP-4.b CONTINGENCY PLAN STORAGE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by securely storing an up-to-date copy of the contingency plan for the information system off-site.

Copies of the current contingency plan are stored in a secure location at an alternate site accessible by management and other key personnel.

### CP-5.b OFF SITE BACKUP STORAGE SITES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by ensuring geographic separation of routine information system operations and backup storage sites.

Backup storage sites are geographically removed from the primary site and environmentally and physically protected.

### CP-6.b INFORMATION BACKUP AND RESTORE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to regularly back up information.

A capability exists to conduct backup storage and restoration of information and access controls. Information backup for the information system is documented and performed [*Assignment: time period which is at least monthly*]. Procedures are in place to test backup via restoration of informa-

tion from backup media every [*Assignment: time period which is at least annually*]. Appropriate physical and technical protection of the backup and restoration files, hardware, firmware, and software, (e.g., router tables, compilers, and other security-related system software) are in place. Audit logs/records are backed up not less than weekly onto a different information system or media than the system being audited. Generally, audit logs/records are retained for [*Assignment: time period which is at least every six months*]. For these specific information types, the audit records are retained for the time period indicated: [*Assignment: pairs of information type / time-period*]. System and application documentation are maintained at the off-site storage location. The technology is implemented in such a manner as to provide appropriate availability, including consideration of: (i) backup procedures; (ii) system configuration; (iii) redundancy; (iv) environmental controls; (v) staff training; and (vi) routine maintenance. Restoration of any security-relevant segment of the information system state (e.g., access control lists, cryptographic keys, deleted system status information) is possible without requiring destruction of other system information. Standalone computer workstation backup information, software and current operating procedures are stored in accordance with the contingency plan.

**CP-7.b BACKUP MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable backing up information and the information system state.

Mechanisms provide for sufficient backup storage capability. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time. A capability to conduct the following types of backup exists: (i) full (complete backup); and (ii) [*Selection of one or more: incremental (changes since last incremental) | differential (changes since last full)*].

**CP-9.b RESTORING INFORMATION UNDER EMERGENCY CONDITIONS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for physical access to information system facilities under emergency conditions.

Facility access is allowed in support of restoration of lost information under the contingency plan in the event of an emergency. Emergency and temporary access authorizations are: (i) documented on standard forms and maintained on file; (ii) approved by appropriate organization managers; (iii) securely communicated to the security function; and (iv) automatically terminated after a predetermined period.

**CP-10.b INFORMATION SYSTEM RECOVERY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to securely recover the information system after failure or other contingency.

Recovery procedures and mechanisms exist to ensure that recovery is done in a trusted, secure, and verifiable manner. Contingency plans, software procedures, and installed security and backup provisions protect against improper modification of information in the event of an information system failure. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures are in place. Adequate manual processing procedures are available for use until automated operations are restored. Restart capabilities are part of any operation that updates files and consumes large amounts of computer time. Mechanisms to allow for the restoration of the information system in a secure and verifiable manner are implemented. Restoration of operational capabilities with minimal loss of service or information is provided. Assurance is provided that the state of the information system after the restore reflects any security-relevant changes to the system between the backup and the restore. Restoration of any security-relevant segment of the

system state (e.g., access control lists, cryptographic keys, deleted system status information) is obtained without requiring destruction of other system data.

**CP-11.b MANAGEMENT ACCOUNTABILITY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to hold management accountable for the ability to respond to contingencies.

Management is able to show how the organization responds to specific disasters/disruptions to: (i) protect lives; (ii) limit damage; (iii) protect information; (iv) circumvent security controls only according to established bypass procedures; and (vi) minimize the impact on organizational operations and assets.

**CP-13.b ALTERNATE COMMUNICATION SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for alternate communications services.

Arrangements are in place for alternate [*Selection (one or more): long haul | short haul*] communications services capable of restoring adequate communications to accomplish the following mission functions [*Assignment: list of functions*] without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations and communications capabilities are unavailable. Arrangements are planned for travel and lodging of necessary personnel if needed.

## OPERATIONAL CONTROLS

**FAMILY:** CONFIGURATION MANAGEMENT (CM)

### CM-1.b CONFIGURATION MANAGEMENT PLAN

CONTROL OBJECTIVE: Enable knowing the information system configuration and controlling changes throughout the system development life cycle by developing a configuration management plan when the organization's plan is not adequate to address system needs.

The configuration management plan for the information system is consistent with the intent of IEEE Standard 828-1998 (or successor if superceded). The configuration management plan is evaluated periodically every [*Assignment: time period (e.g., annually)*] and updated as necessary to verify the plan and the ability of those tasked to carry out the plan.

### CM-2.b CONFIGURATION MANAGEMENT PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage the configuration of the information system.

The configuration management process is consistent with the organization's information technology architecture plans. Formally documented configuration management roles, responsibilities, and procedures to include the management of information system security information and documentation are in place. Changes to the information system are authorized by appropriate organization officials and are not permitted outside of the configuration management process. Personnel involved in configuration management have been trained and are familiar with the organization's configuration management process. The guidance is appropriate for personnel with varying levels of skill and experience. Appropriate tools are used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates. Production program changes are periodically reviewed by appropriate organization officials to determine whether access controls and change controls are being followed. The configuration management plan is evaluated periodically every [*Assignment: time-period (e.g., annually)*].

*Information System Components*

Distribution of new software is controlled. Software licensing agreements are enforced and violations of those agreements are prohibited. The use of personal and public domain software is restricted. The name, brand, type, model, version/release number, and physical location of each information system component (hardware, software, and firmware) are identified and documented.

*Change testing*

Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control). Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control). Test plans include appropriate consideration of security. Unit, integration, and system testing are performed and approved in accordance with the test plan and applying a sufficient range of valid and invalid conditions. A comprehensive set of test transactions and information is developed that represents the various activities and conditions that will be encountered during information system operation. Test results are documented and appropriate responsive actions are taken based on the results. The type of test information to be used on the information system is specified, (i.e., live or simulated). Test results are reviewed and documented. All patches, upgrades, and new applications are tested prior to deployment (compliance testing).

**CM-3.b BASELINE CONFIGURATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to document and maintain a current baseline, operational configuration of the hardware, software, and firmware that comprise the information system.

A current and comprehensive baseline inventory of all hardware and firmware (to include manufacturer, type, and version) required to support the operation of the information system is maintained as part of the configuration management plan. A current and comprehensive baseline inventory of all software (to include manufacturer, type, and version and installation manuals and procedures) required to support the operation of the information system is maintained. Backup copies of the inventory are adequately protected. All system software is current and has current and complete documentation. There are information system diagrams and documentation on the setup of routers, switches, guards, firewalls and any other devices facilitating connections to other systems. The current configuration information is routinely validated for accuracy. For distributed information systems, there are software distribution implementation orders including effective date provided to all locations.

**CM-4.b CHANGE CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control changes to the information system.

Change control mechanisms maintain control of changes to hardware, software, and security mechanisms. Changes to information system specifications are prepared by the programmer and reviewed by a programming supervisor. System components are tested, documented, and approved (operating system, utility, applications) prior to promotion to production. Program changes are moved into production only upon documented approval from users and appropriate officials responsible for system development. Software changes are documented so that they can be traced from authorization to the final approved code. Documentation facilitates traceability of code to design specifications and functional requirements. Documentation is updated for software, hardware, operating personnel, and information system users when a new or modified information system is implemented. Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

*Change Request*

Software change request forms are used to document requests and related approvals. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document. Change requests are approved by appropriate organization officials including, but not limited to, information system users and information system support staff. Change control is effected by: (i) notifying users of the time and date of the last change in information content; (ii) ensuring that changes are executed only by authorized personnel; (iii) ensuring that intended the change is properly implemented; and (iv) providing a secure, unchangeable audit trail to clearly document the change.

*Emergency Changes*

Emergency changes for the information system are documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration are appropriately documented and approved and appropriate personnel are notified for analysis and follow-up.

**CM-6.b CHANGE ACCESS CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce access restrictions associated with change control.

Restrictions are in place for accessing information system software and for using and monitoring use of system software utilities. Responsibilities for using system utilities have been clearly defined and are understood by systems programmers. Responsibilities for monitoring use are defined and understood by organization officials. Application programmer privileges to change production systems (programs and data) are limited and are reviewed [*Assignment: time period (e.g., annually)*]. Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features. Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software. Justification and approval by appropriate organization officials for access to systems software is documented and retained. The use of privileged system software and utilities is reviewed by appropriate organization officials periodically every [*Assignment: time period (e.g., annually)*] to ensure that access permissions correspond with position descriptions and job duties.

**CM-7.b MONITORING CHANGE ACTIVITY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to monitor information system changes and actions by privileged users.

System programmers' activities are monitored and reviewed. The use of information system utilities is logged using access control software reports or job accounting information. All accesses to information system software files are logged by automated logging facilities. Installation of all information system software is logged to establish an audit trail/log and is reviewed by appropriate organization officials.

**CM-8.b MINIMAL SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure systems for only necessary capabilities.

The function and purpose of processes and services are documented and approved by appropriate organization officials. The information system is periodically reviewed to identify and eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls). Protocols that would introduce an unacceptable level of risk are disabled; specifically the following protocols are generally disabled [*Assignment: list of protocols.*]. Available processes/services are minimized, such as through: (i) installing only required services; and (ii) restricting the number of individuals with access to such services, based on the concept of least privilege. The information system that supports the server functionality is, as much as possible, dedicated to that purpose.

**CM-9.b SECURE CONFIGURATION SETTINGS, CHECKLISTS, AND BENCHMARKING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure and benchmark information technology products in accordance with good security practice settings.

Default settings of security features on the information technology products employed within the information system are set to the most restrictive mode compatible with system operational requirements. Vendor-supplied passwords for component products in the information system are changed. Information system initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. The operating system is configured to prevent circumvention of the security software and application controls. An organization reference document such as a security recommendation guide (SRG), security technical implementation guide (STIG), or security checklist constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products and all operational information system and hosted applications. If organization reference documents are not available, other

government guidelines or vendor literature are acceptable sources. When appropriate tools are available, configurations of information systems are benchmarked using automated scoring tools.

**CM-10.b NETWORK CONFIGURATION SETTINGS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure network parameters to reduce exposures.

Networks are appropriately configured to adequately protect access paths between information systems. Each information system boundary interface is configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited. Trust relationships among hosts and external entities are appropriately restricted to the minimum level necessary to accomplish mission tasks. Security attributes of each network service are clearly described.

**CM-11.b PRIVACY POLICY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to indicate user privacy is a priority within the organization.

Privacy policies in effect are posted on appropriate information systems (including web sites) within the organization.

**CM-12.b LIMITING TRAFFIC TYPES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure the information system to control specified types of traffic.

Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within organizational information systems. Both inbound and outbound public service instant messaging traffic is blocked at the information system boundary. [Note: This does not include instant messaging services that are configured by an authorized application or site to perform an authorized and official function.] Voice over Internet Protocol traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within organizational information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the information system boundary. [Note: This does not include Voice over Internet Protocol services that are configured by an authorized application or site to perform an authorized and official function.]

## OPERATIONAL CONTROLS

**FAMILY:** HARDWARE AND SOFTWARE MAINTENANCE (MA)

### MA-1.b PERIODIC MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct periodic on-site and off-site maintenance of the information system and of the physical plant within which this information system resides.

Comprehensive maintenance testing procedures exist that systematically schedule information system hardware for periodic maintenance inspections and testing to ensure the equipment operates within design specifications and is properly calibrated. Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations. Repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks) are documented. Regular and unscheduled hardware maintenance performed is documented. A maintenance log is maintained and includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort; and (iv) a description of the type of maintenance performed to include identification of replacement parts. Maintenance of information systems is performed on-site whenever possible. If information systems or system components are to be removed from the facility for repair, any component containing non-volatile memory is sanitized or appropriate\ cleared and its release is explicitly approved by an appropriate organization official. Maintenance changes that impact the security of the information system receive a configuration management review. After maintenance is performed on the information system, the security features are checked to assure that they are still functioning properly. Maintenance is performed in a manner that maintains security.

### MA-3.b REMOTE MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide additional controls on remotely executed maintenance.

Installation and use of remote diagnostic links are specifically addressed in the security plan and agreed to by the authorizing official. Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. The communications links connecting the components of the information system, associated information communications, and networks are protected in accordance with the FIPS Publication 199 security category of the information that may be transmitted over the link. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed. Unless an exception has been granted by an appropriate organization official, maintenance personnel accessing the information system at the remote site are cleared to the highest FIPS Publication 199 security category of information processed on that system, even if the system was downgraded/sanitized prior to remote access. An audit log is maintained of all remote maintenance, diagnostic, and service transactions including all commands performed and all responses. The log is periodically reviewed by an appropriate organization official. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as tokens; (iii) and remote disconnect verification. Where possible, remote sessions involve an interactive window for coordination with information security official responsible for the system being serviced. When the remote maintenance has been completed, all sessions are terminated and the remote connection is also terminated. Authenticators (e.g.,, passwords) used during remote maintenance are changed following each remote maintenance service.

**MA-4.b MAINTENANCE PERSONNEL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the authorization of an individual to perform maintenance.

The list of authorized maintenance personnel is documented. Only personnel authorized to do so perform maintenance on the information system. Except as authorized by the authorizing official, personnel who perform maintenance on the information system are authorized access to the highest FIPS Publication 199 security category of information processed on that system. Such personnel who perform maintenance or diagnostics on an information system do not require an escort, unless need-to-know controls must be enforced. However, a facility employee who is authorized to access the highest FIPS Publication 199 security category of information and, when possible, technically knowledgeable, is present within the area where the maintenance is being performed to assure that the proper security procedures are being followed. Foreign nationals (with proper authorizations) may be utilized as maintenance personnel for those information systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions are fully documented within a Memorandum of Agreement. A person not authorized access to the information system may be used to perform maintenance on the system provided an escort who is authorized access and is technically qualified monitors and records that person's activities in a maintenance log.

**MA-5.b TIMELY MAINTENANCE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that maintenance services and parts are available in a timely manner.

Spare or backup hardware is used to provide a high level of information system availability for organization applications. Maintenance support and critical maintenance spares and spare parts for [*Assignment: list of key information system assets*] can be obtained within [*Assignment: time period (e.g., twenty-four hours)*] of failure.

## OPERATIONAL CONTROLS

**FAMILY:** SYSTEM AND INFORMATION INTEGRITY (SI)

### SI-1.b FLAW REMEDIATION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate flaw remediation for the information system.

Significant weaknesses in the operational information system are reported and effective remedial actions are taken. This includes the following:

*Patch Management*

Systems affected by recently announced software vulnerabilities are identified. Patches are installed on a timely basis and tested for effectiveness and potential side effects on the organization's information systems. There is verification that patches, service packs, and hot fixes are appropriately installed on affected systems.

*System Software Problems*

A log is used to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.

*Malicious Code Screening*

As needed, incoming information is reviewed for viruses and other malicious code. Anti-viral mechanisms are used to detect and eradicate viruses transported by e-mail or attachments. The information system is automatically safeguarded from virus infections from other sources as well (e.g., central choke points where diskettes are scanned for viruses prior to distribution). There is timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

*Miscellaneous*

Software is up-to-date (latest versions of service packs, patches, and hot fixes are installed). Security weaknesses are being reported and acted upon. Software malfunctions are being reported and acted upon. Hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.

### SI-3.b PROCEDURAL REVIEW

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are periodically reviewed.

A review is conducted every [*Assignment: time period (e.g., twelve months)*] that comprehensively evaluates existing security policies and procedures to ensure procedural consistency and to ensure that they fully support the goal of enabling mission accomplishment. Access authorizations are periodically reviewed for incompatible functions. Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels.

### SI-4.b SOFTWARE AND INFORMATION INTEGRITY

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to both protect against and to detect unauthorized changes to software.

Integrity verification applications are available on the information system to look for evidence of information tampering, errors, and omissions. Tools for automatically monitoring the integrity of the information system and the applications it hosts are implemented. Good engineering practice with regard to commercial off-the-shelf integrity mechanisms, such as parity checks and cyclical redundancy checks are employed. The operating system's operational status and restart integrity is

protected during and after shutdowns. Mechanisms prohibit users from modifying the functional capabilities of boundary protection devices such as firewalls, gateways, and routers. There is limited write access to information system security capabilities (that is., the hardware, software, and firmware that perform operating system or security functions and the hardware, software, and firmware that must be relied upon in order for the system security functionality to operated correctly).

## OPERATIONAL CONTROLS

**FAMILY:** MEDIA PROTECTION (MP)

### MP-1.b MEDIA ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media.

Unauthorized individuals cannot read, copy, alter, or destroy information in printed form or on media removed from the information system. Media accountability and control mechanisms (e.g., audit trail logs), provide protection comparable to that for equivalent paper documents. Electronic media is controlled and protected in a manner similar to that used for paper materials. Output from the information system is given only to authorized users. Random or representative sampling techniques are used to verify the proper marking of large volumes of output. If available and approved, automated techniques are used to verify the proper output marking of information.

### MP-4.b MEDIA DESTRUCTION AND DISPOSAL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the destruction and disposal of media, both electronic and paper, to ensure that organizational information does not become available to unauthorized personnel.

Information system hardware and machine-readable media are cleared, sanitized, or destroyed before being reused or released outside of the organization. Retired, damaged, discarded, or unneeded information is disposed in a manner that prevents unauthorized persons from using it. Information is never disclosed during disposal unless authorized by statute. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category. Sanitized media is downgraded only with appropriate approval(s).

*Destruction of Paper Media*

Hard copy documents are destroyed when no longer needed. For information requiring such protection, destruction methods for organizational information in paper form are as follows: (i) burning - the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (ii) mulching or pulping - all material is reduced to particles one inch or smaller; (iii) shredding or disintegrating - paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative). Information storage media is destroyed in accordance with organization-approved methods. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

*Release of Systems and Components*

Equipment removal procedures for information systems and components that have processed or contained organizational information are followed. This includes inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.

### MP-6.b MEDIA-RELATED RECORDS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the maintenance of disposition records for media, both electronic and paper.

Audit trails are used for receipt of inputs/outputs from the information system. A record is kept of who implemented the media disposal actions and who verified that the information or media was properly sanitized. Inventory records of all storage media containing organizational information

are maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media are recorded in a log that identifies: (i) date received; (ii) reel/cartridge control number contents; (iii) number of records if available; (iv) movement; and (v) if disposed of, the date and method of destruction. Such a log permits all storage media containing organizational information (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged. Periodic inventories of removable storage devices and media containing organizational information are performed every [*Assignment: time period (e.g., semi-annually)*]. When removable storage devices and media containing organizational information are secured, a proper acknowledgement form is signed and returned to the originator. Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output. A record of the equipment release is created indicating the procedure used for sanitization, and to whom the equipment is intended. This record is retained for [*Assignment: time period (e.g., five years)*]. Logging of shipping and receipts and periodic reconciliation of these records is accomplished every [*Assignment: time period (e.g., monthly)*].

**MP-7.b MEDIA STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the secure storage of media, both electronic and paper.

Storage media are physically controlled and safeguarded in the manner prescribed for the highest security category (for confidentiality) of the information ever recorded on it until destroyed or sanitized using approved procedures. In those areas where organizational information is processed, unmarked media that are not in factory-sealed packages are protected at the highest FIPS Publication 199 security category (for confidentiality) for information processing conducted within the facility, until the media is reviewed and appropriately labeled. Records management for information stored in an information system or on external media are governed by the records management policies of the appropriate agency, based on the guidelines from the National Archives and Records Agency.

## OPERATIONAL CONTROLS

**FAMILY:** INCIDENT RESPONSE (IR)

### IR-1.b INCIDENT RESPONSE PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, enable effective response to incidents by developing an incident response plan when the organizational response plan is not adequate to address information system requirements.

An incident response plan consistent with NIST Special Publication 800-61 is developed for the information system that defines reportable incidents, outlines a standard operating procedure for incident response (to include actions to protect evidence in support of forensics), provides for user training, and establishes an incident response team. The incident response plan is tested at least [*Assignment: time period (e.g., semi-annually)*]. The test results are used to modify the incident response plan as necessary to ensure effectiveness.

### IR-2.b INCIDENT MONITORING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct ongoing monitoring of the information system for security events.

Information system-related security incidents are monitored and tracked until resolved. Information system performance monitoring is used to analyze performance logs in real time (or near-real time) to look for availability problems, including active attacks. Network activity logs for the information system are maintained and reviewed. Collected audit information is reviewed at least [*Assignment: time period that is at least weekly*]; taking advantage of audit reduction and analysis tools to effectively review information for unusual or suspicious activity or violations. Physical access to facilities is monitored and remedial actions taken, as appropriate.

### IR-3.b INCIDENT RESPONSE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to security incidents.

Reports of possible security violations and security incidents are accurate and timely. For security incidents, the organization defines appropriate parameters for response that includes: (i) what information employees must provide; (ii) whom they must notify; and (iii) what degree of urgency to place on reporting. Intrusion detection reports are routinely reviewed and suspected incidents handled accordingly. Records of information system activity, such as security incident tracking reports, are regularly reviewed. Security managers investigate security violations, security incidents, and suspicious activities (e.g., failed logon attempts, other failed access attempts; and questionable activity) and report results to appropriate organization officials. Incident information is reported to one or more of the following organizations: the Federal Computer Incident Response Center, the National Information Protection Center, the U.S. Department of Justice and state and local law enforcement agencies as required. Actions are taken to protect and avoid corrupting potential evidence in support of potential forensics.

In response to reported security violations and security incidents, appropriate actions (including disciplinary actions) are taken by organization officials. Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate. An effective malicious software protection and recovery process is implemented. Information system alerts/advisories are received on a regular basis. Alerts and advisories are issued to personnel and responded to, when appropriate. Incident information and common vulnerability and threat information are shared with owners of connected information systems.

**IR-4.b HELP DESK**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate incident response by providing a central incident support resource for information system users.

There is a help desk or group that offers advice to users of the information system and plays an appropriate role in the organization's incident response program.

**IR-5.b INTRUSION DETECTION SYSTEMS AND TOOLS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide attack detection capability for the information system.

An effective intrusion detection system (hardware, software, or firmware) is implemented, providing real-time identification of unauthorized use, misuse, and abuse of the information system. The intrusion detection system includes appropriate placement of intrusion detection sensors and definition of incident thresholds. Security controls on the information system can detect unauthorized access attempts. Auditable events (single events and the accumulation of events) that may indicate an imminent violation of security policies are routinely monitored. Selected information system components at critical control points (e.g., servers and firewalls) provide logs of network and system activity. Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain name servers. All significant events, including access to and modifications of information systems, are logged. Intrusion detection system logs contain appropriate information needed for effective review. Access to audit logs is adequately controlled. Virtual private network traffic is visible to network intrusion detection systems. Appropriate organization officials are notified in case of suspicious events. The organization [*Assignment: response (e.g., least disruptive action or a specific action*] to terminate the suspicious events.

**IR-6.b MALICIOUS CODE PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to identify and isolate suspected malicious software (e.g., viruses, worms, etc.).

The information system (including servers, workstations and mobile computing devices) implements malicious code protection that includes a capability for automatic updates. Virus definitions are up-to-date. Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network. Anti-viral mechanisms are used to detect and eradicate viruses in incoming and outgoing e-mail and attachments.

## OPERATIONAL CONTROLS

**FAMILY:** SECURITY AWARENESS AND TRAINING (AT)

### AT-1.b SECURITY AWARENESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment.

Each information system user is aware of the system security requirements and that user's security responsibilities prior to being authorized access to the system. Security awareness includes continual security awareness training conducted every [*Assignment: time period, typically annually*]. Users have received a copy of or have easy access to: (i) organizational security policies and procedures; and (ii) and rules of behavior for the information system or a user manual containing such rules. All employees fully understand their duties and responsibilities in accordance with their job descriptions as described in NIST Special Publications 800-16 and 800-50.

### AT-2.b SECURITY TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that all personnel with significant information system security responsibilities receive appropriate security training.

The organization identifies all positions and/or roles with significant information system security responsibilities. A security training program consistent with NIST Special Publications 800-16 and 800-50 provides training for individuals within the organization with specific information system security responsibilities. Security training is adjusted to the level of the employee's responsibilities. Employees receive adequate training and have the needed security expertise and skills identified in job descriptions. The employees acknowledge, in writing, having received the security and awareness training. A record of the security subjects covered during training is maintained. Employee training and professional development are documented and monitored. Skill needs are accurately identified and included in job descriptions.

## TECHNICAL CONTROLS

**FAMILY:** IDENTIFICATION AND AUTHENTICATION (IA)

### IA-1.b INDIVIDUAL IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable reliable identification of individual users of the information system.

Identification and authentication mechanisms are implemented that include provisions for uniquely identifying and authenticating entities (i.e., users or information system processes acting on behalf of users). Information system access is gained through the presentation of an individual-identifier (e.g., a unique token or user login ID) and authenticator(s). Any user actions that can be performed prior to reliable identification are explicitly identified (e.g., reading a publicly available web site).

### IA-3.b PASSWORD PROTECTION MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect passwords from unauthorized disclosure or modification.

For information systems employing password-based authentication, passwords are: (i) one-way encrypted for storage; (ii) transmitted on the network in a secure manner (e.g., encrypted); (iii) not displayed when entered; and (iv) controlled by the associated user. When cryptographic functions are needed, FIPS-140-2 validated cryptography is used.

### IA-4.b PASSWORD LIFE

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords are changed and not reused.

Mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. Passwords are changed at least [*Assignment: time period; typically sixty-ninety days*]. Passwords have a minimum life of [*Assignment: time period (e.g., one day)*]. Passwords are prohibited from reuse for a specified period of [*Assignment: number of generations; typically six*].

### IA-5.b PASSWORD CONTENT

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords comply with policy requirements for content and length.

Mechanisms are implemented to ensure that passwords: (i) contain characters from [*Selection: uppercase alphabetic, lowercase alphabetic, numeric, special characters; typically all four are selected*] with [*Assignment: requirements for how many of the selected types of characters must be included, typically three*]; (ii) have a minimum length of [*Assignment: value, minimum of eight characters*]; (iii) are not the same as the user ID; (iv) are not names or words; (v) are unique for specific individuals; and (vi) are not generic user IDs or passwords.

### IA-6.b PASSWORD-BASED ELECTRONIC SIGNATURES

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure appropriate use of password-based, electronic signatures. (*Related to IA-10 Digital Signatures*)

Password is entered solely for the purpose of indicating intent to sign, is known only by the password owner, and is not exposed to offline attacks by an eavesdropper. The user is advised that use of the password will be construed as a binding legal signature and applications make clear the significance of the act of signing with each signature. Passwords are registered to each user by a secure process that provides clear assurance that the password is associated with the correct individual.

**IA-11.b AUTOMATIC INFORMATION SYSTEM IDENTIFICATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable identification of the information system being used or to which a connection is being made.

Automatic information system identification is used to authenticate connections to specific locations and portable information system hardware.

**IA-13.b UNSUCCESSFUL LOGIN ATTEMPTS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to take defined action in the face of multiple unsuccessful login attempts.

For a given user, there is a limit of [*Assignment: number, typically three*] invalid information system access attempts that may occur over [*Assignment: time period (e.g., fifteen minutes)*]. When the maximum number of unsuccessful attempts is exceeded, the information system automatically [*Selection: locks the account/node until released by an administrator, locks the account/node for an* [*Assignment: time period (e.g., fifteen minutes)*], *delays next login prompt according to* [*Assignment: delay algorithm (e.g., the standard Unix algorithm that accomplishes successively longer delays with each subsequent failure)*]].

**IA-14.b IDENTIFIER MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user identifiers.

Users of the information system are appropriately identified. Identification is unique to each user. Registration to receive a user identification (ID) is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the user ID is issued to the intended party. Inactive user Ids are disabled after [*Assignment: time period, for example, one year*].

**IA-15.b AUTHENTICATOR MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user authenticators.

*Public Key Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor, and is done in person before a designated registration authority. Secure procedures ensure that the certificate is issued to the correct, identified party.

*Authenticator Selection, Content, Defaults and Protection*

Selection of passwords or other authentication devices (e.g., tokens, biometrics) is appropriate, based on FIPS Publication 199 security category of the information system. Initial authenticator content and administrative procedures for initial authenticator distribution are defined. Lost or compromised authenticators are addressed. Default authenticators are changed upon information system installation. Authenticators are protected to preserve confidentiality and integrity. Users

maintain possession of their individual tokens, key cards, etc., do not loan or share these items with others, and report lost items immediately.

**IA-16.b PASSWORD MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that passwords meet specified requirements.

*Organization-issued Passwords*

Registration to receive a password is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the password is issued to the intended party. Users are instructed as to the proper methods of protecting their passwords.

*Organization-issued and User-determined Passwords*

For information systems employing password-based authentication, passwords are: (i) distributed securely; (ii) controlled by the assigned user and not subject to disclosure; (iii) prohibited from being embedded in programs; (iv) changed periodically every [*Assignment: time period, typically ninety days*]; (v) contain alphanumeric and special characters and are composed of representatives of at least three of the following character sets: upper case English, lower case English, numeric characters, and special characters (information systems with limited information input capabilities implement these measures to the extent possible.); (vi) have a minimum length of [*Assignment: value, minimum of eight characters*]; (vii) prohibited from reuse for a specified period of [*Assignment: number of generations, typically six*]; (viii) have an appropriate minimum life of [*Assignment: length of time, typically one day*]; (ix) not the same as the user ID; and (x) not names or words.

## TECHNICAL CONTROLS

**FAMILY:** LOGICAL ACCESS CONTROL (AC)

### AC-1.b REMOTE ACCESS RESTRICTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide access protections for remote connections.

There are controls that restrict remote access to the information system.

*Protection of Remote Access - General*

Remote access to organizational information systems always uses encryption to protect the confidentiality of the session. All remote access is mediated through a managed access control point. Information regarding remote access mechanisms (e.g., dial-up connection telephone numbers) is protected.

*Remote Access for Privileged Functions*

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to general security measures for remote access, additional protections such as a virtual private network with blocking mode enabled are implemented.

*Collaborative Computing*

Collaborative computing mechanisms are not remotely activated. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop is required to take an explicit action to turn on the camera and microphone, remote users are not allowed to activate a user's camera or microphone remotely). Peer-to-peer collaborative computing mechanisms between information systems ensure that only the information on the screen is observable to the remote user. Information located elsewhere on the workstation is not observable. The remote user is not able to modify or delete any information on the workstation. These restrictions also apply to any other information system to which the user's workstation is logically connected (e.g., any logically mounted disks). Collaborative computing mechanisms that provide video and/or audio conference capabilities provide some explicit indication that the video and audio mechanisms are operating.

*Public Access Information Systems*

For public access information systems, there are mechanisms implemented to protect the integrity of the information, the application, and the underlying system. These controls are resilient in the face of publicly known attacks.

*Dial-In Access to Information Systems*

Dial-in access to the information system is controlled and monitored. Mechanisms are implemented to limit the access achieved through dial-up, in accordance with organizational policy.

*Remote Terminal Access*

Where enforcement of information system security policy requires, mechanisms are implemented to restrict access through specific workstations or terminals.

### AC-2.b LOGON NOTIFICATION MESSAGE

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide users with information about previous logons both successful and unsuccessful.

Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user's last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon. A warning/notification message is displayed upon successful logon and before gaining system access. This message: (i) is approved and standardized; (ii) remains on the screen until explicit user action to remove it; (iii) warns all users that they have accessed a U.S.

Government information system; (iv) provides appropriate privacy and security notices; (v) notifies the user that system usage may be monitored, recorded, and subject to audit; and (vi) notifies the user that use of the information system indicates (a) the consent of the user to such monitoring and recording and (b) that unauthorized use is prohibited and subject to criminal and civil penalties.

**AC-4.b SESSION LOCK**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable user-commanded locking of the information system session.

Session-lock functionality is associated with each information system node (e.g., terminal, workstation, notebook computer). Upon user activation, a session-lock function prevents access to the node or to any session information. Once the session-lock is activated, access to the node requires knowledge of a unique authenticator. Session-lock is not a substitute for logging out.

**AC-5.b SESSION INACTIVITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable enforcement of defined actions in the event of session inactivity.

The information system detects [*Assignment: time period (e.g., fifteen minutes)*] of inactivity and blocks further access until the user reestablishes the connection using the proper identification and authentication procedures.

**AC-8.b AUTHORIZATION MANAGEMENT MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective assignment and management of access authorizations.

Authorization management mechanisms are implemented that effectively support the following access control capabilities: (i) [*Selection: one or more types of access control: role-based, identity-based*]; and (ii) [*Selection: one or more types of access control: discretionary, non-discretionary*]. Whenever the information system provides for disclosure of information deemed critical/sensitive by the organization (in accordance with FIPS Publication 199), an authorization mechanism is employed to query and receive consent for the disclosure of such information. The information system provides the capability for users (or processes acting on behalf of users) to determine the access authorizations granted to another user or to a communications channel.

**AC-9.b ENFORCEMENT MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce the assigned authorizations for access to information or the information system and for controlling the flow of information.

Information system access enforcement mechanisms (capable of including or excluding access to the granularity of a single user or user-role) enforce the assigned resource authorizations for each attempted access to information or information system. Information flow control enforcement mechanisms provide the granularity of information description and of source and destination description to adequately implement organizational policy.

*For discretionary access control enforcement*

Access is controlled between named users (or processes) and named objects (e.g., files and programs) in the information system. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest, encryption) allow users to specify and control sharing

of those objects by named individuals, or by defined groups of individuals, or by both, and provide controls to limit propagation of access rights. The enforcement mechanisms, either by explicit user action or by default, protect objects from unauthorized access. These access controls are capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission is only assigned by authorized users.

*For non-discretionary access control enforcement*

A non-discretionary access control policy is enforced over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects are assigned labels (implicitly or explicitly) that combine hierarchical levels and non-hierarchical categories; the labels are used as the basis for non-discretionary access control decisions.

*For flow control enforcement*

A flow control policy is enforced over information flows under its control. Information and source and destination objects may be assigned labels (implicitly or explicitly) that are used as the basis for non-discretionary flow control decisions. Additionally, flow control rules (e.g.,, router rules) may be used to enforce information flow policy both discretionary and non-discretionary.

**AC-10.b AUTOMATED ACCOUNT CONTROLS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to manage inactive and special accounts.

Emergency or temporary accounts are automatically terminated after [*Assignment: time period (e.g., thirty days)*]. Inactive accounts are automatically disabled after [*Assignment: time period (e.g., six months)*].

**AC-11.b LEAST PRIVILEGE AND SEPARATION OF DUTIES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to separate duties among individuals within the organization and limit authorizations to the minimum necessary to fulfill assigned duties.

*Least Privilege*

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

*Separation of Duties*

The principle of separation of duties is enforced. Mission functions and distinct information system support functions are divided among different individuals and are performed by different individuals. Access authorizations are periodically reviewed for functions that should be separated to enhance security. Duties that should be separated to enhance security have been identified (e.g., security personnel who administer access control functions should not be those who administer the audit functions on the information system). Information system support functions are performed by different individuals (e.g., functions such system management, system design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, network security, database administration, network administration). As necessary to enhance security, mission-processing functions are distributed among different individuals. Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

**AC-12.b SUPERVISION AND REVIEW — ACCESS CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to supervise personnel and review their actions with respect to enforcement of access controls.

Personnel (those enforcing controls and those who the controls are restricting) are provided adequate supervision and review, including each shift for computer operations. Supervisors routinely review user activity logs for inappropriate actions and investigate any abnormalities. Changes to security access authorizations are logged and periodically reviewed by appropriate organization officials independent of the security function. Unusual activity is investigated.

**AC-13.b NON-DISCRETIONARY ACCESS CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enable enforcement of non-discretionary access requirements.

Non-discretionary access requirements are identified and appropriate authorizations implemented to enable the enforcement of these access requirements. Examples of non-discretionary requirements are: (i) limitations on release of private information; (ii) limitations on release of export-controlled information; and (iii) limitations on public release of information.

**AC-14.b AUTHORIZATION PROCEDURES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system authorizations.

Rules are in place for: (i) granting of access authorizations; (ii) determining initial rights of access to a terminal, transaction, program, process, or information; and (iii) determining the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process or information.

*Granting of Access Rights*

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict assess that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

*Review of Access Rights*

Information system owners periodically review access authorizations for continuing appropriateness. Security managers review access authorizations and discuss any questionable authorizations with information system owners. Access to the information system is authorized only to individuals who: (i) have a valid need-to-know that is demonstrated by assigned official duties and satisfying of all personnel security criteria; or (ii) are otherwise to be granted access based upon intended system usage (e.g., a publicly accessible web site).

*Authorization Definitions*

Authorizations are defined and managed for: (i) mission-specific processing; (ii) program source library; (iii) system resources; (iv) support/technology management systems and/or tools; (v) system libraries; (vi) access to passwords/authentication services and directories; (vii) access authorizations for maintainers of information system resources, including those that are at remote locations; (viii) users who can dial into the information system from remote locations; and (ix) default permissions and rights.

*Miscellaneous*

Standardized naming conventions are used for information system components. Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, scratch, and rename a file. Employees are discouraged from browsing files by making it clear that organizational policy prohibits it. Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.

**AC-15.b SYSTEM ACCOUNT MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system accounts.

Comprehensive account management ensures that only authorized users can gain access to information systems. Account management includes: (i) identifying types of accounts (individual and group, conditions for group membership, associated privileges); (ii) establishing an account (i.e., required identification, approval, and documentation procedures); (iii) activating an account; (iv) modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators); and (v) terminating an account.

*All Accounts*

Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain information system access. The account manager is notified in a timely manner when information system users are terminated or transferred. Unnecessary accounts (defaults, guest accounts) are removed, disabled, or otherwise secured. Inactive accounts and accounts for terminated individuals are disabled or removed on a timely basis.

*Guest and Anonymous Accounts*

Guest and anonymous accounts on the information system are specifically authorized and monitored. Emergency or temporary accounts are appropriately controlled, including: (i) documented, approved by appropriate organization officials; (ii) securely communicated to the appropriate personnel; and (iii) automatically terminated after a predetermined period with a default of [*Assignment: time period (e.g., thirty days)*].

## TECHNICAL CONTROLS

**FAMILY:** ACCOUNTABILITY (INCLUDING AUDIT TRAILS) (AU)

### AU-1.b USER ASSOCIATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the association of an individual user with the actions taken by that user.

Mechanisms are implemented to associate actions taken or attempted in the information system with the specific user responsible for that action.

### AU-2.b CONTENT OF AUDIT RECORDS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to include specified information in audit records.

The audit trail includes sufficient information to establish what events occurred and who or what caused the events. For each security-relevant auditable event (as specified in AU-3), the audit record contains at least the following information: (i) date and time of the event; (ii) information system locale of the event; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

*For Information Release Actions*

Include: (i) identity of releaser; (ii) identity of recipient; (iii) identity of information released; (iv) device identifier (id) (e.g., port ID); (v) time and date of release; and (vi) modification or application of security labels.

*For Information Communications Actions*

Include: (i) identity of sender (e.g., person, information system); (ii) identity of recipient (e.g., IP address, host and user); device ID (e.g., port ID); and (iii) time and date of communication.

The following additional audit information is provided: [*Assignment: list of other information that the information system is able to include in the audit records*].

### AU-3.b AUDITABLE EVENTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to generate an audit record for at least a defined set of events.

The information system audit mechanisms are capable of generating an audit record for each of the following events: (i) start-up and shutdown of the audit functions; (ii) successful and unsuccessful logons and logoffs; (iii) successful and unsuccessful attempts to access security relevant files and utilities including user authentication information; (iv) operations performed to read, modify or destroy the audit information; (v) modifications to the audit configuration that occur while the audit functions are operating; (vi) actions taken due to exceeding of a threshold or audit storage failure; (vii) unsuccessful use of the user identification or authentication mechanisms including the identity provided; (viii) unsuccessful revocations of security attributes; (ix) modifications to the group of users that are part of a role; (x) key recovery requests and associated responses including who made the request and when; (xi) changes to the time; (xii) denial of access resulting from an excessive number of logon attempts; (xiii) blocking or blacklisting a user ID, terminal, or access port and the reason for the action; (xiv) detected replay attacks; (xv) rejections of new sessions based upon any limitation on the number of concurrent sessions; (xvi) other activities that modify, bypass, or negate security controls within the information system; (xvii) use of compilers, and (xviii) use of privileged accounts.

All accesses to information system software files are logged by automated logging facilities. Installation of all system software is logged to establish an audit trail/log and is reviewed by management. The use of system utilities is logged using access control software reports or job accounting information. Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users are logged.

*Mission-specific Processing Activity*

For example: (i) all transactions are logged as entered, along with the user ID of the individual entering the information; and (ii) overriding or bypassing information validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

*Non-discretionary Access Control Events*

For example: (i) attempts to cause information flows contrary to policy; (ii) changes to user formal access permissions; (iii) changes in security labels; (iv) accesses or attempted accesses to objects or information whose labels are inconsistent with user privileges; (v) information downgrades and overrides; and (vi) identified events that may be used in the exploitation of covert channels.

The following additional events generate an audit record: [*Assignment: list of additional events*].

**AU-4.b AUDIT PROCESSING**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable meeting specified requirements for the audit system.

Information system clocks are synchronized for accurate reading of auditable events. In the event of an audit failure or full audit trail, [*Assignment: action to be taken (e.g., shutdown information system, overwrite oldest audit records, or stop generating audit records)*]. Online audit information from the information system is protected against unauthorized access, modification or deletion. Access to information system audit tools is protected to prevent possible misuse or compromise.

**AU-5.b AUDIT REDUCTION AND REPORT GENERATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective human review of audit information and the generation of appropriate audit reports.

Tools are available for the review of audit records and for report generation from audit records. Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents.

**AU-6.b NON-REPUDIATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against later claims by sender to not have transmitted a message or a receiver to not have received a message.

Mechanisms are implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

## TECHNICAL CONTROLS

**FAMILY:** SYSTEM AND COMMUNICATIONS PROTECTION (SP)

### SP-1.b APPLICATION PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to isolate user interfaces from information system management functionality.

User interface services (e.g., web services) are physically or logically separated from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

### SP-2.b INFORMATION SYSTEM PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to separate security-relevant functionality from other information system functionality.

Information system security functions are isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system maintains a separate execution domain (e.g., address space) for each executing process.

### SP-3.b INFORMATION REMNANTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against unauthorized information transfer via shared information system resources.

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) is available to any current user (or current process) that obtains access to a shared system resource that has been released back to the information system. There is no residual information from the shared resource.

### SP-4.b DENIAL OF SERVICE PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to specifically protect against denial of service attacks.

Mechanisms are in place to curtail or prevent well known, detectable, and preventable denial of service attacks. The attacks to be prevented are [*Assignment: list of attacks or pointer to source for current list*].

### SP-5.b RESOURCE PRIORITY

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to limit use of information system resources by priority and by quota.

Mechanisms are implemented to provide for allocation of information system resources based upon priority and upon a quota. Mechanisms are implemented to enforce the information system resource allocations as appropriate for meeting system security needs.. Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

**SP-6.b BOUNDARY PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to proxy, screen, or filter communications at the authorization boundary of the information system.

*Boundary Protection Devices*

Protection mechanisms are implemented at the information system boundary and at layered or internal system boundaries, including, as appropriate, firewalls, gateways, proxies, routers and network intrusion detection systems.

*Protection Capabilities*

Controlled Release: Only traffic that is explicitly permitted (based on traffic review) is released from the boundary of the interconnected information system.

Encryption: Outgoing communication (including the body and attachment of the communication) are encrypted using FIPS 140-2 validated cryptography, as needed, with the appropriate level of encryption for the information, transmission medium, and destination information system.

Fail-secure: The operational failure of the boundary protection for the information system does not result in any unauthorized release of information outside of the system boundary. In the event of an operational failure of the boundary protection, no information external to the interconnected information system enters the information system.

The boundary protection of the information system is at least as strong as the boundary protection of the information system into which the information flows are directed.

Delivery: Incoming communications have an authorized user (and, as applicable, authorized addresses) as a destination.

Filtering: Communications protocols/services from outside the boundary of the interconnected information system are supported and filtered as appropriate to comply with security policy (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications).

Proxies: Protocol-mediation software (i.e., proxies) that is able to understand and take protective action based on application-level protocols and associated data streams (e.g., filtering FTP connections to deny the use of the *put* command, effectively prohibiting the ability to write to an anonymous FTP server) are supported by the information system, as appropriate.

Extensibility: Security support for the incorporation of additional system services (as they become available) is provided, where appropriate.

Platform Protection Requirements: The platform underlying the boundary protection mechanisms must be able to isolate and protect the boundary protection applications.

Information system nodes (e.g., workstations, notebook computers) with dial-up access generate a unique identifier code before connection to the information system is completed.

Non-discretionary policy enforcement: Required capability to implement policy when policy restricts information flows between information systems connected by the boundary protection device(s) and either of the systems is not considered trustworthy enough to maintain only allowed flows.

*Alternate Processing Site*

Information system boundary protections at the designated alternate site provide the same levels of protection as that of the primary site.

**SP-7.b NETWORK SEGREGATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable segregation of functionality and communications.

Information system boundary hosts are appropriately isolated through controls such as segregation from the internal network. External servers are located external to a site's boundary protection (e.g., firewall) or are on a network separate from the site's intranet. All Internet access is through Internet access points that are under the management and control of the information system owner or organization and meets the organizational requirement that such contacts are isolated from other organization information systems by physical or technical means. Any connection to the Internet, or other external networks or information systems, occurs through a proxy, gateway, or firewall. Public wide area network connections between the organizational information systems and the Internet or other public or commercial wide area networks require an information protection network (IPN) that acts as the single point of entry into the site and defends the information system boundary or external connection(s).

**SP-13.b CRYPTOGRAPHIC KEY MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage cryptographic keys.

When encryption is used, documented procedures are being effectively implemented for key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect organizational information are generated in FIPS Publication 140-2 validated cryptographic modules and controlled and distributed using NIST-approved key management guidance. 128, 192, or 256-bit Advanced Encryption Standard (AES) encryption is used, with key agreement or key transport corresponding to the strength of the asymmetric key algorithms (See NIST key management guidance). Asymmetric keys are produced, controlled and distributed using an organization certificate authority (CA) cross-certified with the Federal Bridge CA at a level of medium or high or pre-placed keying material.

**SP-14.b KEY ARCHIVE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to archive keying material for encrypted information.

Keying material needed to recover encrypted stored information is archived in the custody of a designated key recovery custodian and is stored securely. Keys are stored so that an intruder who steals the encrypted information does not obtain the keying material needed to decrypt the information.

**SP-15.b PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance the effectiveness of public key infrastructure.

All public key certificates used in the information system are issued in accordance with a defined certificate policy and certification practice statement.

*Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

**SP-16.b USE OF ENCRYPTION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that when encryption is used, Federal policy requirements are met, to include use of FIPS Publication 140-2 validated cryptography.

*Information at Rest (Encryption for confidentiality)*

When information on the information system is encrypted for confidentiality during storage, it is encrypted with FIPS Publication 140-2 validated cryptography.

*Information in Transit (Encryption for Confidentiality)*

Organizational information that is transmitted through a commercial or wireless network and kept confidential via encryption is encrypted using 128, 192, or 256-bit Advanced Encryption Standard (AES) implemented in FIPS Publication 140-2-validated cryptographic modules.

*Information in Transit (Encryption for Need-To-Know)*

Information in transit through a network at the same FIPS Publication 199 security category (for confidentiality), but which is kept separate for need-to-know reasons via encryption, is encrypted with FIPS Publication 140-2 validated cryptography.

*Non-repudiation*

FIPS Publication 140-2 validated cryptography (e.g., DOD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS Publication 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards are applied as they become available.

## APPENDIX G

# BASELINE SECURITY CONTROLS – MODERATE

FIPS PUBLICATION 199 SECURITY CATEGORIZATION—MODERATE IMPACT

The minimum security controls listed in this baseline (which were extracted from the Catalog of Security Controls in Appendix J) are a recommended starting point for agencies in assessing the actual security controls that may be necessary to protect their information systems. The baseline is associated with the initial security categorization of the information system in accordance with FIPS Publication 199 and provides an estimated threat coverage described in the tables in Appendix E. Organizations should employ risk assessments during the system development life cycle to tailor the security controls in the baseline, as appropriate. The final agreed upon set of security controls should be documented in the security plan providing a justification and rationale for any adjustments to the initial baseline.

The baseline security controls in this Appendix consist of two key components: (i) a *control objective* section; and (ii) a *control description* section. The control objective section provides the overall objective for the particular security control when applied to an information system. The control description section provides the specific control requirements and details of each control. The security controls in the baseline are selected from the catalog in Appendix J and represent a subset of the controls in the catalog. Therefore, the numbering of the controls in the baseline may not always be consecutive.

The security controls are hierarchically constructed and build upon one another. For example, the enhanced version of a security control includes the original requirements from the basic version of the control (indicated by non-bolded text) and includes additional or supplemental requirements (indicated by bolded text).



## Table of Contents – Moderate Baseline

## MANAGEMENT CONTROLS

**FAMILY:** RISK ASSESSMENT (RA)

### RA-1.e SECURITY CATEGORIZATION

CONTROL OBJECTIVE: The potential impact on organizational operations and assets resulting from the operation of the information system is identified.

The information system is categorized in accordance with FIPS Publication 199 and NIST Special Publication 800-60. The security categorization is explicitly documented and approved by an appropriate senior official. **Categorization is based upon an analysis with documented summary that explains the rationale for the categorization selected.**

### RA-2.e RISK ASSESSMENT

CONTROL OBJECTIVE: Risks to organizational operations and assets resulting from the operation of the information system are identified.

An assessment of risk to organizational operations and assets due to the operation of the information system is performed and documented on an [*Assignment: time period which is at least annually*] and whenever there are significant changes to the system, facilities, or other conditions that may impact the security or authorization status of the system. The risk assessment (either formal or informal) is consistent with the intent of NIST Special Publication 800-30. The documented risk assessment includes the following: (i) identification of the conditions for reassessment, indicating the period for periodic reassessment and defining the level of change to the information system or environment that will cause a reassessment to occur; (ii) identification of the security authorization boundary; (iii) the current information system configuration including connections to other systems; (iv) actions that will be taken to ensure that the boundary definition is accurately updated periodically; (v) an inventory of information system assets; (vi) identification and assessment of threat sources; (vii) identification and assessment of information system vulnerabilities; and (viii) identification of risks from third party connections. **Sufficient information is documented by the organization to explain the rationale for the risk assessment results.**

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY PLANNING (PL)

### PL-1.b RULES OF BEHAVIOR AND ACCEPTABLE USE

CONTROL OBJECTIVE: Establish information system policy for rules of behavior and acceptable use when organizational policy is not adequate to address system needs.

A set of rules that describes the security operations of the information system and clearly delineates security responsibilities and expected behavior of all system owners, users, operators, and administrators is in place. Rules include the consequences of inconsistent behavior or non-compliance. Rules include all significant aspects of information system use, including policy on use of electronic mail. Signed acknowledgement of the rules is a condition of access.

### PL-2.b ACCESS CONTROL POLICY

CONTROL OBJECTIVE: Establish an information system policy for access control when organizational policy is not adequate to address system needs.

An explicit, documented access control policy establishes the rules to be implemented to ensure that only designated individuals, under specified conditions (e.g., time of day, port of entry, type of authentication, etc.) can: (i) access the information system (i.e., logon, establish connection); (ii) activate specific system commands; (iii) execute specific programs and procedures; and (iv) create, view, or modify specific objects (programs, information, system parameters). The policy has provisions for periodic review of access authorizations. This policy covers both discretionary and non-discretionary controls. Discretionary controls are those controls established at the discretion of the information owner, usually with constraints called out in the policy. Non-discretionary controls (e.g., restrictions on the viewing of export-controlled information or personal medical information), are those controls established by organizational policy and not subject to determination by the owner of the information.

### PL-3.b GROUP IDENTIFICATION AND AUTHENTICATION POLICY

CONTROL OBJECTIVE: Establish information system policy for group identifiers and the use of those identifiers when organizational policy is not adequate to address system needs.

An explicit, documented group identification and authentication policy establishes the rules to be implemented to ensure that group authenticators are used for information system access only when explicitly authorized and in conjunction with other authenticators as appropriate.

### PL-4.b INFORMATION FLOW CONTROL POLICY

CONTROL OBJECTIVE: Establish information system policy for information flow control when organizational policy is not adequate to address system needs.

An explicit, documented information flow control policy establishes the rules to be implemented to ensure that information is allowed to flow within the information system and across system boundaries only as authorized. This policy covers both discretionary and non-discretionary controls. Discretionary controls are those controls established at the discretion of the information owner, usually with constraints called out in the policy. Non-discretionary controls (e.g., restrictions on the viewing of export-controlled information or personal medical information), are those controls established by organizational policy and not subject to determination by the owner of the information.

### PL-5.b ACCOUNTABILITY POLICY

CONTROL OBJECTIVE: Establish information system policy for accountability when organizational policy is not adequate to address system needs.

An explicit, documented accountability policy establishes the rules to be implemented to ensure that information system users can be held accountable for their actions as needed. Accountability policy elements are, for example: (i) purposes for accountability (e.g., deterrent, incident forensics, etc.); (ii) required granularity for accountability (e.g., to the granularity of individual users); and (iii) time period for which accountability information must be available (e.g., five years).

**PL-6.b CONTINGENCY PLANNING AND OPERATIONS POLICY**

CONTROL OBJECTIVE: Establish information system policy for contingency operations when organizational policy is not adequate to address system needs.

An explicit, documented contingency planning and operations policy addresses all critical aspects of contingency planning consistent with NIST Special Publication 800-34.

**PL-7.b CONFIGURATION MANAGEMENT POLICY**

CONTROL OBJECTIVE: Establish information system policy for configuration management and control of hardware, software and firmware assets when organizational policy is not adequate to address system needs.

An explicit, documented configuration management policy establishes the rules to be implemented to ensure that organization's track and control the hardware, software, and firmware components that comprise the information system.

**PL-8.b INCIDENT RESPONSE POLICY**

CONTROL OBJECTIVE: Establish information system policy for monitoring and responding to incidents when organizational policy is not adequate to address system needs.

An explicit, documented incident response policy addresses all critical aspects of incident handling and response consistent with NIST Special Publication 800-61.

**PL-9.b SECURITY TRAINING AND AWARENESS POLICY**

CONTROL OBJECTIVE: Establish information system policy for security training and awareness when organizational policy is not adequate to address system needs.

An explicit, documented security training and awareness policy addresses all critical aspects of security training and awareness consistent with NIST Special Publications 800-16 and 800-50.

**PL-10.b PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for physical and environmental protection when organizational policy is not adequate to address system needs.

An explicit, documented physical and environmental protection policy addresses all critical aspects of physical and environmental protection consistent with General Services Administration policies, directives, regulations, and guidelines.

**PL-11.b PERSONNEL SECURITY POLICY**

CONTROL OBJECTIVE: Establish information system policy for personnel security when organizational policy is not adequate to address system needs.

An explicit, documented personnel security policy addresses all critical aspects of personnel security consistent with Office of Personnel Management policies, directives, regulations, and guidelines.

**PL-12.b MEDIA PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for media protection when organizational policy is not adequate to address system needs.

An explicit, documented media protection policy addresses all critical aspects of media protection to include: (i) media access; (ii) media labeling; (iii) media transport; (iv) media destruction and disposal; (v) media sanitization and clearing; (vi) media storage; and (vii) disposition of media records.

**PL-13.b SYSTEM MAINTENANCE POLICY**

CONTROL OBJECTIVE: Establish information system policy for information system hardware and software maintenance when organizational policy is not adequate to address system needs.

An explicit, documented information system maintenance policy addresses all critical aspects of hardware and software maintenance to include: (i) scheduling of periodic maintenance; (ii) maintenance tools; (iii) remote maintenance; (iv) maintenance personnel; and (v) timeliness of maintenance.

**PL-14.e SECURITY PLANNING**

CONTROL OBJECTIVE: In accordance with organizational policy, facilitate achieving adequate security by documenting and approving a security plan for the information system.

The content of the security plan is compliant with OMB policy and consistent with the intent of NIST Special Publication 800-18. The security plan is approved by appropriate organization officials and incorporated into the information resources management strategic plan. The security plan is reviewed and updated as needed to reflect current conditions, both on a regular basis every [*Assignment: time period*] and whenever there are significant changes defined as [*Assignment: criteria for significant changes*] to the information system, facilities, or other conditions that may impact security. **Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.**

**PL-15.b STANDARDS FOR SECURITY TEST AND EVALUATION PLANS**

CONTROL OBJECTIVE: Facilitate effective testing and evaluation of the security controls in the information system by developing standards for security test and evaluation plans when organizational standards are not adequate to address system needs.

Test plan standards have been developed and are followed for all levels of testing that define: (i) responsibilities for each party (e.g., users, system analysts, programmers, evaluators, auditors, quality assurance, and library control); (ii) test development requirements; (iii) test coverage requirements; and (iv) test plan, procedures, and report documentation requirements.

## MANAGEMENT CONTROLS

**FAMILY:** SYSTEM AND SERVICES ACQUISITION (SA)

### SA-1.e ACQUISITION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the risk of acquiring ineffective security capabilities by meeting specified requirements.

A discrete line item for information security (or information assurance) is established in programming and budget documentation.

*Solicitation Documents*

The solicitation documents for the information system (e.g., Requests for Proposals), include security controls and security test and evaluation procedures. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

*Information System Specifications*

For all new information systems and major upgrades to existing systems, there are detailed system specifications prepared and reviewed by management. An organization reference document such as a security recommendation guide (SRG) or a security technical implementation guide (STIG) constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products. If organization reference documents are not available, other government guidelines or vendor literature are acceptable sources. Advice from information security specialists is used in the development of requirements, acquisition documentation, and source selection. Appropriate security controls for the information system and associated security test and evaluation procedures are developed as part of the procurement action. Additionally, a clear description is provided of the security attributes of each network service.

*Vendor or Developer Expectations*

For acquired and developed information systems, identify, as early in the life cycle as possible, the network ports, protocols, and services to be used. Design reviews are conducted on the information systems and security test and evaluation is conducted prior to placing the systems into operation. Test results for the developmental information systems are documented. Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. Vendor supplied system software is supported by the vendor.

*Use of Evaluated and Validated Products*

For acquisition of security and security-enabled commercial off-the-shelf (COTS) information technology products, when multiple products meet organizational requirements, preference is given to products that have been evaluated and validated through one or more of the following sources: (i) the NIAP Common Criteria Evaluation and Validation Scheme; (ii) the International Common Criteria Recognition Arrangement; and/or (iii) the NIST Cryptographic Module Validation Program.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### SA-2.e COPYRIGHTED AND PUBLIC DOMAIN WORKS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to comply with software license restrictions and to ensure appropriate use of software and capabilities such as peer-to-peer file trading networks.

The use of copyrighted software or shareware and personally owned software is controlled and documented. Open source software use is permitted but the software is assessed to determine its

security impact prior to use. Public domain software products (excluding open source software products) are not used in organization information systems unless compelling reasons are established, the product is assessed for security impacts, and explicitly approved for use. Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used unless they are necessary for mission accomplishment and there are no alternative solutions available. Such products are assessed for security impacts, and explicitly approved for use. Purchased software is used in accordance with contract agreements and copyright laws. Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software. Use of publicly accessible peer-to-peer file trading networks is also controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### SA-3.e SYSTEM DOCUMENTATION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that adequate documentation is available for the information system.

There is adequate vendor-supplied documentation of purchased software, hardware, and firmware for the information system. There is adequate documentation for applications and for in-house developed software, hardware, and firmware.

*Administrator Guides and Manuals*

There are adequate administrator guides and/or manuals for the information system. Documentation includes guides and/or manuals for the information system's privileged users. The guides and/or manuals provide, at a minimum, information on: (i) configuring, installing, and operating the system; (ii) making optimum use of the system's security features; and (iii) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation is updated as new vulnerabilities are identified.

*User Guides and Manuals*

There is a general user's guide that describes the security mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact. Information system, administrator, and user documentation are updated to include security controls added since development and as new vulnerabilities are identified.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### SA-4.e OUTSOURCED INFORMATION SYSTEM SERVICES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks from outsourced services by explicitly addressing the need for effective security controls at the service provider.

Acquisition or outsourcing of dedicated information system security services such as: (i) incident monitoring, analysis and response; (ii) operation of information system security devices (e.g., firewalls); or (iii) key management services, are supported by a risk assessment and approved by the appropriate, designated organization official. Acquisition or outsourcing of information system services explicitly addresses government, service provider and end user security roles and responsibilities. Appropriate controls are applied to outsourced software development. Appropriate policies and procedures concerning activities of external third parties (e.g., service bureaus, contractors, other service providers such as system development, network management, security man-

agement) are documented, agreed to, implemented, and monitored for compliance and include provisions for: (i) security clearances (where appropriate and required); (ii) background checks; (iii) required expertise; (iv) confidentiality agreements; (v) security roles and responsibilities; (vi) connectivity agreements; and (vii) individual accountability. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**SA-5.e DEVELOPER FUNCTIONAL TESTING**

CONTROL OBJECTIVE: Testing is planned, conducted, and results documented by the developer of the information system.

The developer performs functional testing to establish that the product exhibits the properties necessary to satisfy the functional requirements. Testing is performed according to a documented plan that identifies the security functions to be tested and describes the goal of the tests to be performed. Testing is conducted using documented procedures that provide instructions for using test programs and test suites, including any test ordering requirements, the test environment, test conditions, test data parameters and values, how the test results are derived from the test inputs, and the expected test results.

The developer addresses those aspects of testing that deal with completeness of test coverage; including the extent to which the functional specification is tested and whether or not the testing is sufficiently extensive to demonstrate that the product operates as specified. The testing is designed and conducted with consideration for the correspondence between the tests identified in the test documentation and the requirements in the functional specification.

The developer addresses the level of detail to which the product is tested. The level of testing is appropriate to demonstrate that the implementation is consistent with its design. The objective is to counter the risk of missing an error in the development of the product. Testing is performed to the depth necessary such that the internal interfaces between subsystems of the high-level design have been exercised. The high-level design provides a description in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide.

**Test ordering is based upon an analysis ensuring that testing is structured such as to avoid circular arguments about the correctness of the information system being tested.**

**Test design and conduct is based upon an analysis of the test coverage that demonstrates the correspondence between the functional specification and the tests identified in the test documentation is complete.**

**Testing is performed to the depth necessary such that the internal interfaces between subsystems of the low-level design have been exercised. The low-level design provides a description of the internal workings in terms of modules and their interrelationships and dependencies. For each module, the low-level design describes its purpose, function, interfaces, dependencies, and the implementation of any policy-enforcing functions.**

**SA-6.e LIFE CYCLE SUPPORT**

CONTROL OBJECTIVE: The information system development life cycle is clearly defined.

A system development life cycle (SDLC) methodology has been developed that: (i) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (ii) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (iii) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements. Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology. The developer establishes a life-cycle model encompassing procedures, tools and techniques used to develop and maintain the information system and providing the necessary control over the development and maintenance of

the system. **The life-cycle model is a standardized life-cycle model that has been approved by some group of experts (e.g. academic experts, standards bodies).**

**SA-7.b SECURITY DESIGN DISCIPLINES**

CONTROL OBJECTIVE: The information system is implemented using engineering disciplines.

The principles in NIST Special Publication 800-27 are considered and applied as appropriate.

**SA-8.b SECURITY POLICY MODEL**

CONTROL OBJECTIVE: The information system security policy is informally modeled to facilitate implementation and verification.

The information system is developed based upon a security policy model that in-turn is based on the security policies for the system and establishes a correspondence between the functional specification, the security policy model, and these system security policies. The model describes the rules and characteristics of applicable policies and includes a rationale that demonstrates that it is consistent and complete with respect to all policies modeled.

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY CONTROL REVIEW (CR)

### CR-1.e INFORMATION SYSTEM ASSESSMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to support knowledgeable, risk-based information system authorization by performing a technical assessment of the system.

Assessments of the information system are conducted to: (i) determine if security controls are correctly implemented and, as implemented, are effective in their application; (ii) ensure that security-applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines are met. Assessments of security controls are conducted: (i) prior to initial operational capability and authorization to operate; (ii) prior to each re-authorization to operate; or (iii) when a significant change to the information system occurs. Routine self-assessments are conducted every [*Assignment: time period (e.g., annually)*] to monitor the effectiveness of security controls. Management reviews of system assessment results are conducted and documented forming the basis for management decisions and action plans. Inspection reports, including self-assessment reports, corrective actions and supporting documentation are retained for a minimum [*Assignment: time period (e.g., five years)*]. Assessments are conducted in a manner to minimize disruption of operations. **Assessments of the information system security controls (other than routine self-assessments) are conducted by assessors independent of the program manager, information system owner, system operator, and end user. Assessors are expected to provide a report of findings directly to the program manager or system owner, who in turn provide the results to the authorizing official or to the authorizing official's designated representative. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CR-2.e VULNERABILITY SCANNING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*]. **Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CR-3.b VULNERABILITY ASSESSMENT AND PENETRATION TESTING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to determine the degree to which the information system can be expected to resist attempts to discover and successfully exercise vulnerabilities.

Vulnerability identification is performed on new, existing, and recently modified information systems and facilities. A summary list of vulnerabilities is prepared for each information system and facility being analyzed. Wherever system capabilities permit, automated vulnerability assessment or state management tools are used. Regular internal and external assessments are conducted. The organization conducts periodic testing of the security posture of the information system by at-

tempting to penetrate the system with attack tools and expertise every [*Assignment: time period (e.g., 12 months)*]. Attack tools are used only with the approval from the appropriate authorities and concurrence of legal counsel.

## MANAGEMENT CONTROLS

**FAMILY:** PROCESSING AUTHORIZATION (PA)

### PA-1.e AUTHORIZE INFORMATION SYSTEM CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from connections to information systems by explicit authorization prior to establishing connections.

Management authorizes in writing all connections to other information systems (including systems owned and operated by another program, organization, or contractor). The connections are compliant with established organizational connection rules and approval processes. Connection agreements consistent with intent of NIST Special Publication 800-47 are in place whenever the information system is connected to systems not under the control of the same authorizing official. Trust relationships among hosts and external entities are appropriately restricted. A list is developed and maintained, along with evidence of deployment planning and coordination and exchange of connection rules and requirements for: (i) applications (on all hosting information systems, current and potential); and (ii) the information system (including all hosted applications). Criteria are defined for conditions under which information system connections are to be disabled. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PA-2.e AUTHORIZE MOBILE CODE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from mobile code by explicit authorization prior to establishing a mobile code capability.

Deployment of mobile code is restricted based on its potential to cause damage to the information system if used maliciously. Mobile code registration, approval, and control procedures to prevent the development, acquisition, or introduction of unacceptable mobile code within the information system, are implemented. All mobile code or executable content employed is registered unless otherwise approved by the authorizing official. Uploading of mobile code or executable content from one organizational information system to another system is to be similarly authorized. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PA-3.e AUTHORIZE REMOTE ACCESS CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from remote access (e.g., dial-up access or Internet access) by explicit authorization prior to establishing a remote access capability.

The number of users who can access the information system from remote locations (for information systems other than public web servers or systems specifically designed for public access) is limited and justification for such access is documented, monitored, and approved by a designated organization official. Dial-up lines, other than those that are protected with FIPS 140-2 validated cryptography, are not used for gaining access to an information system that processes organizational information unless the authorizing official provides specific written authorization for a system to operate in this manner. Actions such as periodic monitoring are taken to ensure that installed equipment does not include unanticipated dial-up capabilities. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PA-4.e AUTHORIZE COLLABORATIVE COMPUTING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively imp lemented to reduce risks arising from collaborative computing by explicit authorization prior to establishing a collaborative computing capability.

Running collaborative computing mechanisms (e.g., the IETF standard Web-based Distributed Authoring and Versioning that enables collaborative editing and file management on remote Web servers) on information systems requires explicit authorization by the authorizing official or authorizing official's designated representative. When granted, authorization is specific, identifying allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PA-5.e AUTHORIZE WIRELESS ACCESS POINT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from wireless connections by explicit authorization prior to establishing a wireless capability.

Installation of wireless access points into organizational networks is discouraged and requires explicit authorization by the authorizing official. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PA-6.e AUTHORIZE INFORMATION SYSTEM OPERATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure explicit management authorization to operate the information system and acceptance of risks to the organization's operations and assets.

In compliance with NIST Special Publication 800-37, explicit authorization to operate the information system is received prior to placing the system into operation. If the authorization decision is an interim approval to operate, then: (i) the authorization is granted for a maximum time period (typically in accordance with the designated FIPS Publication 199 security category of the information system) of [*Assignment: time period for each security category (e.g., eighteen months, twelve months, six months)*]. An explicit plan for corrective action is in-place, being effectively implemented, and monitored by the authorizing official. Re-authorization is obtained prior to continued operation following significant information system changes. Re-authorization is obtained at least every [*Assignment: time period, a maximum of three years*]. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## OPERATIONAL CONTROLS

**FAMILY:** PERSONNEL SECURITY (PS)

### PS-1.e POSITION REVIEW

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to review information system-related positions for criticality/sensitivity.

All positions within the organization are assigned a criticality/sensitivity rating (e.g., low, moderate, high) based on the information system access given to individuals filling those positions. The criticality/sensitivity rating is consistent with the FIPS Publication 199 security categories of the information systems accessible to the individuals filling the designated positions. All positions are reviewed for criticality/sensitivity rating periodically every [*Assignment: time period (e.g., five years)*]. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PS-2.e PERSONNEL SCREENING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is not granted without first verifying that the individual seeking access meets organizational personnel security requirements.

Individuals requiring access to information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access for access authorization in accordance with organizational personnel security policies. Privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls), are screened prior to access and periodically every [*Assignment: time period (e.g., two years)*]. For prospective employees, references are contacted and background checks performed, as appropriate. Periodic reinvestigations are performed every [*Assignment: time period, no more than five years*], consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management. Security agreements are required for employees and contractors assigned to work with mission information. The period during which nondisclosure requirements remain in effect is identified. **Non-privileged users are re-screened periodically. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PS-3.e TERMINATION AND TRANSFER

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is terminated upon personnel transfer or termination.

Termination and transfer procedures include: (i) exit interview procedures; (ii) return of property, keys, identification cards, passes, etc.; (iii) notification to security management; and (iv) immediately escorting employees terminated for cause out of the organization's facilities. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PS-4.e THIRD PARTY PERSONNEL SECURITY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that service providers and other third parties apply appropriate personnel security measures.

Personnel security measures employed by service providers and third parties (e.g., service bureaus, contractors, other organizations providing system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include, if appropriate, provisions for: (i) security clearances; (ii) background checks; (iii) required expertise; and (iv) confidentiality agreements. Personnel security measures employed by service providers and third parties are consistent with the intent of NIST Special Publication 800-35. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## OPERATIONAL CONTROLS

**FAMILY:** PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

### PE-1.e IDENTIFICATION OF SENSITIVE FACILITIES AND RESTRICTED AREAS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to identify and designate sensitive facilities and restricted areas containing information systems.

The organization identifies and designates sensitive facilities and restricted areas (i.e., areas, rooms, or groups of rooms containing information system servers, controlled interface equipment, associated peripherals or communications equipment that must be relied upon for the correct enforcement of the system security policy). The organization also identifies and designates non-sensitive facilities and non-restricted areas, (i.e., areas, rooms, or groups of rooms containing information system components not involved in security policy enforcement and possibly accessible to the general public). **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PE-2.e AUTHORIZE PHYSICAL ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage, and make available for enforcement, authorizations for physical access to sensitive facilities and restricted/controlled areas containing information systems.

A list of persons with authorized physical access to sensitive facilities and restricted/controlled areas containing information systems (i.e., access authorizations) is maintained. Access lists also show which individuals are authorized to operate the information system or supporting peripheral equipment. Access lists are documented on standard forms, maintained on file, and approved by appropriate organization officials. The list of persons with authorized physical access to sensitive facilities and restricted/controlled areas is reviewed by appropriate organization officials every [*Assignment: time period (e.g., as needed and at least annually)*]. **Access lists are securely transferred to the enforcement section of the organization. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### PE-3.e PHYSICAL ACCESS ENFORCEMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply physical access controls at designated physical entry points within sensitive facilities and restricted/controlled areas containing information systems.

Physical security perimeters are defined by the organization. Sensitive facilities and restricted/controlled areas are prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that control access. The main entrance to sensitive facilities and restricted areas is controlled/manned. Secondary entrances have cameras and/or electronic entry detection devices (e.g., card keys), to monitor access. Apparent security violations or suspicious physical access activities are investigated and remedial actions taken. Every physical access point to sensitive facilities or restricted areas housing information systems that process or display information is controlled during working hours and guarded or locked during non-work hours. Identification badges are worn. Access authorization is verified before granting physical access. Unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and sys-

tem/media libraries after an emergency-related event (e.g., fire drills, evacuations, etc.). The organization controls access to non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) as appropriate in accordance with the organization's assessment of risk. **The [*Assignment: list of physical access points*] physical access points are controlled twenty-four hours per day, seven days per week through the use of entry devices such as key cards or biometrics. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-4.e ACCESS MONITORING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to monitor physical access controls for both proper operation and response to incidents.

Physical accesses to sensitive facilities and restricted/controlled areas containing information systems and system/media libraries are monitored. Audit logs are reviewed every [*Assignment: time period (e.g., daily)*]. Real-time intrusion alarms are centrally monitored. Apparent security violations or suspicious physical access activities are investigated, and remedial actions taken. Non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) are monitored as appropriate in accordance with the organization's assessment of risk. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-5.e VISITOR CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control visitor access to sensitive facilities and restricted/controlled areas containing information systems and system/media libraries.

Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks. Visitors, contractors, and maintenance personnel are formally signed in, escorted, and activities monitored when required. Registers are maintained and include: (i) the name; (ii) date; (iii) time of entry; (iv) time of departures; (v) purpose of visit; and (vi) person(s) visited. The register is closed out [*Assignment: time period (e.g., at the end of each month)*] and reviewed by appropriate organization officials. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-6.e PHYSICAL ACCESS TO INFORMATION TRANSMISSION MEDIUM**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to mitigate eavesdropping, in-transit modification, and service disruption threats by controlled physical access to information transmission medium.

Physical access to unencrypted information transmission lines is controlled to the extent necessary to mitigate eavesdropping and in-transit modification. Physical access to all information transmission lines is controlled to the extent necessary to mitigate service disruption by physical tampering or destruction. Access to devices that display or output information is appropriately controlled. Devices that display or output information are positioned to deter unauthorized individuals from reading the information. Access to mobile or portable information systems is appropriately controlled. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-7.e ROUTINE PHYSICAL SECURITY CHECKING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance physical security by periodically checking for physical security compliance.

Routine checks (e.g., end of the day security checks and unannounced security checks) are performed periodically to ensure that information is being properly handed and stored. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-9.e STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to securely store information and information systems.

Documents/equipment are stored in approved containers or facilities with maintenance and accountability procedures. All restricted areas used to protect information meet criteria for secured area or security room, or provisions are made to store high value items in appropriate containers during non-working hours. Organizational information in any form is protected during non-working hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization. Mobile and portable information systems are stored securely. Organizational information is locked in cabinets or sealed in packing cartons while in transit. Organizational information remains in the custody of an authorized individual. Accountability is maintained during movement. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-10.e ACCESS DEVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance physical security by using devices to control access.

Keys, combinations, or other access devices are needed to enter sensitive facilities or restricted/controlled areas that contain information or information systems unless other protective measures (e.g., guards) are in place. Keys, combinations, or other access devices are secured. Combinations and keys are changed periodically with changes occurring at least every [*Assignment: time period (e.g., annually for combinations)*]. Combinations are changed when an employee retires, transfers to another position, or is no longer an employee. An envelope containing the combination or duplicate key is secured in a container with the same or higher protections as the material the lock secures. Keys are changed as necessary to prevent or respond to compromise. Issued keys or other entry devices are regularly inventoried. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**PE-11.b PHYSICAL SECURITY CONTAINERS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance physical security by using containers and facilities that meet defined requirements.

Organizational information requiring protective storage is stored in security containers compliant with General Services Administration requirements and guidelines.

**PE-12.e IDENTIFY NATURAL DISRUPTION/DISASTER PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide an effective response to disruptions and natural disasters by explicitly indicating the intended disruption/disaster coverage.

The nature of the disruptions or natural disasters being mitigated and the extent of the expected mitigation are clearly described. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-13.e PLUMBING LINES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the potential damage from plumbing leaks.

Building plumbing lines do not endanger the information system facility or, at a minimum, shutoff valves and their operating procedures exist and are known. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-14.e EMERGENCY LIGHTING**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance safety and availability by providing lighting in the event of a power outage.

An automatic emergency lighting system is installed that covers emergency exits and evacuation routes. **Emergency lighting system also covers all areas necessary to maintain mission or business essential functions. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**PE-15.e FIRE PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to prevent, detect, and respond to fire.

Fire suppression and prevention devices and systems, (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, battery-operated or electric stand-alone smoke detectors) are installed, available, and working properly should an alarm be sounded or a fire be detected. The fire department receives an automatic notification of any activation of the smoke detection or fire suppression system. Fire suppression and prevention devices and systems are periodically checked. Fire ignition sources, such as potential failures of electronic devices or wiring, improper storage of materials, are reviewed periodically. Information system facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved. **A fully automatic fire suppression system (compliant with General Services Administration requirements and guidelines) is installed that automatically activates when it detects heat, smoke or particles with appropriate safeguards for danger to personnel from toxicity. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**PE-16.e TEMPPERATURE AND HUMIDITY CONTROLS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control the temperature of facilities containing information systems.

Heating and air-conditioning systems are regularly maintained. Temperature and humidity are controlled automatically. **Temperature and humidity controls are installed and provide an alarm when temperature and humidity fluctuations potentially harmful to personnel or equipment operation are detected. Adjustments to heating or cooling systems may be made manually. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**PE-17.e POWER**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to maintain safe power for the information system.

Power cabling supporting the information system is protected from damage. A master power switch or emergency cut-off switch to information system equipment is present. It is located near the main entrance of the information system area and it is labeled and protected by a cover to prevent accidental shut-off. **Automatic voltage control is implemented for information systems. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**PE-18.b POWER SUPPLY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide for uninterrupted power.

A short-term uninterruptible power supply is provided so that in the event of loss of primary power source, adequate power is maintained for orderly shut down without need for manual intervention.

**PE-19.e ENVIRONMENTAL CONTROL TESTING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically test environmental protections.

Controls protecting the environment (power, temperature, fire protection, lighting, plumbing) against disruptions and natural disasters are periodically tested every [*Assignment: time period(s) (e.g., by type of test and by type of facility)*]. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-20.e ENVIVONMENTAL CONTROL TRAINING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel on the use of environmental controls.

Individuals that maintain environmental controls or would use the environmental controls in the event of an emergency receive initial training in the operation of the controls. Periodic refresher training is provided every [*Assignment: time period (e.g., annually)*]. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-21.e EQUIPMENT DELIVERY AND REMOVAL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the flow of equipment into and out of the organization.

The organization controls the hardware, firmware, and software entering and exiting the facility, the movement of these items within the facility, and maintains appropriate records of those items. Delivery and loading areas are controlled and, if possible, isolated from information system and system/media libraries to avoid unauthorized access. Information system hardware, firmware, software, or information belonging to the organization is not removed without authorization. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-22.e SEPARATE FACILITIES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance security by physically separating mission functions and assigning separate resources for those functions.

Separate resources are used for: (i) development and operational processing; and (ii) critical mission activities and routine operations. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**PE-23.b ALTERNATE WORK SITE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply specified requirements to alternate work sites.

Alternate work site security requirements are in place and are consistent with the intent of NIST Special Publication 800-46. Means are available to facilitate communication with information system security staff in case of security problems.

## OPERATIONAL CONTROLS

**FAMILY:** CONTINGENCY PLANNING AND OPERATIONS (CP)

### CP-1.e CONTINGENCY PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, an effective response to an information system disruption is enabled by developing a system contingency plan.

A contingency plan is produced for the information system that is compliant with OMB policy and consistent with the intent of NIST SP 800-34. In addition, key affected parties approve the contingency plan for the system. The plan is reviewed once a year, reassessed, tested and, if appropriate, revised to reflect changes in hardware, software and personnel. **Plan includes checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the plan is being implemented as intended.**

### CP-2.e CONTINGENCY PLAN TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel in their contingency roles and responsibilities.

Operational and support personnel (including managers and users of the information system) have received training in contingency operations and understand their emergency roles and responsibilities. Personnel receive periodic training in emergency fire, water, and alarm incident procedures. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CP-3.b CONTINGENCY PLAN EXERCISES AND DRILLS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically test contingency plans and response capabilities.

Contingency plans [*Selection: in their entirety* | [*Assignment: portions*]] are exercised [*Assignment: time period (e.g., annually, quarterly, or semi-annually)*]. Test results are documented and provided to appropriate organizational officials for review.

### CP-4.e CONTINGENCY PLAN STORAGE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by securely storing an up-to-date copy of the contingency plan for the information system off-site.

Copies of the current contingency plan are stored in a secure location at an alternate site accessible by management and other key personnel. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CP-5.b OFF SITE BACKUP STORAGE SITES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by ensuring geographic separation of routine information system operations and backup storage sites.

Backup storage sites are geographically removed from the primary site and environmentally and physically protected.

**CP-6.e INFORMATION BACKUP AND RESTORE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to regularly back up information.

A capability exists to conduct backup storage and restoration of information and access controls. Information backup for the information system is documented and performed [*Assignment: time period which is at least monthly*]. Procedures are in place to test backup via restoration of information from backup media every [*Assignment: time period which is at least annually*]. Appropriate physical and technical protection of the backup and restoration files, hardware, firmware, and software, (e.g., router tables, compilers, and other security-related system software) are in place. Audit logs/records are backed up not less than weekly onto a different information system or media than the system being audited. Generally, audit logs/records are retained for [*Assignment: time period which is at least every six months*]. For these specific information types, the audit records are retained for the time period indicated: [*Assignment: pairs of information type / time-period*]. System and application documentation are maintained at the off-site storage location. The technology is implemented in such a manner as to provide appropriate availability, including consideration of: (i) backup procedures; (ii) system configuration; (iii) redundancy; (iv) environmental controls; (v) staff training; and (vi) routine maintenance. Restoration of any security-relevant segment of the information system state (e.g., access control lists, cryptographic keys, deleted system status information) is possible without requiring destruction of other system information. Standalone computer workstation backup information, software and current operating procedures are stored in accordance with the contingency plan. **Backup storage location allows prompt restoration of information. Backup files are rotated off-site [*Assignment: time period or criteria for what constitutes sufficient rotation*] to avoid disruption if current files are damaged. Back-up copies of the operating system and other critical software are stored in a fire rated container that is not collocated with the operational software. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CP-7.e BACKUP MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable backing up information and the information system state.

Mechanisms provide for sufficient backup storage capability. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time. A capability to conduct the following types of backup exists: (i) full (complete backup); and (ii) [*Selection of one or more: incremental (changes since last incremental) | differential (changes since last full)*]. **Consideration is given to the use of technical features that enhance information integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID) 1 and above, and similar techniques. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CP-8.b ALTERNATE PROCESSING SITE**

CONTROL OBJECTIVE: In accordance with organizational policy, documented procedures are being effectively implemented to maintain operations despite contingencies by providing an alternate processing site.

An alternate site is identified that permits [*Assignment: mission or business essential functions*] operations without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations or capabilities are unavailable. Arrangements and agreements are established for alternate facilities that are in a state of readiness commensurate with the risks of interrupted operations. Alternate processing sites are geographically

removed from the primary site, and environmentally and physically protected. Arrangements are planned for travel and lodging of necessary personnel if needed.

**CP-9.e RESTORING INFORMATION UNDER EMERGENCY CONDITIONS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for physical access to information system facilities under emergency conditions.

Facility access is allowed in support of restoration of lost information under the contingency plan in the event of an emergency. Emergency and temporary access authorizations are: (i) documented on standard forms and maintained on file; (ii) approved by appropriate organization managers; (iii) securely communicated to the security function; and (iv) automatically terminated after a predetermined period. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CP-10.e INFORMATION SYSTEM RECOVERY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to securely recover the information system after failure or other contingency.

Recovery procedures and mechanisms exist to ensure that recovery is done in a trusted, secure, and verifiable manner. Contingency plans, software procedures, and installed security and backup provisions protect against improper modification of information in the event of an information system failure. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures are in place. Adequate manual processing procedures are available for use until automated operations are restored. Restart capabilities are part of any operation that updates files and consumes large amounts of computer time. Mechanisms to allow for the restoration of the information system in a secure and verifiable manner are implemented. Restoration of operational capabilities with minimal loss of service or information is provided. Assurance is provided that the state of the information system after the restore reflects any security-relevant changes to the system between the backup and the restore. Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptographic keys, deleted system status information) is obtained without requiring destruction of other system data. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CP-11.b MANAGEMENT ACCOUNTABILITY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to hold management accountable for the ability to respond to contingencies.

Management is able to show how the organization responds to specific disasters/disruptions to: (i) protect lives; (ii) limit damage; (iii) protect information; (iv) circumvent security controls only according to established bypass procedures; and (vi) minimize the impact on organizational operations and assets.

**CP-12.e INFORMATION SYSTEM MODIFICATION IMPACT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to re-evaluate contingency plans prior to approving major changes to the information system.

Contingency plans are re-evaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to maintain adequate risk mitigation. **With respect to necessitating plan re-evaluation, the term "major change" is clearly defined and this definition documented. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CP-13.b ALTERNATE COMMUNICATION SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for alternate communications services.

Arrangements are in place for alternate [*Selection (one or more): long haul | short haul*] communications services capable of restoring adequate communications to accomplish the following mission functions [*Assignment: list of functions*] without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations and communications capabilities are unavailable. Arrangements are planned for travel and lodging of necessary personnel if needed.

## OPERATIONAL CONTROLS

**FAMILY:** CONFIGURATION MANAGEMENT (CM)

### CM-1.e CONFIGURATION MANAGEMENT PLAN

CONTROL OBJECTIVE: Enable knowing the information system configuration and controlling changes throughout the system development life cycle by developing a configuration management plan when the organization's plan is not adequate to address system needs.

The configuration management plan for the information system is consistent with the intent of IEEE Standard 828-1998 (or successor if superceded). The configuration management plan is evaluated periodically every [*Assignment: time period (e.g., annually)*] and updated as necessary to verify the plan and the ability of those tasked to carry out the plan. **Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.**

### CM-2.e CONFIGURATION MANAGEMENT PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage the configuration of the information system.

The configuration management process is consistent with the organization's information technology architecture plans. Formally documented configuration management roles, responsibilities, and procedures to include the management of information system security information and documentation are in place. Changes to the information system are authorized by appropriate organization officials and are not permitted outside of the configuration management process. Personnel involved in configuration management have been trained and are familiar with the organization's configuration management process. The guidance is appropriate for personnel with varying levels of skill and experience. Appropriate tools are used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates. Production program changes are periodically reviewed by appropriate organization officials to determine whether access controls and change controls are being followed. The configuration management plan is evaluated periodically every [*Assignment: time-period (e.g., annually)*].

*Information System Components*

Distribution of new software is controlled. Software licensing agreements are enforced and violations of those agreements are prohibited. The use of personal and public domain software is restricted. The name, brand, type, model, version/release number, and physical location of each information system component (hardware, software, and firmware) are identified and documented.

*Change testing*

Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control). Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control). Test plans include appropriate consideration of security. Unit, integration, and system testing are performed and approved in accordance with the test plan and applying a sufficient range of valid and invalid conditions. A comprehensive set of test transactions and information is developed that represents the various activities and conditions that will be encountered during information system operation. Test results are documented and appropriate responsive actions are taken based on the results. The type of test information to be used on the information system is specified, (i.e., live or simulated). Test results are reviewed and documented. All patches, upgrades, and new applications are tested prior to deployment (compliance testing).

**Changes to the information system are not technically or procedurally feasible outside of the configuration management process. Procedures include checks to be performed and assigned**

**responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CM-3.e BASELINE CONFIGURATION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to document and maintain a current baseline, operational configuration of the hardware, software, and firmware that comprise the information system.

A current and comprehensive baseline inventory of all hardware and firmware (to include manufacturer, type, and version) required to support the operation of the information system is maintained as part of the configuration management plan. A current and comprehensive baseline inventory of all software (to include manufacturer, type, and version and installation manuals and procedures) required to support the operation of the information system is maintained. Backup copies of the inventory are adequately protected. All system software is current and has current and complete documentation. There are information system diagrams and documentation on the setup of routers, switches, guards, firewalls and any other devices facilitating connections to other systems. The current configuration information is routinely validated for accuracy. For distributed information systems, there are software distribution implementation orders including effective date provided to all locations. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### CM-4.e CHANGE CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control changes to the information system.

Change control mechanisms maintain control of changes to hardware, software, and security mechanisms. Changes to information system specifications are prepared by the programmer and reviewed by a programming supervisor. System components are tested, documented, and approved (operating system, utility, applications) prior to promotion to production. Program changes are moved into production only upon documented approval from users and appropriate officials responsible for system development. Software changes are documented so that they can be traced from authorization to the final approved code. Documentation facilitates traceability of code to design specifications and functional requirements. Documentation is updated for software, hardware, operating personnel, and information system users when a new or modified information system is implemented. Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

*Change Request*

Software change request forms are used to document requests and related approvals. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document. Change requests are approved by appropriate organization officials including, but not limited to, information system users and information system support staff. Change control is effected by: (i) notifying users of the time and date of the last change in information content; (ii) ensuring that changes are executed only by authorized personnel; (iii) ensuring that intended the change is properly implemented; and (iv) providing a secure, unchangeable audit trail to clearly document the change.

*Emergency Changes*

Emergency changes for the information system are documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration are appropriately documented and approved and appropriate personnel are notified for analysis and follow-up.

**The information system is under the control of a chartered configuration control board that meets regularly. The program manager/system owner and the information system security official are represented on the control board. An independent library control group performs migration of tested and approved information system software to production use. Images of program code are maintained and compared before and after changes to ensure that only approved changes are made. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CM-5.e LIBRARY MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to manage software libraries.

Software libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code. Library management software is used to produce audit trails/logs of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates. All deposits and withdrawals of media (e.g., tapes, disks) to/from the software library are authorized and logged. Production source code is maintained in a separate archive library. Separate libraries are maintained for program development and maintenance, testing, and production programs. Outdated versions of information system software are removed from production libraries. A group independent of the user and programmers controls movement of programs and information among libraries. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CM-6.e CHANGE ACCESS CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce access restrictions associated with change control.

Restrictions are in place for accessing information system software and for using and monitoring use of system software utilities. Responsibilities for using system utilities have been clearly defined and are understood by systems programmers. Responsibilities for monitoring use are defined and understood by organization officials. Application programmer privileges to change production systems (programs and data) are limited and are reviewed [*Assignment: time period (e.g., annually)*]. Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features. Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software. Justification and approval by appropriate organization officials for access to systems software is documented and retained. The use of privileged system software and utilities is reviewed by appropriate organization officials periodically every [*Assignment: time period (e.g., annually)*] to ensure that access permissions correspond with position descriptions and job duties. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CM-7.e MONITORING CHANGE ACTIVITY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to monitor information system changes and actions by privileged users.

System programmers' activities are monitored and reviewed. The use of information system utilities is logged using access control software reports or job accounting information. All accesses to information system software files are logged by automated logging facilities. Installation of all information system software is logged to establish an audit trail/log and is reviewed by appropriate organization officials. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**CM-8.e MINIMAL SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure systems for only necessary capabilities.

The function and purpose of processes and services are documented and approved by appropriate organization officials. The information system is periodically reviewed to identify and eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls). Protocols that would introduce an unacceptable level of risk are disabled; specifically the following protocols are generally disabled [*Assignment: list of protocols.*]. Available processes/services are minimized, such as through: (i) installing only required services; and (ii) restricting the number of individuals with access to such services, based on the concept of least privilege. The information system that supports the server functionality is, as much as possible, dedicated to that purpose. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CM-9.e SECURE CONFIGURATION SETTINGS, CHECKLISTS, AND BENCHMARKING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure and benchmark information technology products in accordance with good security practice settings.

Default settings of security features on the information technology products employed within the information system are set to the most restrictive mode compatible with system operational requirements. Vendor-supplied passwords for component products in the information system are changed. Information system initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. The operating system is configured to prevent circumvention of the security software and application controls. An organization reference document such as a security recommendation guide (SRG), security technical implementation guide (STIG), or security checklist constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products and all operational information system and hosted applications. If organization reference documents are not available, other government guidelines or vendor literature are acceptable sources. When appropriate tools are available, configurations of information systems are benchmarked using automated scoring tools. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CM-10.e NETWORK CONFIGURATION SETTINGS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure network parameters to reduce exposures.

Networks are appropriately configured to adequately protect access paths between information systems. Each information system boundary interface is configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited. Trust relationships among hosts and external entities are appropriately restricted to the minimum level necessary to accomplish mission tasks. Security attributes of each network service are clearly described. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CM-11.e PRIVACY POLICY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to indicate user privacy is a priority within the organization.

Privacy policies in effect are posted on appropriate information systems (including web sites) within the organization. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**CM-12.e LIMITING TRAFFIC TYPES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure the information system to control specified types of traffic.

Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within organizational information systems. Both inbound and outbound public service instant messaging traffic is blocked at the information system boundary. [Note: This does not include instant messaging services that are configured by an authorized application or site to perform an authorized and official function.] Voice over Internet Protocol traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within organizational information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the information system boundary. [Note: This does not include Voice over Internet Protocol services that are configured by an authorized application or site to perform an authorized and official function.] **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## OPERATIONAL CONTROLS

**FAMILY:** HARDWARE AND SOFTWARE MAINTENANCE (MA)

### MA-1.e PERIODIC MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct periodic on-site and off-site maintenance of the information system and of the physical plant within which this information system resides.

Comprehensive maintenance testing procedures exist that systematically schedule information system hardware for periodic maintenance inspections and testing to ensure the equipment operates within design specifications and is properly calibrated. Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations. Repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks) are documented. Regular and unscheduled hardware maintenance performed is documented. A maintenance log is maintained and includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort; and (iv) a description of the type of maintenance performed to include identification of replacement parts. Maintenance of information systems is performed on-site whenever possible. If information systems or system components are to be removed from the facility for repair, any component containing non-volatile memory is sanitized or appropriate\ cleared and its release is explicitly approved by an appropriate organization official. Maintenance changes that impact the security of the information system receive a configuration management review. After maintenance is performed on the information system, the security features are checked to assure that they are still functioning properly. Maintenance is performed in a manner that maintains security. **Problems and delays encountered, the reason and elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends. Management periodically reviews and compares the service performance achieved with goals and surveys user departments to see if their needs are being met. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### MA-2.e MAINTENANCE TOOLS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control and monitor the use of maintenance tools.

Introduction of network analyzers (e.g., sniffers) that allow maintenance personnel the capability to monitor the content of network traffic are approved by an appropriate organization official prior to being introduced into an information system. If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a facility, the media containing the programs are checked for malicious code before the media is connected to the information system. **Before leaving the facility, the media are checked to assure that no organizational information has been written on it. All diagnostic equipment and other devices carried into a facility by maintenance personnel are handled as follows: (i) all diagnostic and test equipment is inspected for obvious improper modification; (ii) maintenance equipment that has the capability of retaining information is appropriately sanitized before being released; (iii) if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless explicit exception is authorized by an appropriate organization official. Replacement components that are brought into the facility for the purpose of swapping with facility components are allowed. However, any component placed into an information system remains in the facility until proper release procedures are completed. Any component that is not placed in an information system may be released from the facility. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MA-3.e REMOTE MAINTENANCE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide additional controls on remotely executed maintenance.

Installation and use of remote diagnostic links are specifically addressed in the security plan and agreed to by the authorizing official. Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. The communications links connecting the components of the information system, associated information communications, and networks are protected in accordance with the FIPS Publication 199 security category of the information that may be transmitted over the link. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed. Unless an exception has been granted by an appropriate organization official, maintenance personnel accessing the information system at the remote site are cleared to the highest FIPS Publication 199 security category of information processed on that system, even if the system was downgraded/sanitized prior to remote access. An audit log is maintained of all remote maintenance, diagnostic, and service transactions including all commands performed and all responses. The log is periodically reviewed by an appropriate organization official. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as tokens; (iii) and remote disconnect verification. Where possible, remote sessions involve an interactive window for coordination with information security official responsible for the system being serviced. When the remote maintenance has been completed, all sessions are terminated and the remote connection is also terminated. Authenticators (e.g.,, passwords) used during remote maintenance are changed following each remote maintenance service. **Keystroke monitoring is performed on all remote diagnostic or maintenance services. A technically qualified person reviews the maintenance log, and if appropriate, the audit log to assure the detection of unauthorized changes. Maintenance technicians responsible for performing remote diagnosis/maintenance are advised (e.g., contractually, verbally, or by banner) prior to remote diagnostics/maintenance activities that keystroke monitoring will be performed. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MA-4.e MAINTENANCE PERSONNEL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the authorization of an individual to perform maintenance.

The list of authorized maintenance personnel is documented. Only personnel authorized to do so perform maintenance on the information system. Except as authorized by the authorizing official, personnel who perform maintenance on the information system are authorized access to the highest FIPS Publication 199 security category of information processed on that system. Such personnel who perform maintenance or diagnostics on an information system do not require an escort, unless need-to-know controls must be enforced. However, a facility employee who is authorized to access the highest FIPS Publication 199 security category of information and, when possible, technically knowledgeable, is present within the area where the maintenance is being performed to assure that the proper security procedures are being followed. Foreign nationals (with proper authorizations) may be utilized as maintenance personnel for those information systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions are fully documented within a Memorandum of Agreement. A person not authorized access to the informa-

tion system may be used to perform maintenance on the system provided an escort who is authorized access and is technically qualified monitors and records that person's activities in a maintenance log. **Prior to maintenance, the information system is completely cleared and all nonvolatile information storage media removed or physically disconnected and secured. When an information system cannot be cleared, approved procedures are enforced to deny the maintenance personnel visual and electronic access to any organization information that is contained on the system. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MA-5.b TIMELY MAINTENANCE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that maintenance services and parts are available in a timely manner.

Spare or backup hardware is used to provide a high level of information system availability for organization applications. Maintenance support and critical maintenance spares and spare parts for [*Assignment: list of key information system assets*] can be obtained within [*Assignment: time period (e.g., twenty-four hours)*] of failure.

**MA-6.e MAINTENANCE SCHEDULING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to schedule maintenance operations and accommodate unscheduled maintenance with minimal mission impact.

Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing. A retrievable, exact copy of electronic information exists before movement of equipment used to process such information. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted. Emergency change requests are approved by management either prior or after the fact. Flexibility exists in the organization's operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance. Version control is maintained and contingency plans are updated after any changes. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

.

## OPERATIONAL CONTROLS

**FAMILY:** SYSTEM AND INFORMATION INTEGRITY (SI)

### SI-1.e FLAW REMEDIATION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate flaw remediation for the information system.

Significant weaknesses in the operational information system are reported and effective remedial actions are taken. This includes the following:

*Patch Management*

Systems affected by recently announced software vulnerabilities are identified. Patches are installed on a timely basis and tested for effectiveness and potential side effects on the organization's information systems. There is verification that patches, service packs, and hot fixes are appropriately installed on affected systems.

*System Software Problems*

A log is used to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.

*Malicious Code Screening*

As needed, incoming information is reviewed for viruses and other malicious code. Anti-viral mechanisms are used to detect and eradicate viruses transported by e-mail or attachments. The information system is automatically safeguarded from virus infections from other sources as well (e.g., central choke points where diskettes are scanned for viruses prior to distribution). There is timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

*Miscellaneous*

Software is up-to-date (latest versions of service packs, patches, and hot fixes are installed). Security weaknesses are being reported and acted upon. Software malfunctions are being reported and acted upon. Hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### SI-2.b PERSONNEL SUPERVISION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure adequate supervision of personnel and review of their activities.

Active supervision and review are provided for all personnel, including each shift for computer operations. Staff's performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out. Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities. All mission/business partners are reviewed for compliance with information systems security requirements.

### SI-3.b PROCEDURAL REVIEW

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are periodically reviewed.

A review is conducted every [*Assignment: time period (e.g., twelve months)*] that comprehensively evaluates existing security policies and procedures to ensure procedural consistency and to ensure that they fully support the goal of enabling mission accomplishment. Access authorizations are pe-

riodically reviewed for incompatible functions. Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels.

**SI-4.e SOFTWARE AND INFORMATION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to both protect against and to detect unauthorized changes to software.

Integrity verification applications are available on the information system to look for evidence of information tampering, errors, and omissions. Tools for automatically monitoring the integrity of the information system and the applications it hosts are implemented. Good engineering practice with regard to commercial off-the-shelf integrity mechanisms, such as parity checks and cyclical redundancy checks are employed. The operating system's operational status and restart integrity is protected during and after shutdowns. Mechanisms prohibit users from modifying the functional capabilities of boundary protection devices such as firewalls, gateways, and routers. There is limited write access to information system security capabilities (that is., the hardware, software, and firmware that perform operating system or security functions and the hardware, software, and firmware that must be relied upon in order for the system security functionality to operated correctly). **Message authentication codes, cryptographic hashes, digital signatures and digitally signed timestamps or notarizations are implemented using current standards (i.e., FIPS 198 HMAC, AES -MAC, FIPS 180-2, FIPS 186-3) or subsequently adopted standards, for ensuring the integrity of stored or archived files. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SI-5.e VALIDATION OF MISSION PROCESSING**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable verification of mission processing.

*Input*

Information input to application systems that is directly related to the accomplishment of organization missions is validated to ensure that it is correct and appropriate. Effective use is made of automated entry devices to reduce the potential for information entry errors. Validation and editing are performed at the computer workstation during information entry or are performed as early as possible in the information flow and before updating the master files. All information fields are checked for errors before rejecting a transaction.

*Processing*

Mechanisms are implemented to verify processing of information that is directly related to the accomplishment of organization missions. For example: (i) reconciliation routines are used by information system applications, (i.e., checksums, hash totals, record counts); (ii transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction rollback and transaction journaling, or the technical equivalents of those processes; (iii) computer matching of transaction information with information in master or suspense files occurs to identify missing or duplicate transactions; (iv) trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed; (v) computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing; (vi) system interfaces require that the sending system's output control counts equal the receiving system's input counts; (vii) error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error; (viii) rejected information is automatically written on an automated suspense

file and held until corrected; (ix) each erroneous transaction is annotated with codes indicating the type of error, date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction; (x) general controls effectively protect the suspense file from unauthorized access and modification; (xi) the suspense file is purged of transactions as they are corrected; (xii) record counts and control totals are established over the suspense file and used in reconciling transactions processed; (xiii) programmed validation and edits include checks for reasonableness, dependency, existence, mathematical accuracy, range, check digit, document reconciliation, and relationship or prior information matching, and (xiv) suspense file is regularly reviewed by management for analysis of the level and type of transaction errors and the age of uncorrected errors.

*Output*

Output from an information system that is directly related to the accomplishment of organization missions is validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Action is taken if inappropriate activities are discovered.

**Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SI-6.b SYSTEM OPERATION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to verify the correct operation of security and security-relevant functionality.

Mechanisms are in place to validate the expected operation of the security-relevant software, hardware, and firmware. These mechanisms are exercised [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: time-period*]].

## OPERATIONAL CONTROLS

**FAMILY:** MEDIA PROTECTION (MP)

### MP-1.e MEDIA ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media.

Unauthorized individuals cannot read, copy, alter, or destroy information in printed form or on media removed from the information system. Media accountability and control mechanisms (e.g., audit trail logs), provide protection comparable to that for equivalent paper documents. Electronic media is controlled and protected in a manner similar to that used for paper materials. Output from the information system is given only to authorized users. Random or representative sampling techniques are used to verify the proper marking of large volumes of output. If available and approved, automated techniques are used to verify the proper output marking of information. **Review of Human-Readable Output: Before human-readable output is released outside the information system, an appropriately authorized individual provides a reliable review of the output to determine whether it is accurately marked with the appropriate and applicable security markings. The review is at a level of detail to allow reviewer to accept security responsibility for releasing the information to its recipient. Explicit approval is obtained from the appropriate organization official before forwarding output, which has not had a reliable review for appropriate marking, to recipients who do not have access to the information system. Such approval(s) can be for a specific release, for the overall release procedure(s), or for both. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### MP-2.b LABELING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate securing electronic and paper media by incorporating security labels.

Appropriate security labels that reflect the distribution limitations and handling caveats of the information are affixed to all information system output. Removable information storage media contain external labels indicating the distribution limitations and handling caveats of the information.

*Marking Human-Readable Output*

Human-readable output is marked appropriately, on each human-readable page, screen, or equivalent (e.g., the label appears on each microfiche *and* on each page of text on the fiche). Individual pages of output are marked as appropriate either: (i) to reflect the distribution limitations and handling caveats and applicable associated security markings of the information that is printed on each page; or (ii) with the most restrictive limitations and caveats and all applicable associated security markings of the information that is to be printed.

*Variations*

The following specific types of media or hardware components need not be marked so long as they remain within a single, secure environment: [*Assignment: list of media types and hardware components*].

### MP-3.e MEDIA TRANSPORT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to help protect electronic and paper media that is physically transported.

Only authorized users pick up, receive, or deliver input and output information and media from the information system. Appropriate controls are established for all information entering or leaving the facility, including for mailing media and/or printed output from the information system. Erroneous or unauthorized transfer of information, regardless of media or format, is precluded. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MP-4.e MEDIA DESTRUCTION AND DISPOSAL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the destruction and disposal of media, both electronic and paper, to ensure that organizational information does not become available to unauthorized personnel.

Information system hardware and machine-readable media are cleared, sanitized, or destroyed before being reused or released outside of the organization. Retired, damaged, discarded, or unneeded information is disposed in a manner that prevents unauthorized persons from using it. Information is never disclosed during disposal unless authorized by statute. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category. Sanitized media is downgraded only with appropriate approval(s).

*Destruction of Paper Media*

Hard copy documents are destroyed when no longer needed. For information requiring such protection, destruction methods for organizational information in paper form are as follows: (i) burning - the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (ii) mulching or pulping - all material is reduced to particles one inch or smaller; (iii) shredding or disintegrating - paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative). Information storage media is destroyed in accordance with organization-approved methods. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

*Release of Systems and Components*

Equipment removal procedures for information systems and components that have processed or contained organizational information are followed. This includes inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MP-5.e MEDIA SANITIZATION AND CLEARING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the sanitization and clearing of media, both electronic and paper.

Only approved equipment or software is used to degauss or overwrite magnetic media containing organizational information. Degaussing equipment is tested for correct performance every [*Assignment: time period (e.g., annually)*]. Each action or procedure taken to overwrite or degauss such media is verified.

*Optical Disks*

Optical disks (including compact disk/read only memory, write once/read many, digital versatile disk, and read-write compact discs) offer no mechanism for sanitization.

*Sanitizing*

Magnetic media containing organizational information are sanitized by use of an approved degaussing procedure.

*Clearing*

To clear magnetic media, all memory locations are overwritten three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character). The success of the overwrite procedure is verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) remain at the previously designated FIPS Publication 199 security category (for confidentiality) and remain in a secure, controlled environment.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MP-6.e MEDIA-RELATED RECORDS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the maintenance of disposition records for media, both electronic and paper.

Audit trails are used for receipt of inputs/outputs from the information system. A record is kept of who implemented the media disposal actions and who verified that the information or media was properly sanitized. Inventory records of all storage media containing organizational information are maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media are recorded in a log that identifies: (i) date received; (ii) reel/cartridge control number contents; (iii) number of records if available; (iv) movement; and (v) if disposed of, the date and method of destruction. Such a log permits all storage media containing organizational information (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged. Periodic inventories of removable storage devices and media containing organizational information are performed every [*Assignment: time period (e.g., semi-annually)*]. When removable storage devices and media containing organizational information are secured, a proper acknowledgement form is signed and returned to the originator. Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output. A record of the equipment release is created indicating the procedure used for sanitization, and to whom the equipment is intended. This record is retained for [*Assignment: time period (e.g., five years)*]. Logging of shipping and receipts and periodic reconciliation of these records is accomplished every [*Assignment: time period (e.g., monthly)*]. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**MP-7.e MEDIA STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the secure storage of media, both electronic and paper.

Storage media are physically controlled and safeguarded in the manner prescribed for the highest security category (for confidentiality) of the information ever recorded on it until destroyed or sanitized using approved procedures. In those areas where organizational information is processed, unmarked media that are not in factory-sealed packages are protected at the highest FIPS Publication 199 security category (for confidentiality) for information processing conducted within the facility, until the media is reviewed and appropriately labeled. Records management for information stored in an information system or on external media are governed by the records management policies of the appropriate agency, based on the guidelines from the National Archives and Records Agency. **Procedures include checks to be performed and assigned responsibilities for**

**conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## OPERATIONAL CONTROLS

**FAMILY:** INCIDENT RESPONSE (IR)

### IR-1.e INCIDENT RESPONSE PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, enable effective response to incidents by developing an incident response plan when the organizational response plan is not adequate to address information system requirements.

An incident response plan consistent with NIST Special Publication 800-61 is developed for the information system that defines reportable incidents, outlines a standard operating procedure for incident response (to include actions to protect evidence in support of forensics), provides for user training, and establishes an incident response team. The incident response plan is tested at least [*Assignment: time period (e.g., semi-annually)*]. The test results are used to modify the incident response plan as necessary to ensure effectiveness. **Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.**

### IR-2.e INCIDENT MONITORING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct ongoing monitoring of the information system for security events.

Information system-related security incidents are monitored and tracked until resolved. Information system performance monitoring is used to analyze performance logs in real time (or near-real time) to look for availability problems, including active attacks. Network activity logs for the information system are maintained and reviewed. Collected audit information is reviewed at least [*Assignment: time period that is at least weekly*]; taking advantage of audit reduction and analysis tools to effectively review information for unusual or suspicious activity or violations. Physical access to facilities is monitored and remedial actions taken, as appropriate. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### IR-3.e INCIDENT RESPONSE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively imp lemented to respond to security incidents.

Reports of possible security violations and security incidents are accurate and timely. For security incidents, the organization defines appropriate parameters for response that includes: (i) what information employees must provide; (ii) whom they must notify; and (iii) what degree of urgency to place on reporting. Intrusion detection reports are routinely reviewed and suspected incidents handled accordingly. Records of information system activity, such as security incident tracking reports, are regularly reviewed. Security managers investigate security violations, security incidents, and suspicious activities (e.g., failed logon attempts, other failed access attempts; and questionable activity) and report results to appropriate organization officials. Incident information is reported to one or more of the following organizations: the Federal Computer Incident Response Center, the National Information Protection Center, the U.S. Department of Justice and state and local law enforcement agencies as required. Actions are taken to protect and avoid corrupting potential evidence in support of potential forensics.

In response to reported security violations and security incidents, appropriate actions (including disciplinary actions) are taken by organization officials. Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate. An effective malicious software protection and recovery process is implemented. Information system alerts/advisories are received on a regular basis. Alerts and advisories are issued to personnel and responded to, when appropriate. Incident information and common vulnerability and threat information are shared with owners of connected information systems. **Procedures in-**

**clude checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### IR-4.e HELP DESK

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate incident response by providing a central incident support resource for information system users.

There is a help desk or group that offers advice to users of the information system and plays an appropriate role in the organization's incident response program. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### IR-5.e INTRUSION DETECTION SYSTEMS AND TOOLS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide attack detection capability for the information system.

An effective intrusion detection system (hardware, software, or firmware) is implemented, providing real-time identification of unauthorized use, misuse, and abuse of the information system. The intrusion detection system includes appropriate placement of intrusion detection sensors and definition of incident thresholds. Security controls on the information system can detect unauthorized access attempts. Auditable events (single events and the accumulation of events) that may indicate an imminent violation of security policies are routinely monitored. Selected information system components at critical control points (e.g., servers and firewalls) provide logs of network and system activity. Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain name servers. All significant events, including access to and modifications of information systems, are logged. Intrusion detection system logs contain appropriate information needed for effective review. Access to audit logs is adequately controlled. Virtual private network traffic is visible to network intrusion detection systems. Appropriate organization officials are notified in case of suspicious events. The organization [*Assignment: response (e.g., least disruptive action or a specific action*] to terminate the suspicious events. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### IR-6.e MALICIOUS CODE PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to identify and isolate suspected malicious software (e.g., viruses, worms, etc.).

The information system (including servers, workstations and mobile computing devices) implements malicious code protection that includes a capability for automatic updates. Virus definitions are up-to-date. Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network. Anti-viral mechanisms are used to detect and eradicate viruses in incoming and outgoing e-mail and attachments. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

## OPERATIONAL CONTROLS

**FAMILY:** SECURITY AWARENESS AND TRAINING (AT)

### AT-1.e SECURITY AWARENESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment.

Each information system user is aware of the system security requirements and that user's security responsibilities prior to being authorized access to the system. Security awareness includes continual security awareness training conducted every [*Assignment: time period, typically annually*]. Users have received a copy of or have easy access to: (i) organizational security policies and procedures; and (ii) and rules of behavior for the information system or a user manual containing such rules. All employees fully understand their duties and responsibilities in accordance with their job descriptions as described in NIST Special Publications 800-16 and 800-50. Users understand: (i) the organization's policy for protecting information and information systems (including copyright & proprietary information); (ii) the concept of separation of duty; (iii) the restriction of system access by job positions in key operating and programming activities; (iv) prescribed roles in incident response, configuration management, and continuity of operations; (v) password management (i.e., rules to be followed in creating and changing passwords and the need to keep them confidential); and (vi) the importance of monitoring log in success/failure and how to report discrepancies. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

### AT-2.e SECURITY TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that all personnel with significant information system security responsibilities receive appropriate security training.

The organization identifies all positions and/or roles with significant information system security responsibilities. A security training program consistent with NIST Special Publications 800-16 and 800-50 provides training for individuals within the organization with specific information system security responsibilities. Security training is adjusted to the level of the employee's responsibilities. Employees receive adequate training and have the needed security expertise and skills identified in job descriptions. The employees acknowledge, in writing, having received the security and awareness training. A record of the security subjects covered during training is maintained. Employee training and professional development are documented and monitored. Skill needs are accurately identified and included in job descriptions. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## TECHNICAL CONTROLS

**FAMILY:** IDENTIFICATION AND AUTHENTICATION (IA)

### IA-1.b INDIVIDUAL IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable reliable identification of individual users of the information system.

Identification and authentication mechanisms are implemented that include provisions for uniquely identifying and authenticating entities (i.e., users or information system processes acting on behalf of users). Information system access is gained through the presentation of an individual-identifier (e.g., a unique token or user login ID) and authenticator(s). Any user actions that can be performed prior to reliable identification are explicitly identified (e.g., reading a publicly available web site).

### IA-2.e REMOTE, PRIVILEGED ACCESS AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance authentication for remote access to the information system.

When access to the information system is by a privileged entity (i.e., a user or information system process acting on behalf of a user that possesses authorization to perform system administration or mission processing actions beyond that which average users are allowed to perform) that either resides outside of the system's authorization boundary or whose communications traverse information links (extranets, Internet, phone lines) that are outside of the system's authorization boundary, an identification and authentication mechanism that is resistant to replay attacks is used. **Whenever any user is remotely accessing the information system, an identification and authentication mechanism that is resistant to replay attacks is used. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### IA-3.e PASSWORD PROTECTION MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect passwords from unauthorized disclosure or modification.

For information systems employing password-based authentication, passwords are: (i) one-way encrypted for storage; (ii) transmitted on the network in a secure manner (e.g., encrypted); (iii) not displayed when entered; and (iv) controlled by the associated user. When cryptographic functions are needed, FIPS-140-2 validated cryptography is used. **A FIPS-140-2 validated cryptographic module in an approved operational mode is used for password encryption for transmission. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### IA-4.e PASSWORD LIFE

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords are changed and not reused.

Mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. Passwords are changed at least [*Assignment: time period; typically sixty-ninety days*]. Passwords have a minimum life of [*Assignment: time period (e.g., one day)*]. Passwords are pro-

hibited from reuse for a specified period of [*Assignment: number of generations; typically six*]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**IA-5.e PASSWORD CONTENT**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords comply with policy requirements for content and length.

Mechanisms are implemented to ensure that passwords: (i) contain characters from [*Selection: uppercase alphabetic, lowercase alphabetic, numeric, special characters; typically all four are selected*] with [*Assignment: requirements for how many of the selected types of characters must be included, typically three*]; (ii) have a minimum length of [*Assignment: value, minimum of eight characters*]; (iii) are not the same as the user ID; (iv) are not names or words; (v) are unique for specific individuals; and (vi) are not generic user IDs or passwords. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**IA-6.e PASSWORD-BASED ELECTRONIC SIGNATURES**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure appropriate use of password-based, electronic signatures. (*Related to IA-10 Digital Signatures*)

Password is entered solely for the purpose of indicating intent to sign, is known only by the password owner, and is not exposed to offline attacks by an eavesdropper. The user is advised that use of the password will be construed as a binding legal signature and applications make clear the significance of the act of signing with each signature. Passwords are registered to each user by a secure process that provides clear assurance that the password is associated with the correct individual. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**IA-7.e TOKEN-BASED IDENTIFICATION AND AUTHENTICATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of token-based identification and authentication.

Identification and authentication is accomplished using tokens that may be implemented in software. At a minimum, the authenticator is derived from a FIPS-140-2 approved pseudo random number generator. **Identification and authentication is accomplished using hardware tokens. At a minimum, the authenticator is derived from a FIPS-140-2 approved pseudo random number generator. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**IA-8.e BIOMETRIC-BASED IDENTIFICATION AND AUTHENTICATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of biometrics for identification and authentication.

Identification and authentication is accomplished using biometric devices under the control of the information system. Biometric devices are configured for performance parameters such as number of false positives and number of false negatives and are consistent with information system requirements. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### IA-9.b MUTIFACTOR IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of multiple techniques for user identification and authentication.

Identification and authentication is accomplished using multiple mechanisms such as: (i) biometric reader in conjunction with a password; (ii) biometric reader in conjunction with a token; (iii) multiple, different types of biometric readers; or (iv) multiple, different types of authentication mechanisms other than biometrics.

#### IA-10.e DIGITAL SIGNATURES — MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of digital signatures. (*Related to IA-6 Password Based Electronic Signatures*)

Digital signatures that conform to FIPS 186-3 are used to sign information. Digital signature private keys are not used for any other purpose (e.g., key transport or key agreement), and are not escrowed or purposefully made known to any other party. The key owner is advised that use of the key will be construed as a binding legal signature, and applications make clear the significance of the act of signing with each signature. The application requires a clear separate act to signify the signature (such as clicking on an appropriately labeled box). The system maintains a detailed log of authentications and signatures. The Certification Authority (CA) is cross certified with the Federal Bridge CA at the medium or high level of assurance, or the certificate policy is determined to provide equivalent assurance. **Digital signature private keys are in the sole control of the signer, and are kept on a hardware cryptographic module that is validated at FIPS-140-2 level 2 or higher. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### IA-11.e AUTOMATIC INFORMATION SYSTEM IDENTIFICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable identification of the information system being used or to which a connection is being made.

Automatic information system identification is used to authenticate connections to specific locations and portable information system hardware. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### IA-12.e REMOTE ACCESS IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable higher reliability in the identification and authentication of remote access users.

When remotely accessing via dialup authentication is provided through ID and password encryption for use over public telephone lines. Standard access is provided through a toll-free number and through local telephone numbers to local facilities. **Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user (See IA-7 Token-based Identification and Authentication). It also includes at least one of the following implementation features: (i) biometric identification, (ii) password, (iii) personal identification number (PIN), or (iv) telephone callback procedure. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### IA-13.e UNSUCCESSFUL LOGIN ATTEMPTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to take defined action in the face of multiple unsuccessful login attempts.

For a given user, there is a limit of [*Assignment: number, typically three*] invalid information system access attempts that may occur over [*Assignment: time period (e.g., fifteen minutes)*]. When the maximum number of unsuccessful attempts is exceeded, the information system automatically [*Selection: locks the account/node until released by an administrator, locks the account/node for an* [*Assignment: time period (e.g., fifteen minutes)*], *delays next login prompt according to* [*Assignment: delay algorithm (e.g., the standard Unix algorithm that accomplishes successively longer delays with each subsequent failure)*]]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### IA-14.e IDENTIFIER MANAGEMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user identifiers.

Users of the information system are appropriately identified. Identification is unique to each user. Registration to receive a user identification (ID) is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the user ID is issued to the intended party. Inactive user Ids are disabled after [*Assignment: time period, for example, one year*]. **Multiple, approved forms of individual identification such as documentary evidence or a combination of documents and biometrics are presented to the registration authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### IA-15.e AUTHENTICATOR MANAGEMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user authenticators.

*Public Key Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor, and is done in person before a designated registration authority. Secure procedures ensure that the certificate is issued to the correct, identified party.

*Authenticator Selection, Content, Defaults and Protection*

Selection of passwords or other authentication devices (e.g., tokens, biometrics) is appropriate, based on FIPS Publication 199 security category of the information system. Initial authenticator

content and administrative procedures for initial authenticator distribution are defined. Lost or compromised authenticators are addressed. Default authenticators are changed upon information system installation. Authenticators are protected to preserve confidentiality and integrity. Users maintain possession of their individual tokens, key cards, etc., do not loan or share these items with others, and report lost items immediately.

***Public Key Certificate Registration***

**Multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A biometric, such as a photo or fingerprint is obtained as a part of the registration procedures and retained by the Registration Authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**IA-16.e PASSWORD MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that passwords meet specified requirements.

*Organization-issued Passwords*

Registration to receive a password is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the password is issued to the intended party. Users are instructed as to the proper methods of protecting their passwords.

*Organization-issued and User-determined Passwords*

For information systems employing password-based authentication, passwords are: (i) distributed securely; (ii) controlled by the assigned user and not subject to disclosure; (iii) prohibited from being embedded in programs; (iv) changed periodically every [*Assignment: time period, typically ninety days*]; (v) contain alphanumeric and special characters and are composed of representatives of at least three of the following character sets: upper case English, lower case English, numeric characters, and special characters (information systems with limited information input capabilities implement these measures to the extent possible.); (vi) have a minimum length of [*Assignment: value, minimum of eight characters*]; (vii) prohibited from reuse for a specified period of [*Assignment: number of generations, typically six*]; (viii) have an appropriate minimum life of [*Assignment: length of time, typically one day*]; (ix) not the same as the user ID; and (x) not names or words.

**Multiple, approved forms of individual identification such as documentary evidence or a combination of documents and biometrics are presented to the registration authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## TECHNICAL CONTROLS

**FAMILY:** LOGICAL ACCESS CONTROL (AC)

### AC-1e REMOTE ACCESS RESTRICTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide access protections for remote connections.

There are controls that restrict remote access to the information system.

*Protection of Remote Access - General*

Remote access to organizational information systems always uses encryption to protect the confidentiality of the session. All remote access is mediated through a managed access control point. Information regarding remote access mechanisms (e.g., dial-up connection telephone numbers) is protected.

*Remote Access for Privileged Functions*

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to general security measures for remote access, additional protections such as a virtual private network with blocking mode enabled are implemented.

*Collaborative Computing*

Collaborative computing mechanisms are not remotely activated. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop is required to take an explicit action to turn on the camera and microphone, remote users are not allowed to activate a user's camera or microphone remotely). Peer-to-peer collaborative computing mechanisms between information systems ensure that only the information on the screen is observable to the remote user. Information located elsewhere on the workstation is not observable. The remote user is not able to modify or delete any information on the workstation. These restrictions also apply to any other information system to which the user's workstation is logically connected (e.g., any logically mounted disks). Collaborative computing mechanisms that provide video and/or audio conference capabilities provide some explicit indication that the video and audio mechanisms are operating.

*Public Access Information Systems*

For public access information systems, there are mechanisms implemented to protect the integrity of the information, the application, and the underlying system. These controls are resilient in the face of publicly known attacks.

*Dial-In Access to Information Systems*

Dial-in access to the information system is controlled and monitored. Mechanisms are implemented to limit the access achieved through dial-up, in accordance with organizational policy.

*Remote Terminal Access*

Where enforcement of information system security policy requires, mechanisms are implemented to restrict access through specific workstations or terminals.

**Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### AC-2e LOGON NOTIFICATION MESSAGE

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide users with information about previous logons both successful and unsuccessful.

Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user's last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon. A warning/notification message is displayed upon successful logon and before gaining system access. This message: (i) is approved and standardized; (ii) remains on the screen until explicit user action to remove it; (iii) warns all users that they have accessed a U.S. Government information system; (iv) provides appropriate privacy and security notices; (v) notifies the user that system usage may be monitored, recorded, and subject to audit; and (vi) notifies the user that use of the information system indicates (a) the consent of the user to such monitoring and recording and (b) that unauthorized use is prohibited and subject to criminal and civil penalties. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### AC-3.e CONCURRENT SESSION CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable control of the number of concurrent sessions on the information system for a given user.

If the information system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. The maximum number of concurrent sessions for any user is [*Assignment: number; (e.g., three)*]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### AC-4.e SESSION LOCK

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable user-commanded locking of the information system session.

Session-lock functionality is associated with each information system node (e.g., terminal, workstation, notebook computer). Upon user activation, a session-lock function prevents access to the node or to any session information. Once the session-lock is activated, access to the node requires knowledge of a unique authenticator. Session-lock is not a substitute for logging out. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### AC-5.e SESSION INACTIVITY

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable enforcement of defined actions in the event of session inactivity.

The information system detects [*Assignment: time period (e.g., fifteen minutes)*] of inactivity and blocks further access until the user reestablishes the connection using the proper identification and authentication procedures. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

#### AC-6.e LIMITED CONNECTION TIME

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to limit the length of time given types of connections can be maintained.

Mechanisms are implemented to limit the length of time a defined set of connections can be established. The defined set is: (i) [*Assignment: connection description/length of time*]; and (ii) [*Assignment: additional connection description/length of time*]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### AC-7.e AUTOMATED MARKING AND LABELING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to mark output and label information in storage, in process, and in transmission.

Information systems that store, process, transmit, or display information in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in Federal policy and guidance documents. Markings and labels clearly reflect any special dissemination, handling, or distribution instructions. Internal security labels are an integral part of the electronic information or media. A means is provided for the information system to ensure that the labels a user associates with information provided to the system are consistent with the information that the user is allowed to access. Internal security labels and markings implement standard naming conventions. Documentation is maintained regarding the kind(s) of information allowed on each communications channel within the information system. **Automated marking mechanisms to ensure that either the user or the information system marks all information output from the system. Markings are retained with the information. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### AC-8.e AUTHORIZATION MANAGEMENT MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective assignment and management of access authorizations.

Authorization management mechanisms are implemented that effectively support the following access control capabilities: (i) [*Selection: one or more types of access control: role-based, identity-based*]; and (ii) [*Selection: one or more types of access control: discretionary, non-discretionary*]. Whenever the information system provides for disclosure of information deemed critical/sensitive by the organization (in accordance with FIPS Publication 199), an authorization mechanism is employed to query and receive consent for the disclosure of such information. The information system provides the capability for users (or processes acting on behalf of users) to determine the access authorizations granted to another user or to a communications channel. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### AC-9.e ENFORCEMENT MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce the assigned authorizations for access to information or the information system and for controlling the flow of information.

Information system access enforcement mechanisms (capable of including or excluding access to the granularity of a single user or user-role) enforce the assigned resource authorizations for each attempted access to information or information system. Information flow control enforcement mechanisms provide the granularity of information description and of source and destination description to adequately implement organizational policy.

*For discretionary access control enforcement*

Access is controlled between named users (or processes) and named objects (e.g., files and programs) in the information system. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest, encryption) allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and provide controls to limit propagation of access rights. The enforcement mechanisms, either by explicit user action or by default, protect objects from unauthorized access. These access controls are capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission is only assigned by authorized users.

*For non-discretionary access control enforcement*

A non-discretionary access control policy is enforced over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects are assigned labels (implicitly or explicitly) that combine hierarchical levels and non-hierarchical categories; the labels are used as the basis for non-discretionary access control decisions.

*For flow control enforcement*

A flow control policy is enforced over information flows under its control. Information and source and destination objects may be assigned labels (implicitly or explicitly) that are used as the basis for non-discretionary flow control decisions. Additionally, flow control rules (e.g.,, router rules) may be used to enforce information flow policy both discretionary and non-discretionary.

**Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**AC-10.e AUTOMATED ACCOUNT CONTROLS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to manage inactive and special accounts.

Emergency or temporary accounts are automatically terminated after [*Assignment: time period (e.g., thirty days)*]. Inactive accounts are automatically disabled after [*Assignment: time period (e.g., six months)*]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**AC-11.e LEAST PRIVILEGE AND SEPARATION OF DUTIES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to separate duties among individuals within the organization and limit authorizations to the minimum necessary to fulfill assigned duties.

*Least Privilege*

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

*Separation of Duties*

The principle of separation of duties is enforced. Mission functions and distinct information system support functions are divided among different individuals and are performed by different individuals. Access authorizations are periodically reviewed for functions that should be separated to enhance security. Duties that should be separated to enhance security have been identified (e.g., security personnel who administer access control functions should not be those who administer the audit functions on the information system). Information system support functions are performed by different individuals (e.g., functions such system management, system design, application programming, systems programming, quality assurance/testing, library management/change man-

agement, computer operations, production control and scheduling, network security, database administration, network administration). As necessary to enhance security, mission-processing functions are distributed among different individuals. Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### AC-12.e SUPERVISION AND REVIEW — ACCESS CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to supervise personnel and review their actions with respect to enforcement of access controls.

Personnel (those enforcing controls and those who the controls are restricting) are provided adequate supervision and review, including each shift for computer operations. Supervisors routinely review user activity logs for inappropriate actions and investigate any abnormalities. Changes to security access authorizations are logged and periodically reviewed by appropriate organization officials independent of the security function. Unusual activity is investigated. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### AC-13.e NON-DISCRETIONARY ACCESS CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enable enforcement of non-discretionary access requirements.

Non-discretionary access requirements are identified and appropriate authorizations implemented to enable the enforcement of these access requirements. Examples of non-discretionary requirements are: (i) limitations on release of private information; (ii) limitations on release of export-controlled information; and (iii) limitations on public release of information. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

#### AC-14.e AUTHORIZATION PROCEDURES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system authorizations.

Rules are in place for: (i) granting of access authorizations; (ii) determining initial rights of access to a terminal, transaction, program, process, or information; and (iii) determining the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process or information.

*Granting of Access Rights*

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict assess that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

*Review of Access Rights*

Information system owners periodically review access authorizations for continuing appropriateness. Security managers review access authorizations and discuss any questionable authorizations

with information system owners. Access to the information system is authorized only to individuals who: (i) have a valid need-to-know that is demonstrated by assigned official duties and satisfying of all personnel security criteria; or (ii) are otherwise to be granted access based upon intended system usage (e.g., a publicly accessible web site).

*Authorization Definitions*

Authorizations are defined and managed for: (i) mission-specific processing; (ii) program source library; (iii) system resources; (iv) support/technology management systems and/or tools; (v) system libraries; (vi) access to passwords/authentication services and directories; (vii) access authorizations for maintainers of information system resources, including those that are at remote locations; (viii) users who can dial into the information system from remote locations; and (ix) default permissions and rights.

*Miscellaneous*

Standardized naming conventions are used for information system components. Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, scratch, and rename a file. Employees are discouraged from browsing files by making it clear that organizational policy prohibits it. Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**AC-15.e SYSTEM ACCOUNT MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system accounts.

Comprehensive account management ensures that only authorized users can gain access to information systems. Account management includes: (i) identifying types of accounts (individual and group, conditions for group membership, associated privileges); (ii) establishing an account (i.e., required identification, approval, and documentation procedures); (iii) activating an account; (iv) modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators); and (v) terminating an account.

*All Accounts*

Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain information system access. The account manager is notified in a timely manner when information system users are terminated or transferred. Unnecessary accounts (defaults, guest accounts) are removed, disabled, or otherwise secured. Inactive accounts and accounts for terminated individuals are disabled or removed on a timely basis.

*Guest and Anonymous Accounts*

Guest and anonymous accounts on the information system are specifically authorized and monitored. Emergency or temporary accounts are appropriately controlled, including: (i) documented, approved by appropriate organization officials; (ii) securely communicated to the appropriate personnel; and (iii) automatically terminated after a predetermined period with a default of [*Assignment: time period (e.g., thirty days)*].

***Privileged Accounts***

**All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). Privileged role assignments are tracked. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## TECHNICAL CONTROLS

**FAMILY:** ACCOUNTABILITY (INCLUDING AUDIT TRAILS) (AU)

### AU-1.b USER ASSOCIATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the association of an individual user with the actions taken by that user.

Mechanisms are implemented to associate actions taken or attempted in the information system with the specific user responsible for that action.

### AU-2.b CONTENT OF AUDIT RECORDS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to include specified information in audit records.

The audit trail includes sufficient information to establish what events occurred and who or what caused the events. For each security-relevant auditable event (as specified in AU-3), the audit record contains at least the following information: (i) date and time of the event; (ii) information system locale of the event; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

*For Information Release Actions*

Include: (i) identity of releaser; (ii) identity of recipient; (iii) identity of information released; (iv) device identifier (id) (e.g., port ID); (v) time and date of release; and (vi) modification or application of security labels.

*For Information Communications Actions*

Include: (i) identity of sender (e.g., person, information system); (ii) identity of recipient (e.g., IP address, host and user); device ID (e.g., port ID); and (iii) time and date of communication.

The following additional audit information is provided: [*Assignment: list of other information that the information system is able to include in the audit records*].

### AU-3.b AUDITABLE EVENTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to generate an audit record for at least a defined set of events.

The information system audit mechanisms are capable of generating an audit record for each of the following events: (i) start-up and shutdown of the audit functions; (ii) successful and unsuccessful logons and logoffs; (iii) successful and unsuccessful attempts to access security relevant files and utilities including user authentication information; (iv) operations performed to read, modify or destroy the audit information; (v) modifications to the audit configuration that occur while the audit functions are operating; (vi) actions taken due to exceeding of a threshold or audit storage failure; (vii) unsuccessful use of the user identification or authentication mechanisms including the identity provided; (viii) unsuccessful revocations of security attributes; (ix) modifications to the group of users that are part of a role; (x) key recovery requests and associated responses including who made the request and when; (xi) changes to the time; (xii) denial of access resulting from an excessive number of logon attempts; (xiii) blocking or blacklisting a user ID, terminal, or access port and the reason for the action; (xiv) detected replay attacks; (xv) rejections of new sessions based upon any limitation on the number of concurrent sessions; (xvi) other activities that modify, bypass, or negate security controls within the information system; (xvii) use of compilers, and (xviii) use of privileged accounts.

All accesses to information system software files are logged by automated logging facilities. Installation of all system software is logged to establish an audit trail/log and is reviewed by management. The use of system utilities is logged using access control software reports or job accounting information. Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users are logged.

*Mission-specific Processing Activity*

For example: (i) all transactions are logged as entered, along with the user ID of the individual entering the information; and (ii) overriding or bypassing information validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

*Non-discretionary Access Control Events*

For example: (i) attempts to cause information flows contrary to policy; (ii) changes to user formal access permissions; (iii) changes in security labels; (iv) accesses or attempted accesses to objects or information whose labels are inconsistent with user privileges; (v) information downgrades and overrides; and (vi) identified events that may be used in the exploitation of covert channels.

The following additional events generate an audit record: [*Assignment: list of additional events*].

**AU-4.e AUDIT PROCESSING**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable meeting specified requirements for the audit system.

CONTROL MAPPING: [NIST 800-26: 17.1.4; ISO-17799: 9.73; CMS: 2.1.2; DOD 8500: ECTP-1]

Information system clocks are synchronized for accurate reading of auditable events. In the event of an audit failure or full audit trail, [*Assignment: action to be taken (e.g., shutdown information system, overwrite oldest audit records, or stop generating audit records)*]. Online audit information from the information system is protected against unauthorized access, modification or deletion. Access to information system audit tools is protected to prevent possible misuse or compromise. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**AU-5.b AUDIT REDUCTION AND REPORT GENERATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective human review of audit information and the generation of appropriate audit reports.

Tools are available for the review of audit records and for report generation from audit records. Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents.

**AU-6.e NON-REPUDIATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against later claims by sender to not have transmitted a message or a receiver to not have received a message.

Mechanisms are implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these**

**checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

## TECHNICAL CONTROLS

**FAMILY:** SYSTEM AND COMMUNICATIONS PROTECTION (SP)

### SP-1.e APPLICATION PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to isolate user interfaces from information system management functionality.

User interface services (e.g., web services) are physically or logically separated from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### SP-2.e INFORMATION SYSTEM PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to separate security-relevant functionality from other information system functionality.

Information system security functions are isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system maintains a separate execution domain (e.g., address space) for each executing process. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### SP-3.b INFORMATION REMNANTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against unauthorized information transfer via shared information system resources.

No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) is available to any current user (or current process) that obtains access to a shared system resource that has been released back to the information system. There is no residual information from the shared resource.

### SP-4.e DENIAL OF SERVICE PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to specifically protect against denial of service attacks.

Mechanisms are in place to curtail or prevent well known, detectable, and preventable denial of service attacks. The attacks to be prevented are [*Assignment: list of attacks or pointer to source for current list*]. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### SP-5.e RESOURCE PRIORITY

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to limit use of information system resources by priority and by quota.

Mechanisms are implemented to provide for allocation of information system resources based upon priority and upon a quota. Mechanisms are implemented to enforce the information system resource allocations as appropriate for meeting system security needs.. Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

### SP-6.e BOUNDARY PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to proxy, screen, or filter communications at the authorization boundary of the information system.

*Boundary Protection Devices*

Protection mechanisms are implemented at the information system boundary and at layered or internal system boundaries, including, as appropriate, firewalls, gateways, proxies, routers and network intrusion detection systems.

*Protection Capabilities*

Controlled Release: Only traffic that is explicitly permitted (based on traffic review) is released from the boundary of the interconnected information system.

Encryption: Outgoing communication (including the body and attachment of the communication) are encrypted using FIPS 140-2 validated cryptography, as needed, with the appropriate level of encryption for the information, transmission medium, and destination information system.

Fail-secure: The operational failure of the boundary protection for the information system does not result in any unauthorized release of information outside of the system boundary. In the event of an operational failure of the boundary protection, no information external to the interconnected information system enters the information system.

The boundary protection of the information system is at least as strong as the boundary protection of the information system into which the information flows are directed.

Delivery: Incoming communications have an authorized user (and, as applicable, authorized addresses) as a destination.

Filtering: Communications protocols/services from outside the boundary of the interconnected information system are supported and filtered as appropriate to comply with security policy (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications).

Proxies: Protocol-mediation software (i.e., proxies) that is able to understand and take protective action based on application-level protocols and associated data streams (e.g., filtering FTP connections to deny the use of the *put* command, effectively prohibiting the ability to write to an anonymous FTP server) are supported by the information system, as appropriate.

Extensibility: Security support for the incorporation of additional system services (as they become available) is provided, where appropriate.

Platform Protection Requirements: The platform underlying the boundary protection mechanisms must be able to isolate and protect the boundary protection applications.

Information system nodes (e.g., workstations, notebook computers) with dial-up access generate a unique identifier code before connection to the information system is completed.

Non-discretionary policy enforcement: Required capability to implement policy when policy restricts information flows between information systems connected by the boundary protection de-

vice(s) and either of the systems is not considered trustworthy enough to maintain only allowed flows.

*Alternate Processing Site*

Information system boundary protections at the designated alternate site provide the same levels of protection as that of the primary site.

**Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SP-7.e NETWORK SEGREGATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable segregation of functionality and communications.

Information system boundary hosts are appropriately isolated through controls such as segregation from the internal network. External servers are located external to a site's boundary protection (e.g., firewall) or are on a network separate from the site's intranet. All Internet access is through Internet access points that are under the management and control of the information system owner or organization and meets the organizational requirement that such contacts are isolated from other organization information systems by physical or technical means. Any connection to the Internet, or other external networks or information systems, occurs through a proxy, gateway, or firewall. Public wide area network connections between the organizational information systems and the Internet or other public or commercial wide area networks require an information protection network (IPN) that acts as the single point of entry into the site and defends the information system boundary or external connection(s). **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SP-8.e TRANSMISSION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect the integrity of information being transmitted.

Mechanisms are implemented to enable verification of the contents of a message to determine whether the contents have been changed in transit. Engineering practices such as parity checks and cyclical redundancy checks with respect to the integrity mechanisms of commercial off-the-shelf, government off-the-shelf, and custom developed solutions are implemented for incoming and outgoing information. Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of communication sessions. **Information is transmitted with FIPS Publication 140-2 validated cryptographic integrity controls such as message authentication codes (e.g., FIPS Publication 198 HMAC) or digital signatures (FIPS Publication 186-3) that ensure the authenticity and integrity of information and prevent hijacking of communications sessions. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SP-9.e NETWORK DISCONNECT**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that inactive network connections are terminated.

The network connection automatically disconnects at the end of a session or after being inactive for [*Assignment: time period (e.g., thirty minutes)*]. Where connectivity is not continuous, network connection automatically disconnects at the end of a session. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SP-10.e INFORMATION TRANSMISSION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide for the security of transmitted information.

Where information confidentiality is required, information transmission implements at least one of the following: (i) information is transmitted only within an area approved for open storage of the information; (ii) information is transmitted via a protected distribution system; or (iii) information is transmitted using FIPS Publication 140-2 validated encryption. Dial-up lines, other than those that are protected with FIPS Publication 140-2 validated cryptography or protected distribution systems, are not used for gaining access to information system resources that process organizational information without specific written authorization for the system to operate in this manner. Mechanisms are implemented to detect or prevent the hijacking of a communication session (e.g., encrypted communication channels). Information transmissions of different FIPS Publication 199 security categories (for confidentiality) are segregated from each other (e.g., using encryption, physical separation). Security parameters (e.g., labels, markings) are reliably associated (either explicitly or implicitly) with information exchanged between information systems. **Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.**

**SP-11.b TRUSTED PATH**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable communication with security functionality between a user and the information system.

A trusted communications path between the user and the security functionality of the system for login and authentication is implemented and supported. Communication via this trusted path is initiated exclusively by the user and is unmistakably distinguishable from other paths. In the case of communication between two or more information systems (e.g. client server architecture), bi-directional authentication between the two systems is implemented.

**SP-13.e CRYPTOGRAPHIC KEY MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage cryptographic keys.

When encryption is used, documented procedures are being effectively implemented for key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect organizational information are generated in FIPS Publication 140-2 validated cryptographic modules and controlled and distributed using NIST-approved key management guidance. 128, 192, or 256-bit Advanced Encryption Standard (AES) encryption is used, with key agreement or key transport corresponding to the strength of the asymmetric key algorithms (See NIST key management guidance). Asymmetric keys are produced, controlled and distributed using an organization

certificate authority (CA) cross-certified with the Federal Bridge CA at a level of medium or high or pre-placed keying material. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**SP-14.e KEY ARCHIVE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to archive keying material for encrypted information.

Keying material needed to recover encrypted stored information is archived in the custody of a designated key recovery custodian and is stored securely. Keys are stored so that an intruder who steals the encrypted information does not obtain the keying material needed to decrypt the information. **Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**SP-15.e PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance the effectiveness of public key infrastructure.

All public key certificates used in the information system are issued in accordance with a defined certificate policy and certification practice statement.

*Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done **in person** by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. **Multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A secure process ensures that the certificate is issued to the correct, identified party. A biometric, such as a photo or fingerprint is obtained as a part of the registration process and retained by the Registration Authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

**SP-16.e USE OF ENCRYPTION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that when encryption is used, Federal policy requirements are met, to include use of FIPS Publication 140-2 validated cryptography.

*Information at Rest (Encryption for confidentiality)*

When information on the information system is encrypted for confidentiality during storage, it is encrypted with FIPS Publication 140-2 validated cryptography.

*Information in Transit (Encryption for Confidentiality)*

Organizational information that is transmitted through a commercial or wireless network and kept confidential via encryption is encrypted using 128, 192, or 256-bit Advanced Encryption Standard (AES) implemented in FIPS Publication 140-2-validated cryptographic modules.

*Information in Transit (Encryption for Need-To-Know)*

Information in transit through a network at the same FIPS Publication 199 security category (for confidentiality), but which is kept separate for need-to-know reasons via encryption, is encrypted with FIPS Publication 140-2 validated cryptography.

*Non-repudiation*

FIPS Publication 140-2 validated cryptography (e.g., DOD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS Publication 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards are applied as they become available.

**Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.**

## APPENDIX H

# BASELINE SECURITY CONTROLS – HIGH

FIPS PUBLICATION 199 SECURITY CATEGORIZATION—HIGH IMPACT

Note: Reviewers will notice that the security controls for the high baseline (i.e., those controls for the protection of information systems designated as FIPS Publication 199 security category of high) have not been identified in the first public draft of Special Publication 800-53. These security controls will be provided in subsequent drafts of this special publication. The breadth and depth of the security controls required to protect the most critical/sensitive information systems within the Federal government is substantial. The selection of appropriate security controls for the three baselines in moving from low to moderate to high does not increase in a linear manner, but rather exponentially. Thus, for the high baseline, the number of security controls will increase significantly as will the content of the associated controls (i.e., control robustness). Based on the final selection of security controls for the high baseline, an estimated threat coverage will be determined. NIST plans to hold a public workshop on March 8, 2004 in Gaithersburg, MD, to address the issues associated with constructing the security controls for the high baseline as well as the development of appropriate security controls for that baseline. Obtaining feedback from the first public comment period on Special Publication 800-53 (specifically on the technical content and applicability of the security controls in the catalog) is a prerequisite for taking on this next important task in security control development. Consult http://csrc.nist.gov/sec-cert for additional details on the upcoming workshop.

## APPENDIX I

# BASELINE SECURITY CONTROLS – SUMMARY

SECURITY CONTROLS FOR LOW, MODERATE, AND HIGH IMPACT LEVELS

| CONTROL NO. | CONTROL NAME | *SECURITY CONTROL BASELINES* | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| | **MANAGEMENT CONTROLS** | | | |
| RA-1 | Security Categorization | RA-1.b | RA-1.e | TBD |
| RA-2 | Risk Assessment | RA-2.b | RA-2.e | TBD |
| PL-1 | Security Rules of Behavior and Acceptable Use | PL-1.b | PL-1.b | TBD |
| PL-2 | Access Control Policy | PL-2.b | PL-2.b | TBD |
| PL-3 | Group Identification and Authentication Policy | PL-3.b | PL-3.b | TBD |
| PL-4 | Information Flow Control Policy | --- | PL-4.b | TBD |
| PL-5 | Accountability Policy | PL-5.b | PL-5.b | TBD |
| PL-6 | Contingency Planning and Operations Policy | PL-6.b | PL-6.b | TBD |
| PL-7 | Configuration Management Policy | PL-7.b | PL-7.b | TBD |
| PL-8 | Incident Response Policy | PL-8.b | PL-8.b | TBD |
| PL-9 | Security Awareness and Training Policy | PL-9.b | PL-9.b | TBD |
| PL-10 | Physical and Environmental Protection Policy | PL-10.b | PL-10.b | TBD |
| PL-11 | Personnel Security Policy | PL-11.b | PL-11.b | TBD |
| PL-12 | Media Protection Policy | PL-12.b | PL-12.b | TBD |
| PL-13 | System Maintenance Policy | PL-13.b | PL-13.b | TBD |
| PL-14 | Security Planning | PL-14.b | PL-14.e | TBD |
| PL-15 | Standards for Security Test / Evaluation Plans | --- | PL-15.b | TBD |
| SA-1 | Acquisition Process | SA-1.b | SA-1.e | TBD |
| SA-2 | Copyrighted and Public Domain Works | SA-2.b | SA-2.e | TBD |
| SA-3 | System Documentation | SA-3.b | SA-3.e | TBD |
| SA-4 | Outsourced Information System Services | SA-4.b | SA-4.e | TBD |
| SA-5 | Developer Functional Testing | --- | SA-5.e | TBD |
| SA-6 | Life Cycle Support | --- | SA-6.e | TBD |
| SA-7 | Security Design Disciplines | --- | SA-7.b | TBD |
| SA-8 | Security Policy Model | --- | SA-8.b | TBD |
| CR-1 | Information System Assessment | CR-1.b | CR-1.e | TBD |
| CR-2 | Vulnerability Scanning | CR-2.b | CR-2.e | TBD |
| CR-3 | Vulnerability Assessment / Penetration Testing | --- | CR-3.b | TBD |
| PA-1 | Authorize Information System Connections | PA-1.b | PA-1.e | TBD |
| PA-2 | Authorize Mobile Code | PA-2.b | PA-2.e | TBD |

**TABLE 7: SUMMARY OF BASELINE SECURITY CONTROLS**

| CONTROL NO. | CONTROL NAME | *SECURITY CONTROL BASELINES* | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| PA-3 | Authorize Remote Access Connections | PA-3.b | PA-3.e | TBD |
| PA-4 | Authorize Collaborative Computing | PA-4.b | PA-4.e | TBD |
| PA-5 | Authorize Wireless Access Point | PA-5.b | PA-5.e | TBD |
| PA-6 | Authorize Information System Operation | PA-6.b | PA-6.e | TBD |
| | **OPERATIONAL CONTROLS** | | | |
| PS-1 | Position Review | PS-1.b | PS-1.e | TBD |
| PS-2 | Personnel Screening | PS-2.b | PS-2.e | TBD |
| PS-3 | Termination and Transfer | PS-3.b | PS-3.e | TBD |
| PS-4 | Third Party Personnel Security | PS-4.b | PS-4.e | TBD |
| PE-1 | Identify Sensitive Facilities / Restricted Areas | PE-1.b | PE-1.e | TBD |
| PE-2 | Authorize Physical Access | PE-2.b | PE-2.e | TBD |
| PE-3 | Physical Access Enforcement | PE-3.b | PE-3.e | TBD |
| PE-4 | Access Monitoring | --- | PE-4.e | TBD |
| PE-5 | Visitor Control | PE-5.b | PE-5.e | TBD |
| PE-6 | Physical Access to Transmission Medium | --- | PE-6.e | TBD |
| PE-7 | Routine Physical Security Checking | PE-7.b | PE-7.e | TBD |
| PE-8 | Physical Security Testing | --- | --- | TBD |
| PE-9 | Storage | PE-9.b | PE-9.e | TBD |
| PE-10 | Access Devices | PE-10.b | PE-10.e | TBD |
| PE-11 | Physical Security Containers | --- | PE-11.b | TBD |
| PE-12 | Identify Natural Disruption / Disaster Protection | PE-12.b | PE-12.e | TBD |
| PE-13 | Plumbing Lines | PE-13.b | PE-13.e | TBD |
| PE-14 | Emergency Lighting | PE-14.b | PE-14.e | TBD |
| PE-15 | Fire Protection | PE-15.b | PE-15.e | TBD |
| PE-16 | Temperature Controls | PE-16.b | PE-16.e | TBD |
| PE-17 | Power | PE-17.b | PE-17.e | TBD |
| PE-18 | Power Supply | --- | PE-18.b | TBD |
| PE-19 | Environmental Control Testing | --- | PE-19.e | TBD |
| PE-20 | Environmental Control Training | PE-20.b | PE-20.e | TBD |
| PE-21 | Equipment Delivery and Removal | PE-21.b | PE-21.e | TBD |
| PE-22 | Separate Facilities | --- | PE-22.e | TBD |
| PE-23 | Alternate Work Site | --- | PE-23.b | TBD |
| CP-1 | Contingency Plan | CP-1.b | CP-1.e | TBD |
| CP-2 | Contingency Plan Training | CP-2.b | CP-2.e | TBD |
| CP-3 | Contingency Plan Exercises and Drills | CP-3.b | CP-3.b | TBD |
| CP-4 | Contingency Plan Storage | CP-4.b | CP-4.e | TBD |

**TABLE 7: SUMMARY OF BASELINE SECURITY CONTROLS**

| CONTROL NO. | CONTROL NAME | *SECURITY CONTROL BASELINES* | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| CP-5 | Off-Site Backup Storage Sites | CP-5.b | CP-5.b | TBD |
| CP-6 | Information Backup and Restore | CP-6.b | CP-6.e | TBD |
| CP-7 | Backup Mechanisms | CP-7.b | CP-7.e | TBD |
| CP-8 | Alternate Processing Site | --- | CP-8.b | TBD |
| CP-9 | Restoring Information – Emergency Conditions | CP-9.b | CP-9.e | TBD |
| CP-10 | Information System Recovery | CP-10.b | CP-10.e | TBD |
| CP-11 | Management Accountability | CP-11.b | CP-11.b | TBD |
| CP-12 | Information System Modification Impact | --- | CP-12.e | TBD |
| CP-13 | Alternate Communication Services | CP-13.b | CP-13.b | TBD |
| CM-1 | Configuration Management Plan | CM-1.b | CM-1.e | TBD |
| CM-2 | Configuration Management Process | CM-2.b | CM-2.e | TBD |
| CM-3 | Baseline Configuration | CM-3.b | CM-3.e | TBD |
| CM-4 | Change Control | CM-4.b | CM-4.e | TBD |
| CM-5 | Library Management | --- | CM-5.e | TBD |
| CM-6 | Change Access Control | CM-6.b | CM-6.e | TBD |
| CM-7 | Monitoring Change Activity | CM-7.b | CM-7.e | TBD |
| CM-8 | Minimal Services | CM-8.b | CM-8.e | TBD |
| CM-9 | Secure Configuration Settings | CM-9.b | CM-9.e | TBD |
| CM-10 | Network Configuration Settings | CM-10.b | CM-10.e | TBD |
| CM-11 | Privacy Policy | CM-11.b | CM-11.e | TBD |
| CM-12 | Limiting Traffic Types | CM-12.b | CM-12.e | TBD |
| MA-1 | Periodic Maintenance | MA-1.b | MA-1.e | TBD |
| MA-2 | Maintenance Tools | --- | MA-2.e | TBD |
| MA-3 | Remote Maintenance | MA-3.b | MA-3.e | TBD |
| MA-4 | Maintenance Personnel | MA-4.b | MA-4.e | TBD |
| MA-5 | Timely Maintenance | MA-5.b | MA-5.b | TBD |
| MA-6 | Maintenance Scheduling | --- | MA-6.e | TBD |
| SI-1 | Flaw Remediation Process | SI-1.b | SI-1.e | TBD |
| SI-2 | Personnel Supervision | --- | SI-2.b | TBD |
| SI-3 | Procedural Review | SI-3.b | SI-3.b | TBD |
| SI-4 | Software and Information Integrity | SI-4.b | SI-4.e | TBD |
| SI-5 | Validation of Mission Processing | --- | SI-5.e | TBD |
| SI-6 | System Operation Integrity | --- | SI-6.b | TBD |
| MP-1 | Media Access | MP-1.b | MP-1.e | TBD |
| MP-2 | Labeling | --- | MP-2.b | TBD |

**TABLE 7: SUMMARY OF BASELINE SECURITY CONTROLS**

| CONTROL NO. | CONTROL NAME | *SECURITY CONTROL BASELINES* | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| MP-3 | Media Transport | --- | MP-3.e | TBD |
| MP-4 | Media Destruction and Disposal | MP-4.b | MP-4.e | TBD |
| MP-5 | Media Sanitization and Clearing | --- | MP-5.e | TBD |
| MP-6 | Media-related Records | MP-6.b | MP-6.e | TBD |
| MP-7 | Media Storage | MP-7.b | MP-7.e | TBD |
| IR-1 | Incidence Response Plan | IR-1.b | IR-1.e | TBD |
| IR-2 | Incident Monitoring | IR-2.b | IR-2.e | TBD |
| IR-3 | Incident Response | IR-3.b | IR-3.e | TBD |
| IR-4 | Help Desk | IR-4.b | IR-4.e | TBD |
| IR-5 | Intrusion Detection Systems and Tools | IR-5.b | IR-5.e | TBD |
| IR-6 | Malicious Code Protection | IR-6.b | IR-6.e | TBD |
| AT-1 | Security Awareness | AT-1.b | AT-1.e | TBD |
| AT-2 | Security Training | AT-2.b | AT-2.e | TBD |
| | **TECHNICAL CONTROLS** | | | |
| IA-1 | Individual Identification / Authentication | IA-1.b | IA-1.b | TBD |
| IA-2 | Remote, Privileged Access Authentication | --- | IA-2.e | TBD |
| IA-3 | Password Protection Mechanisms | IA-3.b | IA-3.e | TBD |
| IA-4 | Password Life | IA-4.b | IA-4.e | TBD |
| IA-5 | Password Content | IA-5.b | IA-5.e | TBD |
| IA-6 | Password-based Electronic Signatures | IA-6.b | IA-6.e | TBD |
| IA-7 | Token-based Identification / Authentication | --- | IA-7.e | TBD |
| IA-8 | Biometric-based Identification / Authentication | --- | IA-8.e | TBD |
| IA-9 | Multifactor Identification / Authentication | --- | IA-9.b | TBD |
| IA-10 | Digital Signatures—Mechanisms | --- | IA-10.e | TBD |
| IA-11 | Automatic Information System Identification | IA-11.b | IA-11.e | TBD |
| IA-12 | Remote Access Identification / Authentication | --- | IA-12.e | TBD |
| IA-13 | Unsuccessful Login Attempts | IA-13.b | IA-13.e | TBD |
| IA-14 | Identifier Management | IA-14.b | IA-14.e | TBD |
| IA-15 | Authenticator Management | IA-15.b | IA-15.e | TBD |
| IA-16 | Password Management | IA-16.b | IA-16.e | TBD |
| AC-1 | Remote Access Restrictions | AC-1.b | AC-1.e | TBD |
| AC-2 | Logon Notification Message | AC-2.b | AC-2.e | TBD |
| AC-3 | Concurrent Session Control | --- | AC-3.e | TBD |
| AC-4 | Session Lock | AC-4.b | AC-4.e | TBD |
| AC-5 | Session Inactivity | AC-5.b | AC-5.e | TBD |
| AC-6 | Limited Connection Time | --- | AC-6.e | TBD |

**TABLE 7: SUMMARY OF BASELINE SECURITY CONTROLS**

| CONTROL NO. | CONTROL NAME | *SECURITY CONTROL BASELINES* | | |
|---|---|---|---|---|
| | | Low | Moderate | High |
| AC-7 | Automatic Marking and Labeling | --- | AC-7.e | TBD |
| AC-8 | Authorization Management Mechanisms | AC-8.b | AC-8.e | TBD |
| AC-9 | Enforcement Mechanisms | AC-9.b | AC-9.e | TBD |
| AC-10 | Automated Account Controls | AC-10.b | AC-10.e | TBD |
| AC-11 | Least Privilege and Separation of Duties | AC-11.b | AC-11.e | TBD |
| AC-12 | Supervision and Review—Access Control | AC-12.b | AC-12.e | TBD |
| AC-13 | Non-discretionary Access Control | AC-13.b | AC-13.e | TBD |
| AC-14 | Authorization Procedures | AC-14.b | AC-14.e | TBD |
| AC-15 | System Account Management | AC-15.b | AC-15.e | TBD |
| AU-1 | User Association | AU-1.b | AU-1.b | TBD |
| AU-2 | Content of Audit Records | AU-2.b | AU-2.b | TBD |
| AU-3 | Auditable Events | AU-3.b | AU-3.b | TBD |
| AU-4 | Audit Processing | AU-4.b | AU-4.e | TBD |
| AU-5 | Audit Reduction and Report Generation | AU-5.b | AU-5.b | TBD |
| AU-6 | Non-Repudiation | AU-6.b | AU-6.e | TBD |
| SP-1 | Application Partitioning | SP-1.b | SP-1.e | TBD |
| SP-2 | Information System Partitioning | SP-2.b | SP-2.e | TBD |
| SP-3 | Information Remnants | SP-3.b | SP-3.b | TBD |
| SP-4 | Denial of Service Protection | SP-4.b | SP-4.e | TBD |
| SP-5 | Resource Priority | SP-5.b | SP-5.e | TBD |
| SP-6 | Boundary Protection | SP-6.b | SP-6.e | TBD |
| SP-7 | Network Segregation | SP-7.b | SP-7.e | TBD |
| SP-8 | Transmission Integrity | --- | SP-8.e | TBD |
| SP-9 | Network Disconnect | --- | SP-9.e | TBD |
| SP-10 | Information Transmission | --- | SP-10.e | TBD |
| SP-11 | Trusted Path | --- | SP-11.b | TBD |
| SP-12 | Duress Alarm | --- | --- | TBD |
| SP-13 | Cryptographic Key Management | SP-13.b | SP-13.e | TBD |
| SP-14 | Key Archive | SP-14.b | SP-14.e | TBD |
| SP-15 | Public Key Infrastructure Certificates | SP-15.b | SP-15.e | TBD |
| SP-16 | Use of Encryption | SP-16.b | SP-16.e | TBD |
| **SECURITY CONTROL SUMMARY** | | | | |
| Total Number of Controls: | | 126 | 164 | TBD |
| Number of ***Basic*** Robustness Controls: | | 126 | 38 | TBD |
| Number of ***Enhanced*** Robustness Controls: | | 0 | 126 | TBD |
| Number of ***Strong*** Robustness Controls: | | 0 | 0 | TBD |

**TABLE 7: SUMMARY OF BASELINE SECURITY CONTROLS**

## APPENDIX J

# CATALOG OF SECURITY CONTROLS

BASIC, ENHANCED, AND STRONG SECURITY CONTROLS FOR INFORMATION SYSTEMS

The following catalog of security controls provides a range of safeguards and countermeasures for information systems. The security controls in the catalog are organized by classes and families within classes. The three principal sections within the catalog contain management, operational, and technical controls, respectively. Each family within a particular security control class has a unique two-character identifier along with a numerical identifier indicating the number of the control within the family. In addition to the family and numeric identifiers, there is also an identifier addressing the robustness level of the security control. Robustness levels indicate a basic (b), enhanced (e), or strong (s) version of the security control with regard to strength of function and assurance of effectiveness.

The security controls in the catalog have a well-defined structure that consists of three key components: (i) a *control objective* section; (ii) a *control mapping* section; and (iii) a *control description* section. As the name implies, the control objective section provides the overall objective for the particular security control when applied to an information system. The control mapping section lists source documents considered during the development of the control catalog that have similar security controls. The control description section provides the specific control requirements and details of each control. Thus, a single control objective may have up to three security controls associated with it reflecting the basic, enhanced, and strong versions of the control (if so defined).

With regard to cryptography employed in Federal information systems, organizations must comply with current Federal policy and meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative for organizations. Consult FIPS 140-2 for specific guidance.

| ABBREVIATION | SECURITY CONTROL SOURCE |
|---|---|
| FISCAM | General Accounting Office, *Federal Information System Controls Audit Manual* |
| DOD 8500 | Department of Defense Instruction 8500.2, *Information Assurance Implementation* |
| NIST SP 800-26 | NIST Special Publication 800-26, *Security Self Assessment Guide for Information Technology Systems* |
| CMS | Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements* |
| DCID 6/3 | Director of Central Intelligence Directive (DCID) Manual 6/3, *Protecting Sensitive Compartmented Information within Information Systems* |
| ISO 17799 | International Standard ISO/IEC 17799, Code of Practice for Information Security Management |

**TABLE 8: SECURITY CONTROL SOURCES**

## Table of Contents – Security Controls Catalog

## MANAGEMENT CONTROLS

**FAMILY:** RISK ASSESSMENT (RA)

### RA-1 SECURITY CATEGORIZATION

CONTROL OBJECTIVE: The potential impact on organizational operations and assets resulting from the operation of the information system is identified.

CONTROL MAPPING: [NIST 800-26: 1.1.3, 3.1.1; FISCAM: SP-1, AC-1.1, AC-1.2; DCID 6/3: Chapter 3; CMS: 1.7.1, 1.9.7; DOD 8500: DCII-1]

**RA-1.b** BASIC CONTROL: The information system is categorized in accordance with FIPS Publication 199 and NIST Special Publication 800-60. The security categorization is explicitly documented and approved by an appropriate senior official.

**RA-1.e** ENHANCED CONTROL (Add to basic control):
Categorization is based upon an analysis with documented summary that explains the rationale for the categorization selected.

**RA-1.s** STRONG CONTROL: To be defined.

### RA-2 RISK ASSESSMENT

CONTROL OBJECTIVE: Risks to organizational operations and assets resulting from the operation of the information system are identified.

CONTROL MAPPING: [NIST 800-26: 1.1.1, 1.1.2, 1.1.4, 1.1.5; FISCAM: SP-1, SP-3; ISO-17799: 4.2.1; CMS: 1.8.1, 1.8.2, 1.8.4, 4.1.4,10.9.1, 10.9.4]

**RA-2.b** BASIC CONTROL: An assessment of risk to organizational operations and assets due to the operation of the information system is performed and documented on an [*Assignment: time period which is at least annually*] and whenever there are significant changes to the system, facilities, or other conditions that may impact the security or authorization status of the system. The risk assessment (either formal or informal) is consistent with the intent of NIST Special Publication 800-30. The documented risk assessment includes the following: (i) identification of the conditions for reassessment, indicating the period for periodic reassessment and defining the level of change to the information system or environment that will cause a reassessment to occur; (ii) identification of the security authorization boundary; (iii) the current information system configuration including connections to other systems; (iv) actions that will be taken to ensure that the boundary definition is accurately updated periodically; (v) an inventory of information system assets; (vi) identification and assessment of threat sources; (vii) identification and assessment of information system vulnerabilities; and (viii) identification of risks from third party connections.

**RA-2.e** ENHANCED CONTROL (Add to basic control):
Sufficient information is documented by the organization to explain the rationale for the risk assessment results.

**RA-2.s** STRONG CONTROL: To be defined.

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY PLANNING (PL)

### PL-1 RULES OF BEHAVIOR AND ACCEPTABLE USE

CONTROL OBJECTIVE: Establish information system policy for rules of behavior and acceptable use when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26: 4.1.3; ISO-17799: 3.1.1, 8.7.4, 9.3.2; DCID 6/3: Doc1-b; CMS: 5.1.2; DOD 8500: PRRB-1; CMS: 1.5.1, 1.13.2, 1.13.4, 1.13.5, 10.3.3; FISCAM: SP-1.2]

**PL-1.b** BASIC CONTROL: A set of rules that describes the security operations of the information system and clearly delineates security responsibilities and expected behavior of all system owners, users, operators, and administrators is in place. Rules include the consequences of inconsistent behavior or non-compliance. Rules include all significant aspects of information system use, including policy on use of electronic mail. Signed acknowledgement of the rules is a condition of access.

**PL-1.e** ENHANCED CONTROL: To be defined.

**PL-1.s** STRONG CONTROL: To be defined.

### PL-2 ACCESS CONTROL POLICY

CONTROL OBJECTIVE: Establish an information system policy for access control when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26: 15.2.1, 16.1.9; FISCAM: SD-2.1, AC-2.1, AC-3.2; ISO-17799: 3.1.1, 5.2.1, 9.1.1; CMS: 2.1.2, 10.8.2]

**PL-2.b** BASIC CONTROL: An explicit access control policy establishes the rules to be implemented to ensure that only designated individuals, under specified conditions (e.g., time of day, port of entry, type of authentication, etc.) can: (i) access the information system (i.e., logon, establish connection); (ii) activate specific system commands; (iii) execute specific programs and procedures; and (iv) create, view, or modify specific objects (programs, information, system parameters). The policy has provisions for periodic review of access authorizations. This policy covers both discretionary and non-discretionary controls. Discretionary controls are those controls established at the discretion of the information owner, usually with constraints called out in the policy. Non-discretionary controls (e.g., restrictions on the viewing of export-controlled information or personal medical information), are those controls established by organizational policy and not subject to determination by the owner of the information.

**PL-2.e** ENHANCED CONTROL: To be defined.

**PL-2.s** STRONG CONTROL: To be defined.

### PL-3 GROUP IDENTIFICATION AND AUTHENTICATION POLICY

CONTROL OBJECTIVE: Establish information system policy for group identifiers and the use of those identifiers when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [ISO-17799: 3.1.1; DOD 8500: IAGA-1]

**PL-3.b** BASIC CONTROL: An explicit group identification and authentication policy establishes the rules to be implemented to ensure that group authenticators are used for information system access only when explicitly authorized and in conjunction with other authenticators as appropriate.

**PL-3.e** ENHANCED CONTROL: To be defined.

**PL-3.s** STRONG CONTROL: To be defined.

**PL-4 INFORMATION FLOW CONTROL POLICY**

CONTROL OBJECTIVE: Establish information system policy for information flow control when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [ISO-17799: 3.1.1, 5.2.1, 8.7.1, 8.7.6]

**PL-4.b** BASIC CONTROL: An explicit information flow control policy establishes the rules to be implemented to ensure that information is allowed to flow within the information system and across system boundaries only as authorized. This policy covers both discretionary and non-discretionary controls. Discretionary controls are those controls established at the discretion of the information owner, usually with constraints called out in the policy. Non-discretionary controls (e.g., restrictions on the viewing of export-controlled information or personal medical information), are those controls established by organizational policy and not subject to determination by the owner of the information.

**PL-4.e** ENHANCED CONTROL: To be defined.

**PL-4.s** STRONG CONTROL: To be defined.

**PL-5 ACCOUNTABILITY POLICY**

CONTROL OBJECTIVE: Establish information system policy for accountability when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26: 17.1.1, 17.1.2; FISCAM: AC-4.3, SP-1.2; ISO-17799: 3.1.1]

**PL-5.b** BASIC CONTROL: An explicit accountability policy establishes the rules to be implemented to ensure that information system users can be held accountable for their actions as needed. Accountability policy elements are, for example: (i) purposes for accountability (e.g., deterrent, incident forensics, etc.); (ii) required granularity for accountability (e.g., to the granularity of individual users); and (iii) time period for which accountability information must be available (e.g., five years).

**PL-5.e** ENHANCED CONTROL: To be defined.

**PL-5.s** STRONG CONTROL: To be defined.

**PL-6 CONTINGENCY PLANNING AND OPERATIONS POLICY**

CONTROL OBJECTIVE: Establish information system policy for contingency operations when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26; FISCAM: SC-1.1, SC-1.2, SC-1.3, SP-2.2, SP-3, SP-4]

**PL-6.b** BASIC CONTROL: An explicit contingency planning and operations policy addresses all critical aspects of contingency planning consistent with NIST Special Publication 800-34.

**PL-6.e** ENHANCED CONTROL: To be defined.

**PL-6.s** STRONG CONTROL: To be defined.

**PL-7 CONFIGURATION MANAGEMENT POLICY**

CONTROL OBJECTIVE: Establish information system policy for configuration management and control of hardware, software and firmware assets when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [FISCAM: SP-3]

**PL-7.b** BASIC CONTROL: An explicit configuration management policy establishes the rules to be implemented to ensure that organization's track and control the hardware, software, and firmware components that comprise the information system.

**PL-7.e** ENHANCED CONTROL: To be defined.

**PL-7.s** STRONG CONTROL: To be defined.

**PL-8 INCIDENT RESPONSE POLICY**

CONTROL OBJECTIVE: Establish information system policy for monitoring and responding to incidents when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26; FISCAM: AC-5.1]

**PL-8.b** BASIC CONTROL: An explicit, documented incident response policy addresses all critical aspects of incident handling and response consistent with NIST Special Publication 800-61.

**PL-8.e** ENHANCED CONTROL: To be defined.

**PL-8.s** STRONG CONTROL: To be defined.

**PL-9 SECURITY TRAINING AND AWARENESS POLICY**

CONTROL OBJECTIVE: Establish information system policy for security training and awareness when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26; FISCAM: SP-5]

**PL-9.b** BASIC CONTROL: An explicit, documented security training and awareness policy addresses all critical aspects of security training and awareness consistent with NIST Special Publications 800-16 and 800-50.

**PL-9.e** ENHANCED CONTROL: To be defined.

**PL-9.s** STRONG CONTROL: To be defined.

**PL-10 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for physical and environmental protection when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26; FISCAM: AC-6]

**PL-10.b** BASIC CONTROL: An explicit, documented physical and environmental protection policy addresses all critical aspects of physical and environmental protection consistent with General Services Administration policies, directives, regulations, and guidelines.

**PL-10.e** ENHANCED CONTROL: To be defined.

**PL-10.s** STRONG CONTROL: To be defined.

**PL-11 PERSONNEL SECURITY POLICY**

CONTROL OBJECTIVE: Establish information system policy for personnel security when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26]

**PL-11.b** BASIC CONTROL: An explicit, documented personnel security policy addresses all critical aspects of personnel security consistent with Office of Personnel Management policies, directives, regulations, and guidelines.

**PL-11.e** ENHANCED CONTROL: To be defined.

**PL-11.s** STRONG CONTROL: To be defined.

**PL-12 MEDIA PROTECTION POLICY**

CONTROL OBJECTIVE: Establish information system policy for media protection when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26]

**PL-12.b** BASIC CONTROL: An explicit, documented media protection policy addresses all critical aspects of media protection to include: (i) media access; (ii) media labeling; (iii) media transport; (iv) media destruction and disposal; (v) media sanitization and clearing; (vi) media storage; and (vii) disposition of media records.

**PL-12.e** ENHANCED CONTROL: To be defined.

**PL-12.s** STRONG CONTROL: To be defined.

**PL-13 SYSTEM MAINTENANCE POLICY**

CONTROL OBJECTIVE: Establish information system policy for information system hardware and software maintenance when organizational policy is not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26]

**PL-13.b** BASIC CONTROL: An explicit, documented information system maintenance policy addresses all critical aspects of hardware and software maintenance to include: (i) scheduling of periodic maintenance; (ii) maintenance tools; (iii) remote maintenance; (iv) maintenance personnel; and (v) timeliness of maintenance.

**PL-13.e** ENHANCED CONTROL: To be defined.

**PL-13.s** STRONG CONTROL: To be defined.

**PL-14 SECURITY PLANNING**

CONTROL OBJECTIVE: In accordance with organizational policy, facilitate achieving adequate security by documenting and approving a security plan for the information system.

CONTROL MAPPING: [NIST 800-26: 5.1.2, 5.2.1: FISCAM: SP-2.1, SP-2.2; ISO-17799: 4.1.3, 12.1.1; DCID 6/3: Doc1-a; CMS: 1.9, 1.9.3, 1.9.9, 1.9.10; DOD 8500: DCSD-1]

**PL-14.b** BASIC CONTROL: The content of the security plan is compliant with OMB policy and consistent with the intent of NIST Special Publication 800-18. The security plan is approved by appropriate organization officials and incorporated into the information resources management strategic plan. The security plan is reviewed and updated as needed to reflect current conditions, both on a regular basis every [*Assignment: time period*] and whenever there are significant changes defined as [*Assignment: criteria for significant changes*] to the information system, facilities, or other conditions that may impact security.

**PL-14.e** ENHANCED CONTROL (Add to basic control):
Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.

**PL-14.s** STRONG CONTROL: To be defined.

**PL-15 STANDARDS FOR SECURITY TEST AND EVALUATION PLANS**

CONTROL OBJECTIVE: Facilitate effective testing and evaluation of the security controls in the information system by developing standards for security test and evaluation plans when organizational standards are not adequate to address system needs.

CONTROL MAPPING: [NIST 800-26: 10.1.2, 10.2.2, 10.2.5, 12.1.5; FISCAM: SS-3.1, SS-3.2, CC-2.1, CC-3.2, CC-3.3; CMS: 2.5.11, 6.3.9]

**PL-15.b** BASIC CONTROL: Test plan standards have been developed and are followed for all levels of testing that define: (i) responsibilities for each party (e.g., users, system analysts, programmers, evaluators, auditors, quality assurance, and library control); (ii) test development requirements; (iii) test coverage requirements; and (iv) test plan, procedures, and report documentation requirements.

**PL-15.e** ENHANCED CONTROL: To be defined.

**PL-15.s** STRONG CONTROL: To be defined.

## MANAGEMENT CONTROLS

**FAMILY:** SYSTEM AND SERVICES ACQUISITION (SA)

### SA-1 ACQUISITION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the risk of acquiring ineffective security capabilities by meeting specified requirements.

CONTROL MAPPING: [NIST 800-26: 3.1.2, 3.1.5, 3.1.6, 3.1.10, 3.1.11, 3.1.12, 3.2.1, 3.2.2; ISO-17799: 4.1.5, 8.2.2, 9.4.9, 10.1.1; CMS: 3.4.3, 6.3.8; DOD 8500: DCAS-1, DCPP-1, DCSQ-1; FISCAM: CM-3]

**SA-1.b** BASIC CONTROL: A discrete line item for information security (or information assurance) is established in programming and budget documentation.

*Solicitation Documents*

The solicitation documents for the information system (e.g., Requests for Proposals), include security controls and security test and evaluation procedures. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

*Information System Specifications*

For all new information systems and major upgrades to existing systems, there are detailed system specifications prepared and reviewed by management. An organization reference document such as a security recommendation guide (SRG) or a security technical implementation guide (STIG) constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products. If organization reference documents are not available, other government guidelines or vendor literature are acceptable sources. Advice from information security specialists is used in the development of requirements, acquisition documentation, and source selection. Appropriate security controls for the information system and associated security test and evaluation procedures are developed as part of the procurement action. Additionally, a clear description is provided of the security attributes of each network service.

*Vendor or Developer Expectations*

For acquired and developed information systems, identify, as early in the life cycle as possible, the network ports, protocols, and services to be used. Design reviews are conducted on the information systems and security test and evaluation is conducted prior to placing the systems into operation. Test results for the developmental information systems are documented. Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. Vendor supplied system software is supported by the vendor.

*Use of Evaluated and Validated Products*

For acquisition of security and security-enabled commercial off-the-shelf (COTS) information technology products, when multiple products meet organizational requirements, preference is given to products that have been evaluated and validated through one or more of the following sources: (i) the NIAP Common Criteria Evaluation and Validation Scheme; (ii) the International Common Criteria Recognition Arrangement; and/or (iii) the NIST Cryptographic Module Validation Program.

**SA-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SA-1.s** STRONG CONTROL: To be defined.

### SA-2 COPYRIGHTED AND PUBLIC DOMAIN WORKS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to comply with software license restrictions and to ensure appropriate use of software and capabilities such as peer-to-peer file trading networks.

CONTROL MAPPING: [NIST 800-26: 10.2.10, 10.2.13; ISO-17799: 12.1.2; CMS: 1.1.8, 4.1.1, 6.2.1, 10.7.1, 10.7.2; DOD 8500: DCAS-1, DCPD-1; FISCAM: CM-3]

**SA-2.b** BASIC CONTROL: The use of copyrighted software or shareware and personally owned software is controlled and documented. Open source software use is permitted but the software is assessed to determine its security impact prior to use. Public domain software products (excluding open source software products) are not used in organization information systems unless compelling reasons are established, the product is assessed for security impacts, and explicitly approved for use. Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used unless they are necessary for mission accomplishment and there are no alternative solutions available. Such products are assessed for security impacts, and explicitly approved for use. Purchased software is used in accordance with contract agreements and copyright laws. Managers purchasing software packages protected by quantity licenses ensure that a tracking system is in place to control the copying and distribution of the proprietary software. Use of publicly accessible peer-to-peer file trading networks is also controlled and documented to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**SA-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SA-2.s** STRONG CONTROL: To be defined.

**SA-3 SYSTEM DOCUMENTATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that adequate documentation is available for the information system.

CONTROL MAPPING: [NIST 800-26: 12.1.1, 12.1.2, 12.1.3, 12.1.6, 12.1.7, 3.2.4; DCID 6/3: Doc2, Doc3-c, Doc3-c, Doc4-d; CMS: 2.5.10, 4.1.3; DOD 8500: DCFA-1; FISCAM: SD-2.1, SP-4]

**SA-3.b** BASIC CONTROL: There is adequate vendor-supplied documentation of purchased software, hardware, and firmware for the information system. There is adequate documentation for applications and for in-house developed software, hardware, and firmware.

*Administrator Guides and Manuals*

There are adequate administrator guides and/or manuals for the information system. Documentation includes guides and/or manuals for the information system's privileged users. The guides and/or manuals provide, at a minimum, information on: (i) configuring, installing, and operating the system; (ii) making optimum use of the system's security features; and (iii) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation is updated as new vulnerabilities are identified.

*User Guides and Manuals*

There is a general user's guide that describes the security mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact. Information system, administrator, and user documentation are updated to include security controls added since development and as new vulnerabilities are identified.

**SA-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SA-3.s** STRONG CONTROL: To be defined.

### SA-4 OUTSOURCED INFORMATION SYSTEM SERVICES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks from outsourced services by explicitly addressing the need for effective security controls at the service provider.

CONTROL MAPPING: [NIST 800-26: 12.2.3; ISO-17799: 4.1.6, 4.3.1, 10.5.5; DOD 8500: DCDS-1; FISCAM: SP-8]

**SA-4.b** BASIC CONTROL: Acquisition or outsourcing of dedicated information system security services such as: (i) incident monitoring, analysis and response; (ii) operation of information system security devices (e.g., firewalls); or (iii) key management services, are supported by a risk assessment and approved by the appropriate, designated organization official. Acquisition or outsourcing of information system services explicitly addresses government, service provider and end user security roles and responsibilities. Appropriate controls are applied to outsourced software development. Appropriate policies and procedures concerning activities of external third parties (e.g., service bureaus, contractors, other service providers such as system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include provisions for: (i) security clearances (where appropriate and required); (ii) background checks; (iii) required expertise; (iv) confidentiality agreements; (v) security roles and responsibilities; (vi) connectivity agreements; and (vii) individual accountability.

**SA-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SA-4.s** STRONG CONTROL: To be defined.

### SA-5 DEVELOPER FUNCTIONAL TESTING

CONTROL OBJECTIVE: Testing is planned, conducted, and results documented by the developer of the information system.

CONTROL MAPPING: [NIST 800-26: 12.1.5, 3.2.1, 3.2.2, 3.2.3, 3.2.5; FISCAM: CC-2.1; DCID 6/3: Test3-b; CMS: 2.5.9]

**SA-5.b** BASIC CONTROL: The developer performs functional testing to establish that the product exhibits the properties necessary to satisfy the functional requirements. Testing is performed according to a documented plan that identifies the security functions to be tested and describes the goal of the tests to be performed. Testing is conducted using documented procedures that provide instructions for using test programs and test suites, including any test ordering requirements, the test environment, test conditions, test data parameters and values, how the test results are derived from the test inputs, and the expected test results.

The developer addresses those aspects of testing that deal with completeness of test coverage; including the extent to which the functional specification is tested and whether or not the testing is sufficiently extensive to demonstrate that the product operates as specified. The testing is designed and conducted with consideration for the correspondence between the tests identified in the test documentation and the requirements in the functional specification.

The developer addresses the level of detail to which the product is tested. The level of testing is appropriate to demonstrate that the implementation is consistent with its design. The objective is to counter the risk of missing an error in the development of the product. Testing is performed to the depth necessary such that the internal interfaces between subsystems of the high-level design have been exercised. The high-level design provides a description in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide.

**SA-5.e** ENHANCED CONTROL: (Add to basic control):
Test ordering is based upon an analysis ensuring that testing is structured such as to avoid circular arguments about the correctness of the information system being tested.

Test design and conduct is based upon an analysis of the test coverage that demonstrates the correspondence between the functional specification and the tests identified in the test documentation is complete.

Testing is performed to the depth necessary such that the internal interfaces between subsystems of the low-level design have been exercised. The low-level design provides a description of the internal workings in terms of modules and their interrelationships and dependencies. For each module, the low-level design describes its purpose, function, interfaces, dependencies, and the implementation of any policy-enforcing functions.

**SA-5.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Test ordering is based upon an analysis ensuring that testing is structured such as to avoid circular arguments about the correctness of the system being tested.

Test design and conduct is based upon an analysis of the test coverage that demonstrates the correspondence between the functional specification and the tests identified in the test documentation is complete. **The analysis of the test coverage rigorously demonstrates that all external interfaces identified in the functional specification have been completely tested.**

Testing is performed to the depth necessary such that the internal interfaces between subsystems of the low-level design and **implementation representation** have been exercise. The low-level design provides a description of the internal workings in terms of modules and their interrelationships and dependencies. For each module, the low-level design describes its purpose, function, interfaces, dependencies, and the implementation of any policy-enforcing functions. **The implementation representation in the form of source code, firmware, hardware drawings, etc. captures the detailed internal workings of the system.**

**SA-6 LIFE CYCLE SUPPORT**

CONTROL OBJECTIVE: The information system development life cycle is clearly defined.

CONTROL MAPPING: [NIST 800-26: 3.1, 3.1.4; CMS: 6.3.11, 6.3.12; DOD 8500: DCBP-1]

**SA-6.b** BASIC CONTROL: A system development life cycle (SDLC) methodology has been developed that: (i) provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process; (ii) is sufficiently documented to provide guidance to staff with varying levels of skill and experience; and (iii) provides a means of controlling changes in requirements that occur over the system's life and includes documentation requirements. Programming staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology. The developer establishes a life-cycle model encompassing procedures, tools and techniques used to develop and maintain the information system and providing the necessary control over the development and maintenance of the system.

**SA-6.e** ENHANCED CONTROL (Add to basic control):
The life-cycle model is a standardized life-cycle model that has been approved by some group of experts (e.g. academic experts, standards bodies).

**SA-6.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
The life-cycle model is a standardized life-cycle model that has been approved by some group of experts (e.g. academic experts, standards bodies). **The life-cycle model is a measurable model with arithmetic parameters and/or metrics that measure system development properties (e.g. source code complexity metrics). The developer measures the system development using defined parameters and/or metrics consistent with the model.**

**SA-7 SECURITY DESIGN DISCIPLINES**

CONTROL OBJECTIVE: The information system is implemented using engineering disciplines.

CONTROL MAPPING: [None]

**SA-7.b** BASIC CONTROL: The principles in NIST Special Publication 800-27 are considered and applied as appropriate.

**SA-7.e** ENHANCED CONTROL (Add to basic control):
With respect to security capabilities, the internal structure of the information system is based on an architectural design at a similar level of abstraction as the low-level design (which provides a description of the internal workings in terms of modules and their interrelationships and dependencies). The low-level design and the implementation representation (captures the detailed internal workings of the system and is in the form of source code, firmware, hardware drawings, etc.) are compliant with this architectural design. The architectural design provides for modularity that provides for largely independent modules avoiding unnecessary interactions between the modules of the design; reducing the interdependence between elements, reducing the potential for a change or error in one module will have effects throughout the system, and providing the basis for determining the scope of interaction with other elements of the system.

**SA-7.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
With respect to security capabilities, the internal structure of the information system is based on an architectural design at a similar level of abstraction as the low-level design (which provides a description of the internal workings in terms of modules and their interrelationships and dependencies). The low-level design and the implementation representation (captures the detailed internal workings of the system and is in the form of source code, firmware, hardware drawings, etc.) are compliant with this architectural design. The architectural design provides for modularity that provides for largely independent modules avoiding unnecessary interactions between the modules of the design; reducing the interdependence between elements, reducing the potential for a change or error in one module will have effects throughout the system, and providing the basis for determining the scope of interaction with other elements of the system. **The architectural design provides for layering to separate levels of abstraction, minimizing mutual interactions between layers (keeping only such interactions that are necessary and cannot reasonably be avoided), and minimizing the complexity of access and flow control capabilities. The architectural design provides for minimization of the complexity of policy enforcement mechanisms and the minimization of the amount of non-policy-enforcing functionality within execution domains for policy-enforcing functionality. This minimization, along with modularity and layering, results in policy-enforcement capabilities that are simple enough to be analyzed.**

**SA-8 SECURITY POLICY MODEL**

CONTROL OBJECTIVE: The information system security policy is informally modeled to facilitate implementation and verification.

CONTROL MAPPING: [NIST 800-26: 3.1.6]

**SA-8.b** BASIC CONTROL: The information system is developed based upon a security policy model that in turn is based on the security policies for the system and establishes a correspondence between the functional specification, the security policy model, and these system security policies. The model describes the rules and characteristics of applicable policies and includes a rationale that demonstrates that it is consistent and complete with respect to all policies modeled.

**SA-8.e** ENHANCED CONTROL: To be defined.

**SA-8.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
**The policy is formally modeled whenever formal modeling is feasible.**

## MANAGEMENT CONTROLS

**FAMILY:** SECURITY CONTROL REVIEW (CR)

### CR-1 INFORMATION SYSTEM ASSESSMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to support knowledgeable, risk-based information system authorization by performing a technical assessment of the system.

CONTROL MAPPING: [NIST 800-26: 1.1.6, 1.2.1, 1.2.3, 2.1.1, 2.1.2, 2.1.3; FISCAM: SP-3, SP-5.1, SP-6.1, SP-6.2; ISO-17799: 4.1.7, 12.2.2, 12.3.1; DCID 6/3: Doc3-a, Doc3-b, Doc4-a, Doc4-b, Test1, Test2, Test3-a, Test5-b, Verif1, Verif2; CMS: 1.2.1, 1.4.2, 1.8.7, 1.12.2, 2.5.6, 2.5.8, 2.12.1,10.9.2; DOD 8500: DCII-1]

**CR-1.b** BASIC CONTROL: Assessments of the information system are conducted to: (i) determine if security controls are correctly implemented and, as implemented, are effective in their application; (ii) ensure that security-applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines are met. Assessments of security controls are conducted: (i) prior to initial operational capability and authorization to operate; (ii) prior to each re-authorization to operate; or (iii) when a significant change to the information system occurs. Routine self-assessments are conducted every [*Assignment: time period (e.g., annually)*] to monitor the effectiveness of security controls. Management reviews of system assessment results are conducted and documented forming the basis for management decisions and action plans. Inspection reports, including self-assessment reports, corrective actions and supporting documentation are retained for a minimum [*Assignment: time period (e.g., five years)*]. Assessments are conducted in a manner to minimize disruption of operations.

**CR-1.e** ENHANCED CONTROL (Add to basic control):
Assessments of the information system security controls (other than routine self-assessments) are conducted by assessors independent of the program manager, information system owner, system operator, and end user. Assessors are expected to provide a report of findings directly to the program manager or system owner, who in turn provide the results to the authorizing official or to the authorizing official's designated representative. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CR-1.s** STRONG CONTROL: To be defined.

### CR-2 VULNERABILITY SCANNING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically scan for vulnerabilities in the information system.

CONTROL MAPPING: [NIST 800-26: 2.1.4; ISO-17799: 12.2.2; DCID 6/3: SysAssur3-b; DOD 8500: VIVM-1]

**CR-2.b** BASIC CONTROL: Vulnerability assessment tools are implemented by the organization and personnel are trained in their use. The organization conducts periodic testing of the security posture of the information system by scanning the system with vulnerability detection tools every [*Assignment: time period (e.g., every 6 months)*].

**CR-2.e** ENHANCED CONTROL (Add to basic control):
Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CR-2.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned. The list of vulnerabilities scanned is updated periodically, at least prior to each periodic scan. Vulnerability scanning procedures include vulnerability list update and vulnerability scan when a significant, new vulnerability is announced. **Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.** Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

### CR-3 VULNERABILITY ASSESSMENT AND PENETRATION TESTING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to determine the degree to which the information system can be expected to resist attempts to discover and successfully exercise vulnerabilities.

CONTROL MAPPING: [NIST 800-26: 2.1.4, 10.3.2; ISO-17799: 12.2.2, 12.3.2; DCID 6/3: Test4, Test5-a; CMS: 1.9.8; DOD 8500: ECMT-2]

**CR-3.b** BASIC CONTROL: Vulnerability identification is performed on new, existing, and recently modified information systems and facilities. A summary list of vulnerabilities is prepared for each information system and facility being analyzed. Wherever system capabilities permit, automated vulnerability assessment or state management tools are used. Regular internal and external assessments are conducted. The organization conducts periodic testing of the security posture of the information system by attempting to penetrate the system with attack tools and expertise every [*Assignment: time period (e.g., 12 months)*]. Attack tools are used only with the approval from the appropriate authorities and concurrence of legal counsel.

**CR-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CR-3.s** STRONG CONTROL: To be defined.

## MANAGEMENT CONTROLS

**FAMILY:** PROCESSING AUTHORIZATION (PA)

### PA-1 AUTHORIZE INFORMATION SYSTEM CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from connections to information systems by explicit authorization prior to establishing connections.

CONTROL MAPPING: [NIST 800-26: 4.1.8, 12.2.3; DOD 8500: EBCR-1; ISO-17799: 4.2.2, 8.1.6; CMS: 1.6.2, 1.9.5, 2.2.6, 2.2.20, 2.5.7, 2.6.1, 2.8.2, 2.9.13; DCID 6/3: 8.B.7.d(all); FISCAM: AC-1]

**PA-1.b** BASIC CONTROL: Management authorizes in writing all connections to other information systems (including systems owned and operated by another program, organization, or contractor). The connections are compliant with established organizational connection rules and approval processes. Connection agreements consistent with intent of NIST Special Publication 800-47 are in place whenever the information system is connected to systems not under the control of the same authorizing official. Trust relationships among hosts and external entities are appropriately restricted. A list is developed and maintained, along with evidence of deployment planning and coordination and exchange of connection rules and requirements for: (i) applications (on all hosting information systems, current and potential); and (ii) the information system (including all hosted applications). Criteria are defined for conditions under which information system connections are to be disabled.

**PA-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-1.s** STRONG CONTROL: To be defined.

### PA-2 AUTHORIZE MOBILE CODE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from mobile code by explicit authorization prior to establishing a mobile code capability.

CONTROL MAPPING: [DCID 6/3: 7.E.5.a, 7.E.5.d; FISCAM: AC-4]

**PA-2.b** BASIC CONTROL: Deployment of mobile code is restricted based on its potential to cause damage to the information system if used maliciously. Mobile code registration, approval, and control procedures to prevent the development, acquisition, or introduction of unacceptable mobile code within the information system, are implemented. All mobile code or executable content employed is registered unless otherwise approved by the authorizing official. Uploading of mobile code or executable content from one organizational information system to another system is to be similarly authorized.

**PA-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-2.s** STRONG CONTROL: To be defined.

### PA-3 AUTHORIZE REMOTE ACCESS CONNECTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from remote access (e.g.,

dial-up access or Internet access) by explicit authorization prior to establishing a remote access capability.

CONTROL MAPPING: [NIST 880-26: 16.2.4, 16.2.8; FISCAM: AC-1, AC-3.2; CMS: 2.8.4]

**PA-3.b** BASIC CONTROL: The number of users who can access the information system from remote locations (for information systems other than public web servers or systems specifically designed for public access) is limited and justification for such access is documented, monitored, and approved by a designated organization official. Dial-up lines, other than those that are protected with FIPS 140-2 validated cryptography, are not used for gaining access to an information system that processes organizational information unless the authorizing official provides specific written authorization for a system to operate in this manner. Actions such as periodic monitoring are taken to ensure that installed equipment does not include unanticipated dial-up capabilities.

**PA-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-3.s** STRONG CONTROL: To be defined.

### PA-4 AUTHORIZE COLLABORATIVE COMPUTING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from collaborative computing by explicit authorization prior to establishing a collaborative computing capability.

CONTROL MAPPING: [None]

**PA-4.b** BASIC CONTROL: Running collaborative computing mechanisms (e.g., the IETF standard Web-based Distributed Authoring and Versioning that enables collaborative editing and file management on remote Web servers) on information systems requires explicit authorization by the authorizing official or authorizing official's designated representative. When granted, authorization is specific, identifying allowed mechanisms, allowed purpose, and the information system upon which mechanisms can be used.

**PA-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-4.s** STRONG CONTROL: To be defined.

### PA-5 AUTHORIZE WIRELESS ACCESS POINT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce risks arising from wireless connections by explicit authorization prior to establishing a wireless capability.

CONTROL MAPPING: [ISO-17799: 9.8.1; DOD 8500: ECWN-1; FISCAM: AC-1]

**PA-5.b** BASIC CONTROL: Installation of wireless access points into organizational networks is discouraged and requires explicit authorization by the authorizing official.

**PA-5.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-5.s** STRONG CONTROL: To be defined.

**PA-6 AUTHORIZE INFORMATION SYSTEM OPERATION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure explicit management authorization to operate the information system and acceptance of risks to the organization's operations and assets.

CONTROL MAPPING: [NIST 800-26: 3.2.7, 4.2.1, 12.2.5; ISO-17799: 4.1.4, 12.1.5, 12.2.1; FISCAM: SP-6.2]

**PA-6.b** BASIC CONTROL: In compliance with NIST Special Publication 800-37, explicit authorization to operate the information system is received prior to placing the system into operation. If the authorization decision is an interim approval to operate, then: (i) the authorization is granted for a maximum time period (typically in accordance with the designated FIPS Publication 199 security category of the information system) of [*Assignment: time period for each security category (e.g., eighteen months, twelve months, six months)*]. An explicit plan for corrective action is in-place, being effectively implemented, and monitored by the authorizing official. Re-authorization is obtained prior to continued operation following significant information system changes. Re-authorization is obtained at least every [*Assignment: time period, a maximum of three years*].

**PA-6.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PA-6.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** PERSONNEL SECURITY (PS)

### PS-1 POSITION REVIEW

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to review information system-related positions for criticality/sensitivity.

CONTROL MAPPING: [NIST 800-26: 6.1.1: FISCAM: SD-1.2; CMS: 1.4.1]

**PS-1.b** BASIC CONTROL: All positions within the organization are assigned a criticality/sensitivity rating (e.g., low, moderate, high) based on the information system access given to individuals filling those positions. The criticality/sensitivity rating is consistent with the FIPS Publication 199 security categories of the information systems accessible to the individuals filling the designated positions. All positions are reviewed for criticality/sensitivity rating periodically every [*Assignment: time period (e.g., five years)*].

**PS-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PS-1-s** STRONG CONTROL: To be defined.

### PS-2 PERSONNEL SCREENING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is not granted without first verifying that the individual seeking access meets organizational personnel security requirements.

CONTROL MAPPING: [NIST 800-26: 6.2.1, 6.2.2, 6.2.4; FISCAM: SP-4.1, SP-7.1, AC-2.2; ISO-17799: 6.1.2; CMS: 1.4.1, 1.10.1, 1.10.5, 1.10.6]

**PS-2.b** BASIC CONTROL: Individuals requiring access to information must be screened (e.g., verification of background checks and investigations as well as security and non-disclosure agreements) prior to being granted access for access authorization in accordance with organizational personnel security policies. Privileged users (i.e., individuals who are authorized to bypass significant technical and operational controls), are screened prior to access and periodically every [*Assignment: time period (e.g., two years)*]. For prospective employees, references are contacted and background checks performed, as appropriate. Periodic reinvestigations are performed every [*Assignment: time period, no more than five years*], consistent with the criticality/sensitivity rating of the position, according to criteria from the Office of Personnel Management. Security agreements are required for employees and contractors assigned to work with mission information. The period during which nondisclosure requirements remain in effect is identified.

**PS-2.e** ENHANCED CONTROL (Add to basic control):
Non-privileged users are re-screened periodically. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PS-2-s** STRONG CONTROL: To be defined.

### PS-3 TERMINATION AND TRANSFER

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system access is terminated upon personnel transfer or termination.

CONTROL MAPPING: [NIST 800-26: 6.1.7, 6.1.8; FISCAM: SP-4.1, SP-7.1; CMS: 1.10.4, 2.8.1]

**PS-3.b** BASIC CONTROL: Termination and transfer procedures include: (i) exit interview procedures; (ii) return of property, keys, identification cards, passes, etc.; (iii) notification to security management; and (iv) immediately escorting employees terminated for cause out of the organization's facilities.

**PS-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PS-3-s** STRONG CONTROL: To be defined.

### PS-4 THIRD PARTY PERSONNEL SECURITY

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that service providers and other third parties apply appropriate personnel security measures.

CONTROL MAPPING: [ISO-17799: 4.2.1]

**PS-4.b** BASIC CONTROL: Personnel security measures employed by service providers and third parties (e.g., service bureaus, contractors, other organizations providing system development, network management, security management) are documented, agreed to, implemented, and monitored for compliance and include, if appropriate, provisions for: (i) security clearances; (ii) background checks; (iii) required expertise; and (iv) confidentiality agreements. Personnel security measures employed by service providers and third parties are consistent with the intent of NIST Special Publication 800-35.

**PS-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PS-4-s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

### PE-1 IDENTIFICATION OF SENSITIVE FACILITIES AND RESTRICTED AREAS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to identify and designate sensitive facilities and restricted areas containing information systems.

CONTROL MAPPING: [FISCAM: AC-4]

**PE-1.b** BASIC CONTROL: The organization identifies and designates sensitive facilities and restricted areas (i.e., areas, rooms, or groups of rooms containing information system servers, controlled interface equipment, associated peripherals or communications equipment that must be relied upon for the correct enforcement of the system security policy). The organization also identifies and designates non-sensitive facilities and non-restricted areas, (i.e., areas, rooms, or groups of rooms containing information system components not involved in security policy enforcement and possibly accessible to the general public).

**PE-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE.1-s** STRONG CONTROL: To be defined.

### PE-2 AUTHORIZE PHYSICAL ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage, and make available for enforcement, authorizations for physical access to sensitive facilities and restricted/controlled areas containing information systems.

CONTROL MAPPING: [NIST 800-26: 7.1.1, 7.1.2; FISCAM: AC-3, AC-3.1, AC-6; DCID 6/3: Access1; CMS: 1.3.15, 2.1.2, 2.2.22, 10.1.1, 10.1.2]

**PE-2.b** BASIC CONTROL: A list of persons with authorized physical access to sensitive facilities and restricted/controlled areas containing information systems (i.e., access authorizations) is maintained. Access lists also show which individuals are authorized to operate the information system or supporting peripheral equipment. Access lists are documented on standard forms, maintained on file, and approved by appropriate organization officials. The list of persons with authorized physical access to sensitive facilities and restricted/controlled areas is reviewed by appropriate organization officials every [*Assignment: time period (e.g., as needed and at least annually)*].

**PE-2.e** ENHANCED CONTROL (Add to basic control):
Access lists are securely transferred to the enforcement section of the organization. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE.2-s** STRONG CONTROL: To be defined.

### PE-3 PHYSICAL ACCESS ENFORCEMENT

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply physical access controls at designated physical entry points within sensitive facilities and restricted/controlled areas containing information systems.

CONTROL MAPPING: [NIST 800-26: 7.1.1, 7.1.4, 7.1.6, 7.1.7; FISCAM: AC-3, AC-3.1, AC-6; ISO-17799: 7.1.1, 7.1.2, 7.1.3, 7.1.4; DCID 6/3: Access1; CMS: 1.4.1, 2.1.2, 2.2.4, 2.2.7, 2.2.27, 5.2.7]

**PE-3.b** BASIC CONTROL: Physical security perimeters are defined by the organization. Sensitive facilities and restricted/controlled areas are prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that control access. The main entrance to sensitive facilities and restricted areas is controlled/manned. Secondary entrances have cameras and/or electronic entry detection devices (e.g., card keys), to monitor access. Apparent security violations or suspicious physical access activities are investigated and remedial actions taken. Every physical access point to sensitive facilities or restricted areas housing information systems that process or display information is controlled during working hours and guarded or locked during non-work hours. Identification badges are worn. Access authorization is verified before granting physical access. Unauthorized personnel are denied access to areas containing protected information. Appropriately authorized personnel are granted physical access, with escort if necessary, to facilities. Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter sensitive facilities and restricted/controlled areas containing information systems and system/media libraries after an emergency-related event (e.g., fire drills, evacuations, etc.). The organization controls access to non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) as appropriate in accordance with the organization's assessment of risk.

**PE-3.e** ENHANCED CONTROL (Add to basic control):
The [*Assignment: list of physical access points*] physical access points are controlled twenty-four hours per day, seven days per week through the use of entry devices such as key cards or biometrics. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-3.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
The [*Assignment: list of physical access points*] physical access points are controlled twenty-four hours per day, seven days per week through the use of entry devices such as key cards or biometrics. **The [*Assignment: list of physical access points*] physical access points are controlled and observed twenty-four hours per day, seven days per week through the use of guards or monitored alarms.** Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-4 ACCESS MONITORING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to monitor physical access controls for both proper operation and response to incidents.

CONTROL MAPPING: [NIST 800-26: 7.1.4, 7.1.9, 7.1.10; FISCAM: SC-2.3, AC-3.1, AC-4, AC-4.3; DCID 6/3: Access1; CMS: 2.2.6, 2.6.1, 2.13.1]

**PE-4.b** BASIC CONTROL: Physical accesses to sensitive facilities and restricted/controlled areas containing information systems and system/media libraries are monitored. Audit logs are reviewed every [*Assignment: time period (e.g., daily)*]. Real-time intrusion alarms are centrally monitored. Apparent security violations or suspicious physical access activities are investigated, and remedial actions taken. Non-sensitive facilities and non-restricted/controlled areas (e.g., publicly accessible areas) are monitored as appropriate in accordance with the organization's assessment of risk.

**PE-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-4.s** STRONG CONTROL: To be defined.

**PE-5 VISITOR CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control visitor access to sensitive facilities and restricted/controlled areas containing information systems and system/media libraries.

CONTROL MAPPING: [NIST 800-26: 7.1.11, FISCAM: AC-3.1, AC-6; DCID 6/3: Access1; CMS: 2.2.23, 2.6.3; DOD 8500: PEVC-1]

**PE-5.b** BASIC CONTROL: Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks. Visitors, contractors, and maintenance personnel are formally signed in, escorted, and activities monitored when required. Registers are maintained and include: (i) the name; (ii) date; (iii) time of entry; (iv) time of departures; (v) purpose of visit; and (vi) person(s) visited. The register is closed out [*Assignment: time period (e.g., at the end of each month)*] and reviewed by appropriate organization officials.

**PE-5.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-5.s** STRONG CONTROL: To be defined.

**PE-6 PHYSICAL ACCESS TO INFORMATION TRANSMISSION MEDIUM**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to mitigate eavesdropping, in-transit modification, and service disruption threats by controlled physical access to information transmission medium.

CONTROL MAPPING: [NIST 800-26: 7.2.1, 7.2.2; DCID 6/3: Access1; CMS: 2.2.8; FISCAM: AC-2, AC-6]

**PE-6.b** BASIC CONTROL: Physical access to unencrypted information transmission lines is controlled to the extent necessary to mitigate eavesdropping and in-transit modification. Physical access to all information transmission lines is controlled to the extent necessary to mitigate service disruption by physical tampering or destruction. Access to devices that display or output information is appropriately controlled. Devices that display or output information are positioned to deter unauthorized individuals from reading the information. Access to mobile or portable information systems is appropriately controlled.

**PE-6.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-6.s** STRONG CONTROL: To be defined.

**PE-7 ROUTINE PHYSICAL SECURITY CHECKING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance physical security by periodically checking for physical security compliance.

CONTROL MAPPING: [None]

**PE-7.b** BASIC CONTROL: Routine checks (e.g., end of the day security checks and unannounced security checks) are performed periodically to ensure that information is being properly handed and stored.

**PE-7.e** ENHANCED CONTROL (Add to basic control):

Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-7.s** STRONG CONTROL: To be defined.

**PE-8 PHYSICAL SECURITY TESTING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically stress the organization's physical security controls with penetration testing.

CONTROL MAPPING: [DOD 8500: PEPS-1]

**PE.8-b** BASIC CONTROL: There are periodic, unannounced attempts to penetrate organizational facilities containing information systems and system/media libraries.

**PE.8-e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE.8-s** STRONG CONTROL: To be defined.

**PE-9 STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to securely store information and information systems.

CONTROL MAPPING: [NIST 800-26: 7.3.2; DCID 6/3: Storage; CMS: 2.2.5, 2.2.14, 2.2.24, 2.2.25; DOD 8500: PESS-1; FISCAM: AC-6]

**PE-9.b** BASIC CONTROL: Documents/equipment are stored in approved containers or facilities with maintenance and accountability procedures. All restricted areas used to protect information meet criteria for secured area or security room, or provisions are made to store high value items in appropriate containers during non-working hours. Organizational information in any form is protected during non-working hours through a combination of a secured or locked perimeter, a secured area, or appropriate containerization. Mobile and portable information systems are stored securely. Organizational information is locked in cabinets or sealed in packing cartons while in transit. Organizational information remains in the custody of an authorized individual. Accountability is maintained during movement.

**PE-9.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-9.s** STRONG CONTROL: To be defined.

**PE-10 ACCESS DEVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance physical security by using devices to control access.

CONTROL MAPPING: [NIST 800-26: 7.1.5, 7.1.8; FISCAM: AC-3.1; CMS: 2.2.15, 2.2.16, 2.2.18; DOD 8500: PEPF-2; FISCAM: AC-6]

**PE-10.b** BASIC CONTROL: Keys, combinations, or other access devices are needed to enter sensitive facilities or restricted/controlled areas that contain information or information systems unless other pro-

tective measures (e.g., guards) are in place. Keys, combinations, or other access devices are secured. Combinations and keys are changed periodically with changes occurring at least every [*Assignment: time period (e.g., annually for combinations)* ]. Combinations are changed when an employee retires, transfers to another position, or is no longer an employee. An envelope containing the combination or duplicate key is secured in a container with the same or higher protections as the material the lock secures. Keys are changed as necessary to prevent or respond to compromise. Issued keys or other entry devices are regularly inventoried.

**PE-10.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-10.s** STRONG CONTROL: To be defined.

### PE-11 PHYSICAL SECURITY CONTAINERS

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance physical security by using containers and facilities that meet defined requirements.

CONTROL MAPPING: [CMS: 2.2.1, 2.2.2, 2.2.3, 2.2.5, 2.2.9, 2.2.10, 2.2.11, 2.2.13, 2.2.19, 2.2.25]

**PE-11.b** BASIC CONTROL: Organizational information requiring protective storage is stored in security containers compliant with General Services Administration requirements and guidelines.

**PE-11.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-11.s** STRONG CONTROL: To be defined.

### PE-12 IDENTIFY NATURAL DISRUPTION/DISASTER PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide an effective response to disruptions and natural disasters by explicitly indicating the intended disruption/disaster coverage.

CONTROL MAPPING: [NIST 800-26: 7.1.19; FISCAM: SC-2.2]

**PE-12.b** BASIC CONTROL: The nature of the disruptions or natural disasters being mitigated and the extent of the expected mitigation are clearly described.

**PE-12.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-12.s** STRONG CONTROL: To be defined.

### PE-13 PLUMBING LINES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to reduce the potential damage from plumbing leaks.

CONTROL MAPPING: [NIST 800-26: 7.1.7; FISCAM: SC-2.2; ISO-17799: 7.2.1; CMS: 5.1.1]

**PE-13.b** BASIC CONTROL: Building plumbing lines do not endanger the information system facility or, at a minimum, shut-off valves and their operating procedures exist and are known.

**PE-13.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-13.s** STRONG CONTROL: To be defined.

### PE-14 EMERGENCY LIGHTING

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance safety and availability by providing lighting in the event of a power outage.

CONTROL MAPPING: [DOD 8500: PEEL-2]

**PE-14.b** BASIC CONTROL: An automatic emergency lighting system is installed that covers emergency exits and evacuation routes.

**PE-14.e** ENHANCED CONTROL (Add to basic control):
Emergency lighting system also covers all areas necessary to maintain mission or business essential functions. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-14.s** STRONG CONTROL: To be defined.

### PE-15 FIRE PROTECTION

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to prevent, detect, and respond to fire.

CONTROL MAPPING: [NIST 800-26: 7.1.12; FISCAM: SC-2.2; 7.1.13; CMS: 5.1.6; DOD 8500: PEFD-2, PEFI-1, PEFS-2; FISCAM: SC-2.2]

**PE-15.b** BASIC CONTROL: Fire suppression and prevention devices and systems, (e.g., sprinkler systems, handheld fire extinguishers, fixed fire hoses, battery-operated or electric stand-alone smoke detectors) are installed, available, and working properly should an alarm be sounded or a fire be detected. The fire department receives an automatic notification of any activation of the smoke detection or fire suppression system. Fire suppression and prevention devices and systems are periodically checked. Fire ignition sources, such as potential failures of electronic devices or wiring, improper storage of materials, are reviewed periodically. Information system facilities undergo a periodic fire marshal inspection. Deficiencies are promptly resolved.

**PE-15.e** ENHANCED CONTROL (Add to basic control):
A fully automatic fire suppression system (compliant with General Services Administration requirements and guidelines) is installed that automatically activates when it detects heat, smoke or particles with appropriate safeguards for danger to personnel from toxicity. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-15.s** STRONG CONTROL: To be defined.

### PE-16 TEMPPERATURE AND HUMIDITY CONTROLS

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control the temperature and humidity of facilities containing information systems.

CONTROL MAPPING: [NIST 800-26: 7.1.14, 7.1.15; FISCAM: SC-2.2; CMS: 5.1.5; DOD 8500: PEHC-2, PETC-2]

**PE-16.b** BASIC CONTROL: Heating and air-conditioning systems are regularly maintained. Temperature and humidity are controlled automatically.

**PE-16.e** ENHANCED CONTROL (Add to basic control):
Temperature and humidity controls are installed and provide an alarm when temperature and humidity fluctuations potentially harmful to personnel or equipment operation are detected. Adjustments to heating or cooling systems may be made manually. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-16.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Temperature and humidity controls are installed and provide an alarm when temperature fluctuations potentially harmful to personnel or equipment operation are detected; adjustments to heating or cooling systems may be made manually. **There is a redundant system in place at the facility to continue temperature and humidity control in the event of the loss of the primary system.** Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

### PE-17 POWER

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to maintain safe power for the information system.

CONTROL MAPPING: [ISO-17799: 7.2.2; DOD 8500: PEMS-1, PEVR-1; FISCAM: SC-2.2]

**PE-17.b** BASIC CONTROL: Power cabling supporting the information system is protected from damage. A master power switch or emergency cut-off switch to information system equipment is present. It is located near the main entrance of the information system area and it is labeled and protected by a cover to prevent accidental shut-off.

**PE-17.e** ENHANCED CONTROL (Add to basic control):
Automatic voltage control is implemented for information systems. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-17.s** STRONG CONTROL: To be defined.

### PE-18 POWER SUPPLY

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide for uninterrupted power.

CONTROL MAPPING: [NIST 800-26: 7.1.18; FISCAM: SC-2.2; ISO-17799: 7.2.2, 7.2.3; DCID 6/3: Power1, Power2; CMS: 5.1.7; DOD 8500: COPS-3]

**PE-18.b** BASIC CONTROL: A short-term uninterruptible power supply is provided so that in the event of loss of primary power source, adequate power is maintained for orderly shut down without need for manual intervention.

**PE-18.e** ENHANCED CONTROL (Add to basic control):
Electrical systems are configured to allow continuous or uninterrupted power to key information system assets and all users accessing the key system assets to perform mission or business-essential functions. This alternative power may be in the form of a short-term, automatically acti-

vated source that provides sufficient power until the source for alternative, ongoing power is activated which may be done manually. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**PE-18.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Electrical systems are configured to allow continuous or uninterrupted power **adequate for maintaining operations**. This alternative power may be in the form of a short-term, automatically activated source that provides sufficient power until the source for alternative, ongoing power is activated which **is done automatically**. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

### PE-19 ENVIRONMENTAL CONTROL TESTING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically test environmental protections.

CONTROL MAPPING: [NIST 800-26: 7.1.19; FISCAM: SC-2.2; CMS: 5.1.3, 5.1.4; DOD 8500: COED-2]

**PE-19.b** BASIC CONTROL: Controls protecting the environment (power, temperature, fire protection, lighting, plumbing) against disruptions and natural disasters are periodically tested every [*Assignment: time period(s) (e.g., by type of test and by type of facility)*].

**PE-19.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-19.s** STRONG CONTROL: To be defined.

### PE-20 ENVIVONMENTAL CONTROL TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel on the use of environmental controls.

CONTROL MAPPING: [DOD 8500: PETN-1]

**PE-20.b** BASIC CONTROL: Individuals that maintain environmental controls or would use the environmental controls in the event of an emergency receive initial training in the operation of the controls. Periodic refresher training is provided every [*Assignment: time period (e.g., annually)*].

**PE-20.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-20.s** STRONG CONTROL: To be defined.

### PE-21 EQUIPMENT DELIVERY AND REMOVAL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the flow of equipment into and out of the organization.

CONTROL MAPPING: [NIST 800-26: 7.1.3, 8.2.2, 8.2.3,10.1.3; FISCAM: AC-3.1, SC-2.3; ISO-17799: 7.1.5; CMS: 2.2.2, 2.2.28]

**PE-21.b** BASIC CONTROL: The organization controls the hardware, firmware, and software entering and exiting the facility, the movement of these items within the facility, and maintains appropriate re-

cords of those items. Delivery and loading areas are controlled and, if possible, isolated from information system and system/media libraries to avoid unauthorized access. Information system hardware, firmware, software, or information belonging to the organization is not removed without authorization.

**PE-21.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-21.s** STRONG CONTROL: To be defined.

**PE-22 SEPARATE FACILITIES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance security by physically separating mission functions and assigning separate resources for those functions.

CONTROL MAPPING: [ISO-17799: 8.1.5, 9.6.2]

**PE-22.b** BASIC CONTROL: Separate resources are used for: (i) development and operational processing; and (ii) critical mission activities and routine operations.

**PE-22.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-22.s** STRONG CONTROL: To be defined.

**PE-23 ALTERNATE WORK SITE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to apply specified requirements to alternate work sites.

CONTROL MAPPING: [ISO-17799: 9.8.2]

**PE-23.b** BASIC CONTROL: Alternate work site security requirements are in place and are consistent with the intent of NIST Special Publication 800-46. Means are available to facilitate communication with information system security staff in case of security problems.

**PE-23.e** ENHANCED CONTROL (Add to basic control):
Only organization-owned (or mission-partner-owned) information systems are used to process, access, or store organizational information. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**PE-23.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** CONTINGENCY PLANNING AND OPERATIONS (CP)

### CP-1 CONTINGENCY PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, an effective response to an information system disruption is enabled by developing a system contingency plan.

CONTROL MAPPING: [NIST 800-26: 9.2.1, 9.3.3; FISCAM: SC-3.1; ISO-17799: 11.1.1, 11.1.2, 11.1.3; DCID 6/3: Cont1; CMS: 5.2.1, 5.2.3, 5.2.5, 5.2.9, 5.4.4, 5.7.1, 5.7.2, 5.7.5, 5.8.1, 6.1.1, 6.1.2; DOD 8500: CODP-3]

**CP-1.b** BASIC CONTROL: A contingency plan is produced for the information system that is compliant with OMB policy and consistent with the intent of NIST SP 800-34. In addition, key affected parties approve the contingency plan for the system. The plan is reviewed once a year, reassessed, tested and, if appropriate, revised to reflect changes in hardware, software and personnel.

**CP-1.e** ENHANCED CONTROL (Add to basic control):
Plan includes checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the plan is being implemented as intended.

**CP-1.s** STRONG CONTROL: To be defined.

### CP-2 CONTINGENCY PLAN TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to train personnel in their contingency roles and responsibilities.

CONTROL MAPPING: [NIST 800-26: 9.3.2; FISCAM: SC-2.3; CMS: 1.1.7, 5.6.1, 5.6.3]

**CP-2.b** BASIC CONTROL: Operational and support personnel (including managers and users of the information system) have received training in contingency operations and understand their emergency roles and responsibilities. Personnel receive periodic training in emergency fire, water, and alarm incident procedures.

**CP-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-2.s** STRONG CONTROL: To be defined.

### CP-3 CONTINGENCY PLAN EXERCISES AND DRILLS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to periodically test contingency plans and response capabilities.

CONTROL MAPPING: [NIST 800-26: 9.3.3; FISCAM: SC-3.1; ISO-17799: 11.1.5; DCID 6/3: Cont2-b; DOD 8500: COED-2; CMS: 5.6.4, 5.7.4; FISCAM: SC-4.1, SC4.2]

**CP-3.b** BASIC CONTROL: Contingency plans [*Selection: in their entirety* | [*Assignment: portions*]] are exercised [*Assignment: time period (e.g., annually, quarterly, or semi-annually)*]. Test results are documented and provided to appropriate organizational officials for review.

**CP-3.e** ENHANCED CONTROL (Add to basic control):
Current plan has been tested under conditions that simulate a disaster. The technology is appropriately considered in periodic tests of the contingency plan and resultant adjustments to the plan. Procedures include checks to be performed and assigned responsibilities for conducting these

checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-3.s** STRONG CONTROL: To be defined.

**CP-4 CONTINGENCY PLAN STORAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by securely storing an up-to-date copy of the contingency plan for the information system off-site.

CONTROL MAPPING: [NIST 800-26: 9.2.10, 9.3.1; FISCAM: SC-3.1; CMS: 5.7.3]

**CP-4.b** BASIC CONTROL: Copies of the current contingency plan are stored in a secure location at an alternate site accessible by management and other key personnel.

**CP-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-4.s** STRONG CONTROL: To be defined.

**CP-5 OFF SITEBACKUP STORAGE SITES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to contingencies by ensuring geographic separation of routine information system operations and backup storage sites.

CONTROL MAPPING: [NIST 800-26: 9.2.9; FISCAM: SC-2.1, SC-3.1; DCID 6/3: Backup3, Backup4-d; CMS: 1.3.6, 5.4.3]

**CP-5.b** BASIC CONTROL: Backup storage sites are geographically removed from the primary site and environmentally and physically protected.

**CP-5.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-5.s** STRONG CONTROL: To be defined.

**CP-6 INFORMATION BACKUP AND RESTORE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to regularly back up information.

CONTROL MAPPING: [NIST 800-26: 9.1.1, 9.2.4, 9.2.5, 9.2.6, 9.2.7; FISCAM: SC-1.1, SC-2.1, SC-3.1; ISO-17799: 8.4.1; DCID 6/3: Avail, Backup1, Backup2, Backup4, Backup5, CM1; CMS: 5.4.1, 5.4.2, 5.11.1, 5.11.2; DOD 8500: CODB-3, COBR-1, COSW-1, ECRR-1, ECTB-1; FISCAM: AC-5.2, SC-2.1]

**CP-6.b** BASIC CONTROL: A capability exists to conduct backup storage and restoration of information and access controls. Information backup for the information system is documented and performed [*Assignment: time period which is at least monthly*]. Procedures are in place to test backup via restoration of information from backup media every [*Assignment: time period which is at least annually*]. Appropriate physical and technical protection of the backup and restoration files, hardware, firmware, and software, (e.g., router tables, compilers, and other security-related system software) are in place. Audit logs/records are backed up not less than weekly onto a different information system or media than the system being audited. Generally, audit logs/records are retained for [*Assignment: time period which is at least every six months*]. For these specific information types, the audit records are retained for the time period indicated: [*Assignment: pairs of information type / time-period*]. System and application documentation are maintained at the off-site storage loca-

tion. The technology is implemented in such a manner as to provide appropriate availability, including consideration of: (i) backup procedures; (ii) system configuration; (iii) redundancy; (iv) environmental controls; (v) staff training; and (vi) routine maintenance. Restoration of any security-relevant segment of the information system state (e.g., access control lists, cryptographic keys, deleted system status information) is possible without requiring destruction of other system information. Standalone computer workstation backup information, software and current operating procedures are stored in accordance with the contingency plan.

**CP-6.e** ENHANCED CONTROL (Add to basic control):
Backup storage location allows prompt restoration of information. Backup files are rotated off-site [*Assignment: time period or criteria for what constitutes sufficient rotation*] to avoid disruption if current files are damaged. Back-up copies of the operating system and other critical software are stored in a fire rated container that is not collocated with the operational software. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-6.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Backup files are rotated off-site [*Assignment: time period or criteria for what constitutes sufficient rotation*] to avoid disruption if current files are damaged. **Information backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.** Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

### CP-7 BACKUP MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable backing up information and the information system state.

CONTROL MAPPING: [DCID 6/3: Backup2, Backup6]

**CP.7.b** BASIC CONTROL: Mechanisms provide for sufficient backup storage capability. Checkpoint capabilities are part of any backup operation that updates files and consumes large amounts of information system time. A capability to conduct the following types of backup exists: (i) full (complete backup); and (ii) [*Selection of one or more: incremental (changes since last incremental) | differential (changes since last full)*].

**CP-7.e** ENHANCED CONTROL (Add to basic control):
Consideration is given to the use of technical features that enhance information integrity and availability including, among others, remote journaling, Redundant Array of Inexpensive Disks (RAID) 1 and above, and similar techniques. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CP-7.s** STRONG CONTROL: To be defined.

### CP-8 ALTERNATE PROCESSING SITE

CONTROL OBJECTIVE: In accordance with organizational policy, documented procedures are being effectively implemented to maintain operations despite contingencies by providing an alternate processing site.

CONTROL MAPPING: [NIST 800-26: 9.2.4; FISCAM: SC-3.1, SC-3.2; DCID 6/3: Cont2-a; CMS: 5.10.1; DOD 8500: COAS-2, COEB-2, COEF-2]

**CP-8.b** BASIC CONTROL: An alternate site is identified that permits [*Assignment: mission or business essential functions*] operations without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)* ] when the primary operations or capabilities are un-

available. Arrangements and agreements are established for alternate facilities that are in a state of readiness commensurate with the risks of interrupted operations. Alternate processing sites are geographically removed from the primary site, and environmentally and physically protected. Arrangements are planned for travel and lodging of necessary personnel if needed.

**CP-8.e** ENHANCED CONTROL (Add to basic control):
An alternate site is identified that permits **full** operations without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations or capabilities are unavailable. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-8.s** STRONG CONTROL: To be defined.

**CP-9 RESTORING INFORMATION UNDER EMERGENCY CONDITIONS**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for physical access to information system facilities under emergency conditions.

CONTROL MAPPING: [DCID 6/3: Access1; CMS: 2.4.1, 2.4.2, 5.5.1, 5.6.2]

**CP-9.b** BASIC CONTROL: Facility access is allowed in support of restoration of lost information under the contingency plan in the event of an emergency. Emergency and temporary access authorizations are: (i) documented on standard forms and maintained on file; (ii) approved by appropriate organization managers; (iii) securely communicated to the security function; and (iv) automatically terminated after a predetermined period.

**CP-9.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-9.s** STRONG CONTROL: To be defined.

**CP-10 INFORMATION SYSTEM RECOVERY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to securely recover the information system after failure or other contingency.

CONTROL MAPPING: [DCID 6/3: Avail, Backup2, Recovery; CMS: 5.2.2; DOD 8500: COTR-1; FISCAM: SC-3.1]

**CP-10.b** BASIC CONTROL: Recovery procedures and mechanisms exist to ensure that recovery is done in a trusted, secure, and verifiable manner. Contingency plans, software procedures, and installed security and backup provisions protect against improper modification of information in the event of an information system failure. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures are in place. Adequate manual processing procedures are available for use until automated operations are restored. Restart capabilities are part of any operation that updates files and consumes large amounts of computer time. Mechanisms to allow for the restoration of the information system in a secure and verifiable manner are implemented. Restoration of operational capabilities with minimal loss of service or information is provided. Assurance is provided that the state of the information system after the restore reflects any security-relevant changes to the system between the backup and the restore. Restoration of any security-relevant segment of the system state (e.g., access control lists, cryptographic keys, deleted system status information) is obtained without requiring destruction of other system data.

**CP-10.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CP-10.s** STRONG CONTROL: To be defined.

**CP-11 MANAGEMENT ACCOUNTABILITY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to hold management accountable for the ability to respond to contingencies.

CONTROL MAPPING: [ISO-17799: 4.1.1, 12.2.1; CMS: 5.2.6]

**CP-11.b** BASIC CONTROL: Management is able to show how the organization responds to specific disasters/disruptions to: (i) protect lives; (ii) limit damage; (iii) protect information; (iv) circumvent security controls only according to established bypass procedures; and (vi) minimize the impact on organizational operations and assets.

**CP-11.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-11.s** STRONG CONTROL: To be defined.

**CP-12 INFORMATION SYSTEM MODIFICATION IMPACT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to re-evaluate contingency plans prior to approving major changes to the information system.

CONTROL MAPPING: [None]

**CP-12.b** BASIC CONTROL: Contingency plans are re-evaluated before proposed changes to the information system are approved to determine if major modifications have security ramifications that require operational changes in order to maintain adequate risk mitigation.

**CP-12.e** ENHANCED CONTROL (Add to basic control):
With respect to necessitating plan re-evaluation, the term "major change" is clearly defined and this definition documented. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-12.s** STRONG CONTROL: To be defined.

**CP-13 ALTERNATE COMMUNICATION SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide for alternate communications services.

CONTROL MAPPING: [DCID 6/3: Commun; CMS: 5.10.2; FISCAM: SC-3.1, SC-3.2]

**CP-13.b** BASIC CONTROL: Arrangements are in place for alternate [*Selection (one or more): long haul | short haul*] communications services capable of restoring adequate communications to accomplish the following mission functions [*Assignment: list of functions*] without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations and communications capabilities are unavailable. Arrangements are planned for travel and lodging of necessary personnel if needed.

**CP-13.e** ENHANCED CONTROL (Add to basic control):
Arrangements are in place for alternate [*Selection of one or more: Long Haul | Short Haul*] communications services capable of restoring adequate communications to accomplish **full operations** without loss of operational continuity within [*Assignment: time period (e.g., twenty-four or seventy-two hours)*] when the primary operations and communications capabilities are unavailable. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CP-13.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** CONFIGURATION MANAGEMENT (CM)

### CM-1 CONFIGURATION MANAGEMENT PLAN

CONTROL OBJECTIVE: Enable knowing the information system configuration and controlling changes throughout the system development life cycle by developing a configuration management plan when the organization's plan is not adequate to address system needs.

CONTROL MAPPING: [DCID 6/3: CM2-a, CM3-a; FISCAM: SP-4]

**CM-1.b** BASIC CONTROL: The configuration management plan for the information system is consistent with the intent of IEEE Standard 828-1998 (or successor if superceded). The configuration management plan is evaluated periodically every [*Assignment: time period (e.g., annually)*] and updated as necessary to verify the plan and the ability of those tasked to carry out the plan.

**CM-1.e** ENHANCED CONTROL (Add to basic control):
Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.

**CM-1.s** STRONG CONTROL: To be defined.

### CM-2 CONFIGURATION MANAGEMENT PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage the configuration of the information system.

CONTROL MAPPING: [NIST 80-26: 10.2.3, 10.2.4, 10.2.5, 10.2.10, 10.2.13; FISCAM: AC-1, AC-2, CM-1, CM-3, SP-4, SS-3.2, CC-1.2, CC-2.1; ISO-17799: 8.1.2, 8.6.4, 10.5.2, 10.5.3, 10.5.4, 12.1.2; DCID 6/3: CM2-b, CM3-c; CMS: 6.3.1, 6.3.2, 6.3.3, 6.3.7, 6.3.10; DOD 8500: DCPD-1]

**CM-2.b** BASIC CONTROL: The configuration management process is consistent with the organization's information technology architecture plans. Formally documented configuration management roles, responsibilities, and procedures to include the management of information system security information and documentation are in place. Changes to the information system are authorized by appropriate organization officials and are not permitted outside of the configuration management process. Personnel involved in configuration management have been trained and are familiar with the organization's configuration management process. The guidance is appropriate for personnel with varying levels of skill and experience. Appropriate tools are used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates. Production program changes are periodically reviewed by appropriate organization officials to determine whether access controls and change controls are being followed. The configuration management plan is evaluated periodically every [*Assignment: time-period (e.g., annually)*].

*Information System Components*

Distribution of new software is controlled. Software licensing agreements are enforced and violations of those agreements are prohibited. The use of personal and public domain software is restricted. The name, brand, type, model, version/release number, and physical location of each information system component (hardware, software, and firmware) are identified and documented.

*Change testing*

Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control). Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control). Test plans include appropriate consideration of security. Unit, integration, and system testing are performed and approved in accordance with the test plan and applying a sufficient range of valid and invalid

conditions. A comprehensive set of test transactions and information is developed that represents the various activities and conditions that will be encountered during information system operation. Test results are documented and appropriate responsive actions are taken based on the results. The type of test information to be used on the information system is specified, (i.e., live or simulated). Test results are reviewed and documented. All patches, upgrades, and new applications are tested prior to deployment (compliance testing).

**CM-2.e** ENHANCED CONTROL (Add to basic control):
Changes to the information system are not technically or procedurally feasible outside of the configuration management process. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-2.s** STRONG CONTROL: To be defined.

### CM-3 BASELINE CONFIGURATION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to document and maintain a current baseline, operational configuration of the hardware, software, and firmware that comprise the information system.

CONTROL MAPPING: [NIST 800-26: 10.2.7, 12.1.1, 12.1.2, 12.1.3, 12.1.7; FISCAM: CC-2.3, CM-2, CM-4; ISO-17799: 5.1.1; CMS: 3.4.6, 6.5.1; DOD 8500: DCHW-1, DCSW-1]

**CM-3.b** BASIC CONTROL: A current and comprehensive baseline inventory of all hardware and firmware (to include manufacturer, type, and version) required to support the operation of the information system is maintained as part of the configuration management plan. A current and comprehensive baseline inventory of all software (to include manufacturer, type, and version and installation manuals and procedures) required to support the operation of the information system is maintained. Backup copies of the inventory are adequately protected. All system software is current and has current and complete documentation. There are information system diagrams and documentation on the setup of routers, switches, guards, firewalls and any other devices facilitating connections to other systems. The current configuration information is routinely validated for accuracy. For distributed information systems, there are software distribution implementation orders including effective date provided to all locations.

**CM-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-3.s** STRONG CONTROL: To be defined.

### CM-4 CHANGE CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to control changes to the information system.

CONTROL MAPPING: [NIST 800-26: 3.1.4, 3.2.1, 3.2.2, 10.2.2, 10.2.3, 10.2.5, 10.2.7, 10.2.10, 10.2.11; FISCAM: SS-3.2, CC-1.2, CC-2.1, CC-2.2, CC-3.1, CM-1, CM-3, CM-6; ISO-17799: 10.4.1, 10.5.1; DCID 6/3: Change2-a, CM3-b; CMS: 3.4.2, 3.5.4, 3.5.6, 6.3.4, 6.3.5, 6.3.6, 6.7.1, 6.7.2, 6.8.1,10.7.3; DOD 8500: DCCB-2, DCPR-1, ECSD-2]

**CM-4.b** BASIC CONTROL: Change control mechanisms maintain control of changes to hardware, software, and security mechanisms. Changes to information system specifications are prepared by the programmer and reviewed by a programming supervisor. System components are tested, documented, and approved (operating system, utility, applications) prior to promotion to production. Program changes are moved into production only upon documented approval from users and appropriate

officials responsible for system development. Software changes are documented so that they can be traced from authorization to the final approved code. Documentation facilitates traceability of code to design specifications and functional requirements. Documentation is updated for software, hardware, operating personnel, and information system users when a new or modified information system is implemented. Implementation orders, including effective date, are provided to all locations and are maintained on file at each location.

*Change Request*

Software change request forms are used to document requests and related approvals. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document. Change requests are approved by appropriate organization officials including, but not limited to, information system users and information system support staff. Change control is effected by: (i) notifying users of the time and date of the last change in information content; (ii) ensuring that changes are executed only by authorized personnel; (iii) ensuring that intended the change is properly implemented; and (iv) providing a secure, unchangeable audit trail to clearly document the change.

*Emergency Changes*

Emergency changes for the information system are documented and approved by appropriate organization officials, either prior to the change or after the fact. Emergency changes to the configuration are appropriately documented and approved and appropriate personnel are notified for analysis and follow-up.

**CM-4.e** ENHANCED CONTROL (Add to basic control):
The information system is under the control of a chartered configuration control board that meets regularly. The program manager/system owner and the information system security official are represented on the control board. An independent library control group performs migration of tested and approved information system software to production use. Images of program code are maintained and compared before and after changes to ensure that only approved changes are made. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CM-4.s** STRONG CONTROL: To be defined.

**CM-5 LIBRARY MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to manage software libraries.

CONTROL MAPPING: [NIST 800-26: 10.1.2; FISCAM: CC-3.2, CC-3.3, CM-3; ISO-17799: 10.4.3; CMS: 3.4.5, 6.4.3, 6.4.4, 6.6.1, 6.8.2; DOD 8500: DCSL-1]

**CM-5.b** BASIC CONTROL: Software libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code. Library management software is used to produce audit trails/logs of program changes, maintain program version numbers, record and report program changes, maintain creation/date information for production modules, maintain copies of previous versions, and control concurrent updates. All deposits and withdrawals of media (e.g., tapes, disks) to/from the software library are authorized and logged. Production source code is maintained in a separate archive library. Separate libraries are maintained for program development and maintenance, testing, and production programs. Outdated versions of information system software are removed from production libraries. A group independent of the user and programmers controls movement of programs and information among libraries.

**CM-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CM-5.s** STRONG CONTROL: To be defined.

**CM-6 CHANGE ACCESS CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce access restrictions associated with change control.

CONTROL MAPPING: [NIST 800-26: 6.1.3, 6.1.4, 10.1.1, 10.1.4, 10.1.5; FISCAM: SS-1.2, SS-2.1, SS-3.1, SD-1, SD-1.1, CM-3; ISO-17799: 9.5.5, 10.4.2 | DCID 6/3: Change1-b; CMS: 2.6.2, 2.10.3, 2.11.3, 3.1.3, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.6.4, 4.3.1, 6.4.1; DOD 8500: ECCD-2, ECPC-2]

**CM-6.b** BASIC CONTROL: Restrictions are in place for accessing information system software and for using and monitoring use of system software utilities. Responsibilities for using system utilities have been clearly defined and are understood by systems programmers. Responsibilities for monitoring use are defined and understood by organization officials. Application programmer privileges to change production systems (programs and data) are limited and are reviewed [*Assignment: time period (e.g., annually)*]. Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features. Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software. Justification and approval by appropriate organization officials for access to systems software is documented and retained. The use of privileged system software and utilities is reviewed by appropriate organization officials periodically every [*Assignment: time period (e.g., annually)*] to ensure that access permissions correspond with position descriptions and job duties.

**CM-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CM-6.s** STRONG CONTROL: To be defined.

**CM-7 MONITORING CHANGE ACTIVITY**

CONTROL OBJECTIVE: In accordance with organizational policy, mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to monitor information system changes and actions by privileged users.

CONTROL MAPPING: [NIST 800-26: 17.1.1, 17.1.6, FISCAM: AC-4.1, SD-2.1; DCID 6/3: Change1-a; CMS: 2.1.6, 3.1.4, 3.4.1, 3.6.1]

**CM-7.b** BASIC CONTROL: System programmers' activities are monitored and reviewed. The use of information system utilities is logged using access control software reports or job accounting information. All accesses to information system software files are logged by automated logging facilities. Installation of all information system software is logged to establish an audit trail/log and is reviewed by appropriate organization officials.

**CM-7.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**CM-7.s** STRONG CONTROL: To be defined.

**CM-8 MINIMAL SERVICES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure systems for only necessary capabilities.

CONTROL MAPPING: [NIST 80-26: 10.3.1; ISO-17799: 8.1.4; DCID 6/3: Audit7, LeastPrv; FISCAM: AC-1, AC-2, SP-4]

**CM-8.b** BASIC CONTROL: The function and purpose of processes and services are documented and approved by appropriate organization officials. The information system is periodically reviewed to identify and eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls). Protocols that would introduce an unacceptable level of risk are disabled; specifically the following protocols are generally disabled [*Assignment: list of protocols.*]. Available processes/services are minimized, such as through: (i) installing only required services; and (ii) restricting the number of individuals with access to such services, based on the concept of least privilege. The information system that supports the server functionality is, as much as possible, dedicated to that purpose.

**CM-8.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-8.s** STRONG CONTROL: To be defined.

### CM-9 SECURE CONFIGURATION SETTINGS, CHECKLISTS, AND BENCHMARKING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure and benchmark information technology products in accordance with good security practice settings.

CONTROL MAPPING: [NIST 800-26: 10.2.6; CMS: 2.5.1, 2.9.8, 3.6.2, 3.6.5, 3.6.6; DOD 8500: DCSS-2, ECSC-1; FISCAM: AC-3.2]

**CM-9.b** BASIC CONTROL: Default settings of security features on the information technology products employed within the information system are set to the most restrictive mode compatible with system operational requirements. Vendor-supplied passwords for component products in the information system are changed. Information system initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. The operating system is configured to prevent circumvention of the security software and application controls. An organization reference document such as a security recommendation guide (SRG), security technical implementation guide (STIG), or security checklist constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired information technology products and all operational information system and hosted applications. If organization reference documents are not available, other government guidelines or vendor literature are acceptable sources. When appropriate tools are available, configurations of information systems are benchmarked using automated scoring tools.

**CM-9.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-9.s** STRONG CONTROL: To be defined.

### CM-10 NETWORK CONFIGURATION SETTINGS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure network parameters to reduce exposures.

CONTROL MAPPING: [NIST 800-26: 16.2.7; ISO-17799: 8.5.1, 9.4.9; DCID 6/3: 7.B.2.d; FISCAM: AC-1]

**CM-10.b** BASIC CONTROL: Networks are appropriately configured to adequately protect access paths between information systems. Each information system boundary interface is configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not ex-

plicitly permitted are prohibited. Trust relationships among hosts and external entities are appropriately restricted to the minimum level necessary to accomplish mission tasks. Security attributes of each network service are clearly described.

**CM-10.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-10.s** STRONG CONTROL: To be defined.

**CM-11 PRIVACY POLICY**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to indicate user privacy is a priority within the organization.

CONTROL MAPPING: [NIST 800-26: 16.3.1; ISO-17799: 12.1.4]

**CM-11.b** BASIC CONTROL: Privacy policies in effect are posted on appropriate information systems (including web sites) within the organization.

**CM-11.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-11.s** STRONG CONTROL: To be defined.

**CM-12 LIMITING TRAFFIC TYPES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to configure the information system to control specified types of traffic.

CONTROL MAPPING: [DOD 8500: ECIM-1, ECVI-1]

**CM-12.b** BASIC CONTROL: Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within organizational information systems. Both inbound and outbound public service instant messaging traffic is blocked at the information system boundary. [Note: This does not include instant messaging services that are configured by an authorized application or site to perform an authorized and official function.] Voice over Internet Protocol traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within organizational information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the information system boundary. [Note: This does not include Voice over Internet Protocol services that are configured by an authorized application or site to perform an authorized and official function.]

**CM-12.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**CM-12.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** HARDWARE AND SOFTWARE MAINTENANCE (MA)

### MA-1 PERIODIC MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct periodic on-site and off-site maintenance of the information system and of the physical plant within which this information system resides.

CONTROL MAPPING: [NIST 800-26: 10.1.3, 10.2.1, 10.2.2; FISCAM: SC-2.4, SC-2.4, SS-3.1, SS-3.2, CC-2.1; ISO-17799: 7.2.4, 7.3.2; DCID 6/3: Maint-a, 8.B.8.c(1), 8.B.8.c(2), 8.B.8.c(3), 8.B.8.c(7), 8.B.8.c(8); CMS: 2.2.30, 5.9.10, 5.9.11]

**MA-1.b** BASIC CONTROL: Comprehensive maintenance testing procedures exist that systematically schedule information system hardware for periodic maintenance inspections and testing to ensure the equipment operates within design specifications and is properly calibrated. Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations. Repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks) are documented. Regular and unscheduled hardware maintenance performed is documented. A maintenance log is maintained and includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort; and (iv) a description of the type of maintenance performed to include identification of replacement parts. Maintenance of information systems is performed on-site whenever possible. If information systems or system components are to be removed from the facility for repair, any component containing non-volatile memory is sanitized or appropriate\ cleared and its release is explicitly approved by an appropriate organization official. Maintenance changes that impact the security of the information system receive a configuration management review. After maintenance is performed on the information system, the security features are checked to assure that they are still functioning properly. Maintenance is performed in a manner that maintains security.

**MA-1.e** ENHANCED CONTROL (Add to basic control):
Problems and delays encountered, the reason and elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends. Management periodically reviews and compares the service performance achieved with goals and surveys user departments to see if their needs are being met. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-1.s** STRONG CONTROL: To be defined.

### MA-2 MAINTENANCE TOOLS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control and monitor the use of maintenance tools.

CONTROL MAPPING: [NIST 800-26: 10.1.3, 11.2.4; DCID 6/3: Maint-c, 8.B.8.c(4), 8.B.8.c(5), 8.B.8.c(6) (all)]

**MA-2.b** BASIC CONTROL: Introduction of network analyzers (e.g., sniffers) that allow maintenance personnel the capability to monitor the content of network traffic are approved by an appropriate organization official prior to being introduced into an information system. If maintenance personnel bring diagnostic test programs (e.g., software/firmware used for maintenance or diagnostics) into a facility, the media containing the programs are checked for malicious code before the media is connected to the information system.

**MA-2.e** ENHANCED CONTROL (Add to basic control):

Before leaving the facility, the media are checked to assure that no organizational information has been written on it. All diagnostic equipment and other devices carried into a facility by maintenance personnel are handled as follows: (i) all diagnostic and test equipment is inspected for obvious improper modification; (ii) maintenance equipment that has the capability of retaining information is appropriately sanitized before being released; (iii) if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless explicit exception is authorized by an appropriate organization official. Replacement components that are brought into the facility for the purpose of swapping with facility components are allowed. However, any component placed into an information system remains in the facility until proper release procedures are completed. Any component that is not placed in an information system may be released from the facility. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-2.s** STRONG CONTROL: To be defined.

### MA-3 REMOTE MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to provide additional controls on remotely executed maintenance.

CONTROL MAPPING: [NIST 800-26: 10.1.1; FISCAM: SS-3.1, AC-1; ISO-17799: 9.4.5; DCID 6/3: Maint-d, 8.B.8.d(all)]

**MA-3.b** BASIC CONTROL: Installation and use of remote diagnostic links are specifically addressed in the security plan and agreed to by the authorizing official. Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. The communications links connecting the components of the information system, associated information communications, and networks are protected in accordance with the FIPS Publication 199 security category of the information that may be transmitted over the link. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed. Unless an exception has been granted by an appropriate organization official, maintenance personnel accessing the information system at the remote site are cleared to the highest FIPS Publication 199 security category of information processed on that system, even if the system was downgraded/sanitized prior to remote access. An audit log is maintained of all remote maintenance, diagnostic, and service transactions including all commands performed and all responses. The log is periodically reviewed by an appropriate organization official. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as tokens; (iii) and remote disconnect verification. Where possible, remote sessions involve an interactive window for coordination with information security official responsible for the system being serviced. When the remote maintenance has been completed, all sessions are terminated and the remote connection is also terminated. Authenticators (e.g.,, passwords) used during remote maintenance are changed following each remote maintenance service.

**MA-3.e** ENHANCED CONTROL (Add to basic control):
Keystroke monitoring is performed on all remote diagnostic or maintenance services. A technically qualified person reviews the maintenance log, and if appropriate, the audit log to assure the detection of unauthorized changes. Maintenance technicians responsible for performing remote diagnosis/maintenance are advised (e.g., contractually, verbally, or by banner) prior to remote diagnostics/maintenance activities that keystroke monitoring will be performed. Procedures include

checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-3.s** STRONG CONTROL: To be defined.

### MA-4 MAINTENANCE PERSONNEL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to control the authorization of an individual to perform maintenance.

CONTROL MAPPING: [NIST 800-26: 10.1.1, 10.1.3; FISCAM: SS-3.1; DOD 8500: PRMP-2; DCID 6/3: 8.B.8.a(all), 8.B.8.b(all)]

**MA-4.b** BASIC CONTROL: The list of authorized maintenance personnel is documented. Only personnel authorized to do so perform maintenance on the information system. Except as authorized by the authorizing official, personnel who perform maintenance on the information system are authorized access to the highest FIPS Publication 199 security category of information processed on that system. Such personnel who perform maintenance or diagnostics on an information system do not require an escort, unless need-to-know controls must be enforced. However, a facility employee who is authorized to access the highest FIPS Publication 199 security category of information and, when possible, technically knowledgeable, is present within the area where the maintenance is being performed to assure that the proper security procedures are being followed. Foreign nationals (with proper authorizations) may be utilized as maintenance personnel for those information systems jointly owned and operated by the US and a foreign allied government, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions are fully documented within a Memorandum of Agreement. A person not authorized access to the information system may be used to perform maintenance on the system provided an escort who is authorized access and is technically qualified monitors and records that person's activities in a maintenance log.

**MA-4.e** ENHANCED CONTROL (Add to basic control):
Prior to maintenance, the information system is completely cleared and all nonvolatile information storage media removed or physically disconnected and secured. When an information system cannot be cleared, approved procedures are enforced to deny the maintenance personnel visual and electronic access to any organization information that is contained on the system. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-4.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Prior to maintenance, the information system is completely cleared and all nonvolatile information storage media removed or physically disconnected and secured. When an information system cannot be cleared, approved procedures are enforced to deny the maintenance personnel visual and electronic access to any organization information that is contained on the system. **For US-owned and operated information systems, maintenance personnel must be US citizens. A separate copy of the operating system and application software, including any micro-coded floppy disks, cassettes, or optical disks that are integral to the information, that has not been used in the processing of organizational information is used for all maintenance operations performed by personnel not authorized access to information processed by the system. The copy is labeled "For Maintenance Only" and protected in accordance with procedures established in the security plan.** Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

### MA-5 TIMELY MAINTENANCE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that maintenance services and parts are available in a timely manner.

CONTROL MAPPING: [DCID 6/3: Maint-b; DOD 8500: COMS-2, COPS-2; CMS: 9.9.8, 5.9.9; FISCAM: SC-2.4]

**MA-5.b** BASIC CONTROL: Spare or backup hardware is used to provide a high level of information system availability for organization applications. Maintenance support and critical maintenance spares and spare parts for [*Assignment: list of key information system assets*] can be obtained within [*Assignment: time period (e.g., twenty-four hours)*] of failure.

**MA-5.e** ENHANCED CONTROL (Add to basic control):
Maintenance support and critical maintenance spares and spare parts for **all information system assets** can be obtained within [*Assignment: time period (e.g., twenty-four hours)*] of failure. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-5.s** STRONG CONTROL: To be defined.

### MA-6 MAINTENANCE SCHEDULING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to schedule maintenance operations and accommodate unscheduled maintenance with minimal mission impact.

CONTROL MAPPING: [NIST 800-26: 10.2.8, 10.2.11, 10.2.12; FISCAM: CC-2.2, SC-2.1, SC-2.4; CMS: 3.4.4, 5.9.5, 5.9.6]

**MA-6.b** BASIC CONTROL: Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing. A retrievable, exact copy of electronic information exists before movement of equipment used to process such information. Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted. Emergency change requests are approved by management either prior or after the fact. Flexibility exists in the organization's operations to accommodate regular and a reasonable amount of unscheduled hardware maintenance. Version control is maintained and contingency plans are updated after any changes.

**MA-6.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MA-6.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** SYSTEM AND INFORMATION INTEGRITY (SI)

### SI-1 FLAW REMEDIATION PROCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate flaw remediation for the information system.

CONTROL MAPPING: [NIST 800-26: 10.3.2, 11.1.1, 11.1.2, 11.1.2, 11.2.2, 11.2.7; FISCAM: SS-2.2, CM-5; ISO-17799: 6.3.2, 6.3.3, 8.3.1, 8.4.3; DCID 6/3: Integrty2, F.2(all); CMS: 2.1.7, 3.5.3; DOD 8500: DCCT-1]

**SI-1.b** BASIC CONTROL: Significant weaknesses in the operational information system are reported and effective remedial actions are taken. This includes the following:

*Patch Management*

Systems affected by recently announced software vulnerabilities are identified. Patches are installed on a timely basis and tested for effectiveness and potential side effects on the organization's information systems. There is verification that patches, service packs, and hot fixes are appropriately installed on affected systems.

*System Software Problems*

A log is used to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.

*Malicious Code Screening*

As needed, incoming information is reviewed for viruses and other malicious code. Anti-viral mechanisms are used to detect and eradicate viruses transported by e-mail or attachments. The information system is automatically safeguarded from virus infections from other sources as well (e.g., central choke points where diskettes are scanned for viruses prior to distribution). There is timely updating of those mechanisms intended to prevent the introduction of malicious code (e.g., updating anti-viral software).

*Miscellaneous*

Software is up-to-date (latest versions of service packs, patches, and hot fixes are installed). Security weaknesses are being reported and acted upon. Software malfunctions are being reported and acted upon. Hardware fault control routines are logged to indicate all detected errors and determine if recovery from the malfunction is possible.

**SI-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SI-1.s** STRONG CONTROL: To be defined.

### SI-2 PERSONNEL SUPERVISION

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure adequate supervision of personnel and review of their activities.

CONTROL MAPPING: [NIST 800-26: 17.1.6, 17.1.8; FISCAM: AC-4.3, SD-2.2; ISO-17799: 8.4.2; CMS: 1.10.2, 4.2.2, 4.2.4, 4.4.2]

**SI-2.b** BASIC CONTROL: Active supervision and review are provided for all personnel, including each shift for computer operations. Staff's performance is monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out. Supervisors routinely review user activity logs for incompatible actions and investigate any abnormalities. All mission/business partners are reviewed for compliance with information systems security requirements.

**SI-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SI-2.s** STRONG CONTROL: To be defined.

**SI-3 PROCEDURAL REVIEW**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are periodically reviewed.

CONTROL MAPPING: [NIST 800-26: 2.1.1, 6.1.2, 6.1.3; FISCAM: SP-5.1, SD-1, SD-1.1, SD-2.2; ISO-17799: 3.1.2; CMS: 3.1.2, 4.4.1; DOD 8500: DCAR-1]

**SI-3.b** BASIC CONTROL: A review is conducted every [*Assignment: time period (e.g., twelve months)*] that comprehensively evaluates existing security policies and procedures to ensure procedural consistency and to ensure that they fully support the goal of enabling mission accomplishment. Access authorizations are periodically reviewed for incompatible functions. Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels.

**SI-3.e** ENHANCED CONTROL: To be defined.

**SI-3.s** STRONG CONTROL: To be defined.

**SI-4 SOFTWARE AND INFORMATION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to both protect against and to detect unauthorized changes to software.

CONTROL MAPPING: [NIST 800-26: 11.2.1, 11.2.4, 11.2.5, 11.2.9; ISO-17799: 8.7.6, 10.3.3; DCID 6/3: Integrty1, Integrty2, SysAssur1-b, SysAssur2, 7.B.2.a(1); DOD 8500: ECND-2, ECTM-2; FISCAM: AC-4]

**SI-4.b** BASIC CONTROL: Integrity verification applications are available on the information system to look for evidence of information tampering, errors, and omissions. Tools for automatically monitoring the integrity of the information system and the applications it hosts are implemented. Good engineering practice with regard to commercial off-the-shelf integrity mechanisms, such as parity checks and cyclical redundancy checks are employed. The operating system's operational status and restart integrity is protected during and after shutdowns. Mechanisms prohibit users from modifying the functional capabilities of boundary protection devices such as firewalls, gateways, and routers. There is limited write access to information system security capabilities (that is., the hardware, software, and firmware that perform operating system or security functions and the hardware, software, and firmware that must be relied upon in order for the system security functionality to operated correctly).

**SI-4.e** ENHANCED CONTROL (Add to basic control):
Message authentication codes, cryptographic hashes, digital signatures and digitally signed timestamps or notarizations are implemented using current standards (i.e., FIPS 198 HMAC, AES-MAC, FIPS 180-2, FIPS 186-3) or subsequently adopted standards, for ensuring the integrity of stored or archived files. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SI-4.s** STRONG CONTROL: To be defined.

**SI-5 VALIDATION OF MISSION PROCESSING**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable verification of mission processing.

CONTROL MAPPING: [NIST 800-26: 11.2.1, 11.2.2; FISCAM: SS-2.2; ISO-17799: 10.2.1, 10.2.2, 10.2.4; DCID 6/3: Change2-b; CMS: 2.1.3, 8.1.1, 8.2.2, 8.3.1, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.5.1, 9.1.2, 9.2.1, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.8.2, 9.8.3; DOD 8500: ECDC-1]

**SI-5.b** BASIC CONTROL:

*Input*

Information input to application systems that is directly related to the accomplishment of organization missions is validated to ensure that it is correct and appropriate. Effective use is made of automated entry devices to reduce the potential for information entry errors. Validation and editing are performed at the computer workstation during information entry or are performed as early as possible in the information flow and before updating the master files. All information fields are checked for errors before rejecting a transaction.

*Processing*

Mechanisms are implemented to verify processing of information that is directly related to the accomplishment of organization missions. For example: (i) reconciliation routines are used by information system applications, (i.e., checksums, hash totals, record counts); (ii transaction-based systems (e.g., database management systems, transaction processing systems) implement transaction rollback and transaction journaling, or the technical equivalents of those processes; (iii) computer matching of transaction information with information in master or suspense files occurs to identify missing or duplicate transactions; (iv) trailer labels or control records containing record counts and control totals are generated for all computer files and tested by application programs to determine that all records have been processed; (v) computer-generated control totals (run-to-run totals) are automatically reconciled between jobs to check for completeness of processing; (vi) system interfaces require that the sending system's output control counts equal the receiving system's input counts; (vii) error reports or error files accessible by computer workstations show rejected transactions with error messages that have clearly understandable corrective actions for each type of error; (viii) rejected information is automatically written on an automated suspense file and held until corrected; (ix) each erroneous transaction is annotated with codes indicating the type of error, date and time the transaction was processed and the error identified, and the identity of the user who originated the transaction; (x) general controls effectively protect the suspense file from unauthorized access and modification; (xi) the suspense file is purged of transactions as they are corrected; (xii) record counts and control totals are established over the suspense file and used in reconciling transactions processed; (xiii) programmed validation and edits include checks for reasonableness, dependency, existence, mathematical accuracy, range, check digit, document reconciliation, and relationship or prior information matching, and (xiv) suspense file is regularly reviewed by management for analysis of the level and type of transaction errors and the age of uncorrected errors.

*Output*

Output from an information system that is directly related to the accomplishment of organization missions is validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Action is taken if inappropriate activities are discovered.

**SI-5.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SI-5.s** STRONG CONTROL: To be defined.

**SI-6 SYSTEM OPERATION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to verify the correct operation of security and security-relevant functionality.

CONTROL MAPPING: [DCID 6/3: SysAssur1-a, SysAssur2, SysIntgr1, Validate]

**SI-6.b** BASIC CONTROL: Mechanisms are in place to validate the expected operation of the security-relevant software, hardware, and firmware. These mechanisms are exercised [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: time-period*]].

**SI-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SI-6.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** MEDIA PROTECTION (MP)

### MP-1 MEDIA ACCESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure adequate supervision of personnel and review of their activities to protect against unauthorized receipt, change, or destruction of electronic and paper media.

CONTROL MAPPING: [NIST 800-26: 8.2.1, 8.2.2, 8.2.6, 8.2.7; ISO-17799: 5.2.2, 8.6.1, 8.6.3; CMS: 1.3.8, 2.2.2; DCID 6/3: 8.B.4]

**MP-1.b** BASIC CONTROL: Unauthorized individuals cannot read, copy, alter, or destroy information in printed form or on media removed from the information system. Media accountability and control mechanisms (e.g., audit trail logs), provide protection comparable to that for equivalent paper documents. Electronic media is controlled and protected in a manner similar to that used for paper materials. Output from the information system is given only to authorized users. Random or representative sampling techniques are used to verify the proper marking of large volumes of output. If available and approved, automated techniques are used to verify the proper output marking of information.

**MP-1.e** ENHANCED CONTROL (Add to basic control):
Review of Human-Readable Output: Before human-readable output is released outside the information system, an appropriately authorized individual provides a reliable review of the output to determine whether it is accurately marked with the appropriate and applicable security markings. The review is at a level of detail to allow reviewer to accept security responsibility for releasing the information to its recipient. Explicit approval is obtained from the appropriate organization official before forwarding output, which has not had a reliable review for appropriate marking, to recipients who do not have access to the information system. Such approval(s) can be for a specific release, for the overall release procedure(s), or for both. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-1.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Review of Human-Readable Output: Before human-readable output is released outside the information system, an appropriately authorized individual provides a reliable review of the output to determine whether it is accurately marked with the appropriate and applicable security markings. The review is at a level of detail to allow the reviewer to accept security responsibility for releasing the information to its recipient. **Electronic output (i.e., softcopy) to be released outside the information system is verified by a review (in human-readable form) of all information including embedded text (e.g., headers and footers, hidden text, notes, edited text, control characters) before being released. Information on media that is not in human-readable form (e.g., embedded graphics, sound, video, imagery) is examined for content with the appropriate software, hardware, and firmware. Care is required to ensure that all layers or levels of the graphics or image are reviewed.** Explicit approval is obtained from the appropriate organization official before forwarding output, which has not had a reliable review for appropriate marking, to recipients who do not have access to the information system. Such approval(s) can be for a specific release, for the overall release procedure(s), or for both. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

### MP-2 LABELING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate securing electronic and paper media by incorporating security labels.

CONTROL MAPPING: [NIST 800-26: 8.2.5, 8.2.6, 10.2.9; FISCAM: CC-3.1; ISO-17799: 5.2.2; DCID 6/3: Label1, Label2, 8.B.2.a(all), 8.B.2.b(all), 8.B.2.c(all), 8.B.2.d(all)]

**MP-2.b** BASIC CONTROL: Appropriate security labels that reflect the distribution limitations and handling caveats of the information are affixed to all information system output. Removable information storage media contain external labels indicating the distribution limitations and handling caveats of the information.

*Marking Human-Readable Output*

Human-readable output is marked appropriately, on each human-readable page, screen, or equivalent (e.g., the label appears on each microfiche *and* on each page of text on the fiche). Individual pages of output are marked as appropriate either: (i) to reflect the distribution limitations and handling caveats and applicable associated security markings of the information that is printed on each page; or (ii) with the most restrictive limitations and caveats and all applicable associated security markings of the information that is to be printed.

*Variations*

The following specific types of media or hardware components need not be marked so long as they remain within a single, secure environment: [*Assignment: list of media types and hardware components*].

**MP-2.e** ENHANCED CONTROL (Add to basic control):
Security labels are an integral part of the electronic media contents.

*Adding a Banner Page*

The first page of the output (the banner page) includes a warning message reminding the person receiving the output to control every page according to the markings on the banner page until a reliable human review has determined that the output is marked appropriately. If the capability to provide automatic banner pages does not exist, printed output is marked manually or other steps taken to ensure output is reviewed, as appropriate.

Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-2.s** STRONG CONTROL: To be defined.

**MP-3 MEDIA TRANSPORT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to help protect electronic and paper media that is physically transported.

CONTROL MAPPING: [NIST 800-26: 8.2.2, 8.2.4; ISO-17799: 7.3.2, 8.7.3; CMS: 1.1.3, 2.2.12]

**MP-3.b** BASIC CONTROL: Only authorized users pick up, receive, or deliver input and output information and media from the information system. Appropriate controls are established for all information entering or leaving the facility, including for mailing media and/or printed output from the information system. Erroneous or unauthorized transfer of information, regardless of media or format, is precluded.

**MP-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-3.s** STRONG CONTROL: To be defined.

**MP-4 MEDIA DESTRUCTION AND DISPOSAL**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the destruction and disposal of media, both electronic and paper, to ensure that organizational information does not become available to unauthorized personnel.

CONTROL MAPPING: [NIST 800-26: 3.2.11, 3.2.12, 3.2.13, 8.2.8, 8.2.10, 10.1.3; FISCAM: AC-3.4, AC-4; ISO-17799: 7.2.6, 8.6.1, 8.6.2; CMS: 1.3.4, 1.3.5, 1.3.7, 1.3.11, 1.3.13; DOD 8500: PEDD-1]

**MP-4.b** BASIC CONTROL: Information system hardware and machine-readable media are cleared, sanitized, or destroyed before being reused or released outside of the organization. Retired, damaged, discarded, or unneeded information is disposed in a manner that prevents unauthorized persons from using it. Information is never disclosed during disposal unless authorized by statute. Cleared or sanitized media that previously contained information at a designated FIPS Publication 199 security category (for confidentiality) is reused at the same or higher security category. Sanitized media is downgraded only with appropriate approval(s).

*Destruction of Paper Media*

Hard copy documents are destroyed when no longer needed. For information requiring such protection, destruction methods for organizational information in paper form are as follows: (i) burning - the material is burned in either an incinerator that produces enough heat to burn the entire bundle or the bundle is separated to ensure all pages are consumed; (ii) mulching or pulping - all material is reduced to particles one inch or smaller; (iii) shredding or disintegrating - paper is shredded in cross-cut shredders (preferred) or strip shredders (alternative). Information storage media is destroyed in accordance with organization-approved methods. An authorized contractor accomplishes document destruction in the absence of the organization's direct participation.

*Release of Systems and Components*

Equipment removal procedures for information systems and components that have processed or contained organizational information are followed. This includes inspection of the information system by designated individuals to ensure that all media, including internal disks, have been removed or sanitized.

**MP-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-4.s** STRONG CONTROL: To be defined.

**MP-5 MEDIA SANITIZATION AND CLEARING**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the sanitization and clearing of media, both electronic and paper.

CONTROL MAPPING: [NIST 800-26: 8.2.8, 8.2.10, 10.1.3; FISCAM: AC-3.4; ISO-17799: 8.6.2; DOD 8500: PECS-2; DCID 6/3: 8.B.5(all)]

**MP-5.b** BASIC CONTROL: Only approved equipment or software is used to degauss or overwrite magnetic media containing organizational information. Degaussing equipment is tested for correct performance every [*Assignment: time period (e.g., annually)*]. Each action or procedure taken to overwrite or degauss such media is verified.

*Optical Disks*

Optical disks (including compact disk/read only memory, write once/read many, digital versatile disk, and read-write compact discs) offer no mechanism for sanitization.

*Sanitizing*

Magnetic media containing organizational information are sanitized by use of an approved degaussing procedure.

*Clearing*

To clear magnetic media, all memory locations are overwritten three times (the first time with a random character, the second time with a specified character, and the third time with the complement of that specified character). The success of the overwrite procedure is verified through random sampling of the overwritten media. Items that have been cleared (i.e., not sanitized) remain at the previously designated FIPS Publication 199 security category (for confidentiality) and remain in a secure, controlled environment.

**MP-5.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-5.s** STRONG CONTROL: To be defined.

### MP-6 MEDIA-RELATED RECORDS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the maintenance of disposition records for media, both electronic and paper.

CONTROL MAPPING: [NIST 800-26: 8.2.3, 8.2.7, 10.1.2; FISCAM: CC-3.2, CC-3.3, AC-6; CMS: 1.3.12, 1.3.13, 9.6.5]

**MP-6.b** BASIC CONTROL: Audit trails are used for receipt of inputs/outputs from the information system. A record is kept of who implemented the media disposal actions and who verified that the information or media was properly sanitized. Inventory records of all storage media containing organizational information are maintained for purposes of control and accountability. Such storage media, any hard copy printout of such media, or any file resulting from the processing of such media are recorded in a log that identifies: (i) date received; (ii) reel/cartridge control number contents; (iii) number of records if available; (iv) movement; and (v) if disposed of, the date and method of destruction. Such a log permits all storage media containing organizational information (including those used only for backups) to be readily identified and controlled. All withdrawals of such storage media from the storage area or library are authorized and logged. Periodic inventories of removable storage devices and media containing organizational information are performed every [*Assignment: time period (e.g., semi-annually)*]. When removable storage devices and media containing organizational information are secured, a proper acknowledgement form is signed and returned to the originator. Each output produced is logged, manually if not automatically, including the recipient(s) who receive the output. A record of the equipment release is created indicating the procedure used for sanitization, and to whom the equipment is intended. This record is retained for [*Assignment: time period (e.g., five years)*]. Logging of shipping and receipts and periodic reconciliation of these records is accomplished every [*Assignment: time period (e.g., monthly)*].

**MP-6.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-6.s** STRONG CONTROL: To be defined.

### MP-7 MEDIA STORAGE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate the secure storage of media, both electronic and paper.

CONTROL MAPPING: [ISO-17799: 5.2.2, 8.6.3; DCID 6/3: Storage, 8.B.9]

**MP-7.b** BASIC CONTROL: Storage media are physically controlled and safeguarded in the manner prescribed for the highest security category (for confidentiality) of the information ever recorded on it until destroyed or sanitized using approved procedures. In those areas where organizational information is processed, unmarked media that are not in factory-sealed packages are protected at the highest FIPS Publication 199 security category (for confidentiality) for information processing conducted within the facility, until the media is reviewed and appropriately labeled. Records management for information stored in an information system or on external media are governed by the records management policies of the appropriate agency, based on the guidelines from the National Archives and Records Agency.

**MP-7.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**MP-7.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** INCIDENT RESPONSE (IR)

### IR-1 INCIDENT RESPONSE PLAN

CONTROL OBJECTIVE: In accordance with organizational policy, enable effective response to incidents by developing an incident response plan when the organizational response plan is not adequate to address information system requirements.

CONTROL MAPPING: [ISO-17799: 12.1.7; DOD 8500: VIIR-2; DCID 6/3: 8.B.7.a; FISCAM: AC-5.1]

**IR-1.b** BASIC CONTROL: An incident response plan consistent with NIST Special Publication 800-61 is developed for the information system that defines reportable incidents, outlines a standard operating procedure for incident response (to include actions to protect evidence in support of forensics), provides for user training, and establishes an incident response team. The incident response plan is tested at least [*Assignment: time period (e.g., semi-annually)*]. The test results are used to modify the incident response plan as necessary to ensure effectiveness.

**IR-1.e** ENHANCED CONTROL (Add to basic control):
Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.

**IR-1.s** STRONG CONTROL: To be defined.

### IR-2 INCIDENT MONITORING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to conduct ongoing monitoring of the information system for security events.

CONTROL MAPPING: [NIST 800-26: 14.1.3, 17.1.7, 17.1.8, FISCAM: AC-4.3, AC-5.1, AC-5.2, AC-5.3; DCID 6/3: Audit5-b, Audit8-b; CMS: 2.6.1]

**IR-2.b** BASIC CONTROL: Information system-related security incidents are monitored and tracked until resolved. Information system performance monitoring is used to analyze performance logs in real time (or near-real time) to look for availability problems, including active attacks. Network activity logs for the information system are maintained and reviewed. Collected audit information is reviewed at least [*Assignment: time period that is at least weekly*]; taking advantage of audit reduction and analysis tools to effectively review information for unusual or suspicious activity or violations. Physical access to facilities is monitored and remedial actions taken, as appropriate.

**IR-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IR-2.s** STRONG CONTROL: To be defined.

### IR-3 INCIDENT RESPONSE

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to respond to security incidents.

CONTROL MAPPING: [NIST 800-26: 14.1.2, 14.1.3, 14.1.5 14.2.1, 14.2.2, 14.2.3; FISCAM: SP-3.4, AC-5.1, AC-5.3; ISO-17799: 4.1.6, 6.3.1, 6.3.4, 6.3.5, 8.1.3, 8.3.1, 12.1.7; CMS: 1.4.5, 1.6.1, 2.6.1, 2.13.1, 2.13.2, 2.13.3, 3.1.1; DCID 6/3: 8.B.7.b, 8.B.7.c(all)]

**IR-3.b** BASIC CONTROL: Reports of possible security violations and security incidents are accurate and timely. For security incidents, the organization defines appropriate parameters for response that includes: (i) what information employees must provide; (ii) whom they must notify; and (iii) what degree of urgency to place on reporting. Intrusion detection reports are routinely reviewed and

suspected incidents handled accordingly. Records of information system activity, such as security incident tracking reports, are regularly reviewed. Security managers investigate security violations, security incidents, and suspicious activities (e.g., failed logon attempts, other failed access attempts; and questionable activity) and report results to appropriate organization officials. Incident information is reported to one or more of the following organizations: the Federal Computer Incident Response Center, the National Information Protection Center, the U.S. Department of Justice and state and local law enforcement agencies as required. Actions are taken to protect and avoid corrupting potential evidence in support of potential forensics.

In response to reported security violations and security incidents, appropriate actions (including disciplinary actions) are taken by organization officials. Access control policies and techniques are modified when violations, incidents, and related risk assessments indicate that such changes are appropriate. An effective malicious software protection and recovery process is implemented. Information system alerts/advisories are received on a regular basis. Alerts and advisories are issued to personnel and responded to, when appropriate. Incident information and common vulnerability and threat information are shared with owners of connected information systems.

**IR-3.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IR-3.s** STRONG CONTROL: To be defined.

### IR-4 HELP DESK

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to facilitate incident response by providing a central incident support resource for information system users.

CONTROL MAPPING: [NIST 800-26: 8.1.1]

**IR-4.b** BASIC CONTROL: There is a help desk or group that offers advice to users of the information system and plays an appropriate role in the organization's incident response program.

**IR-4.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IR-4.s** STRONG CONTROL: To be defined.

### IR-5 INTRUSION DETECTION SYSTEMS AND TOOLS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide attack detection capability for the information system.

CONTROL MAPPING: [NIST 800-26: 11.2.5, 11.2.6; ISO-17799: 8.5.1, 12.3.2; DCID 6/3: Audit2-b, Audit9, Monit; CMS: 2.1.3, 2.1.4, 2.2.1,10.2.1, 10.2.3; DOD 8500: ECID-1; FISCAM: AC-5.1, AC-5.2]

**IR-5.b** BASIC CONTROL: An effective intrusion detection system (hardware, software, or firmware) is implemented, providing real-time identification of unauthorized use, misuse, and abuse of the information system. The intrusion detection system includes appropriate placement of intrusion detection sensors and definition of incident thresholds. Security controls on the information system can detect unauthorized access attempts. Auditable events (single events and the accumulation of events) that may indicate an imminent violation of security policies are routinely monitored. Selected information system components at critical control points (e.g., servers and firewalls) provide logs of network and system activity. Host-based intrusion detection systems are deployed for major applications and for network management assets such as routers, switches, and domain

name servers. All significant events, including access to and modifications of information systems, are logged. Intrusion detection system logs contain appropriate information needed for effective review. Access to audit logs is adequately controlled. Virtual private network traffic is visible to network intrusion detection systems. Appropriate organization officials are notified in case of suspicious events. The organization [*Assignment: response (e.g., least disruptive action or a specific action*] to terminate the suspicious events.

**IR-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IR-5.s** STRONG CONTROL: To be defined.

**IR-6 MALICIOUS CODE PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to identify and isolate suspected malicious software (e.g., viruses, worms, etc.).

CONTROL MAPPING: [NIST 800-26: 11.1.1, 11.1.2; ISO-17799: 8.3.1, 8.5.1, 10.5.4; DCID 6/3: Integrty2, MalCode; CMS: 10.2.2; DOD 8500: ECVP-1; FISCAM: CM-5]

**IR-6.b** BASIC CONTROL: The information system (including servers, workstations and mobile computing devices) implements malicious code protection that includes a capability for automatic updates. Virus definitions are up-to-date. Virus-scanning software is provided at critical entry points, such as remote-access servers and at each desktop system on the network. Anti-viral mechanisms are used to detect and eradicate viruses in incoming and outgoing e-mail and attachments.

**IR-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IR-6.s** STRONG CONTROL: To be defined.

## OPERATIONAL CONTROLS

**FAMILY:** SECURITY AWARENESS AND TRAINING (AT)

### AT-1 SECURITY AWARENESS

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that information system users are aware of the system security requirements and their responsibilities toward enabling effective mission accomplishment.

CONTROL MAPPING: [NIST 800-26: 13.1.1, 13.1.3, 13.1.5; ISO-17799: 6.2.1; CMS: 1.1.1, 1.1.3, 1.1.8, 1.4.4, 4.6.1, 4.6.3; FISCAM: SD-1.3]

**AT-1.b** BASIC CONTROL: Each information system user is aware of the system security requirements and that user's security responsibilities prior to being authorized access to the system. Security awareness includes continual security awareness training conducted every [*Assignment: time period, typically annually*]. Users have received a copy of or have easy access to: (i) organizational security policies and procedures; and (ii) and rules of behavior for the information system or a user manual containing such rules. All employees fully understand their duties and responsibilities in accordance with their job descriptions as described in NIST Special Publications 800-16 and 800-50.

**AT-1.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AT-1.s** STRONG CONTROL: To be defined.

### AT-2 SECURITY TRAINING

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that all personnel with significant information system security responsibilities receive appropriate security training.

CONTROL MAPPING: [NIST 800-26: 13.1.2, FISCAM: SP-4.2, SD-1.2, SP-5, SP-7.2; ISO-17799: 6.2.1, 8.3.1; CMS: 1.1.2, 1.1.4, 1.1.5, 1.1.6; DOD 8500: DCBP-1; DCID 6/3: 8.B.1.b(all), 8.B.1.c(all)]

**AT-2.b** BASIC CONTROL: The organization identifies all positions and/or roles with significant information system security responsibilities. A security training program consistent with NIST Special Publications 800-16 and 800-50 provides training for individuals within the organization with specific information system security responsibilities. Security training is adjusted to the level of the employee's responsibilities. Employees receive adequate training and have the needed security expertise and skills identified in job descriptions. The employees acknowledge, in writing, having received the security and awareness training. A record of the security subjects covered during training is maintained. Employee training and professional development are documented and monitored. Skill needs are accurately identified and included in job descriptions.

**AT-2.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AT-2.s** STRONG CONTROL: To be defined.

## TECHNICAL CONTROLS

**FAMILY:** IDENTIFICATION AND AUTHENTICATION (IA)

### IA-1 INDIVIDUAL IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable reliable identification of individual users of the information system.

CONTROL MAPPING: [NIST 800-26: 15.1; ISO-17799: 9.5.2; DCID 6/3: I&A1, I&A2; CMS: 2.2.21; DOD 8500: IAIA-1; FISCAM: AC-3.2]

**IA-1.b** BASIC CONTROL: Identification and authentication mechanisms are implemented that include provisions for uniquely identifying and authenticating entities (i.e., users or information system processes acting on behalf of users). Information system access is gained through the presentation of an individual-identifier (e.g., a unique token or user login ID) and authenticator(s). Any user actions that can be performed prior to reliable identification are explicitly identified (e.g., reading a publicly available web site).

**IA-1.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-1.s** STRONG CONTROL: To be defined.

### IA-2 REMOTE, PRIVILEGED ACCESS AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enhance authentication for remote access to the information system.

CONTROL MAPPING: [NIST 800-26: 16.2.4; ISO-17799: 9.4.3, 9.4.4; DCID 6/3: I&A5, 7.B.2.i(1); FISCAM: AC-1]

**IA-2.b** BASIC CONTROL: When access to the information system is by a privileged entity (i.e., a user or information system process acting on behalf of a user that possesses authorization to perform system administration or mission processing actions beyond that which average users are allowed to perform) that either resides outside of the system's authorization boundary or whose communications traverse information links (extranets, Internet, phone lines) that are outside of the system's authorization boundary, an identification and authentication mechanism that is resistant to replay attacks is used.

**IA-2.e** ENHANCED CONTROL (Add to basic control):
Whenever any user is remotely accessing the information system, an identification and authentication mechanism that is resistant to replay attacks is used. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-2.s** STRONG CONTROL: To be defined.

### IA-3 PASSWORD PROTECTION MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect passwords from unauthorized disclosure or modification.

CONTROL MAPPING: [NIST 800-26: 15.1.2; FISCAM: AC-3.2; ISO-17799: 8.5.1; DCID 6/3: I&A2-g; CMS: 2.9.7,10.5.1]

**IA-3.b** BASIC CONTROL: For information systems employing password-based authentication, passwords are: (i) one-way encrypted for storage; (ii) transmitted on the network in a secure manner (e.g., encrypted); (iii) not displayed when entered; and (iv) controlled by the associated user. When cryptographic functions are needed, FIPS-140-2 validated cryptography is used.

**IA-3.e** ENHANCED CONTROL (Add to basic control):
A FIPS-140-2 validated cryptographic module in an approved operational mode is used for password encryption for transmission. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-3.s** STRONG CONTROL: To be defined.

### IA-4 PASSWORD LIFE

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords are changed and not reused.

CONTROL MAPPING: [NIST 800-26: 15.1.6; FISCAM: AC-3.2; DCID 6/3: I&A2-e]

**IA-4.b** BASIC CONTROL: Mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. Passwords are changed at least [*Assignment: time period; typically sixty-ninety days*]. Passwords have a minimum life of [*Assignment: time period (e.g., one day)*]. Passwords are prohibited from reuse for a specified period of [*Assignment: number of generations; typically six*].

**IA-4.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-4.s** STRONG CONTROL: To be defined.

### IA-5 PASSWORD CONTENT

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that passwords comply with policy requirements for content and length.

CONTROL MAPPING: [NIST 800-26:15.7; FISCAM: AC-3.2; ISO-17799: 9.5.4; DCID 6/3: I&A2-c, I&A4]

**IA-5.b** BASIC CONTROL: Mechanisms are implemented to ensure that passwords: (i) contain characters from [*Selection: uppercase alphabetic, lowercase alphabetic, numeric, special characters; typically all four are selected*] with [*Assignment: requirements for how many of the selected types of characters must be included, typically three*]; (ii) have a minimum length of [*Assignment: value, minimum of eight characters*]; (iii) are not the same as the user ID; (iv) are not names or words; (v) are unique for specific individuals; and (vi) are not generic user IDs or passwords.

**IA-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-5.s** STRONG CONTROL: To be defined.

### IA-6 PASSWORD-BASED ELECTRONIC SIGNATURES

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented

to ensure appropriate use of password-based, electronic signatures. (*Related to IA-10 Digital Signatures*)

CONTROL MAPPING: [FISCAM: AC-3.2]

**IA-6.b** BASIC CONTROL: Password is entered solely for the purpose of indicating intent to sign, is known only by the password owner, and is not exposed to offline attacks by an eavesdropper. The user is advised that use of the password will be construed as a binding legal signature and applications make clear the significance of the act of signing with each signature. Passwords are registered to each user by a secure process that provides clear assurance that the password is associated with the correct individual.

**IA-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-6.s** STRONG CONTROL: To be defined.

### IA-7 TOKEN-BASED IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of token-based identification and authentication.

CONTROL MAPPING: [NIST 800-26: 15.1; DOD 8500: IATS-2]

**IA-7.b** BASIC CONTROL: Identification and authentication is accomplished using tokens that may be implemented in software. At a minimum, the authenticator is derived from a FIPS-140-2 approved pseudo random number generator.

**IA-7.e** ENHANCED CONTROL (Add to basic control):
Identification and authentication is accomplished using hardware tokens. At a minimum, the authenticator is derived from a FIPS-140-2 approved pseudo random number generator. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-7.s** STRONG CONTROL (Add to basic control; bold text represents change from enhanced control):
Identification and authentication is accomplished using symmetric or asymmetric key cryptographic hardware tokens validated at FIPS 140-2 level **4**. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

### IA-8 BIOMETRIC-BASED IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of biometrics for identification and authentication.

CONTROL MAPPING: [NIST 800-26: 15.1]

**IA-8.b** BASIC CONTROL: Identification and authentication is accomplished using biometric devices under the control of the information system. Biometric devices are configured for performance parameters such as number of false positives and number of false negatives and are consistent with information system requirements.

**IA-8.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-8.s** STRONG CONTROL: To be defined.

**IA-9 MUTIFACTOR IDENTIFICATION AND AUTHENTICATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of multiple techniques for user identification and authentication.

CONTROL MAPPING: [NIST 800-26: 15.1]

**IA-9.b** BASIC CONTROL: Identification and authentication is accomplished using multiple mechanisms such as: (i) biometric reader in conjunction with a password; (ii) biometric reader in conjunction with a token; (iii) multiple, different types of biometric readers; or (iv) multiple, different types of authentication mechanisms other than biometrics.

**IA-9.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-9.s** STRONG CONTROL: To be defined.

**IA-10 DIGITAL SIGNATURES — MECHANISMS**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable use of digital signatures. (*Related to IA-6 Password Based Electronic Signatures*)

CONTROL MAPPING: [NIST 80-26:15.1.2, 16.1.7; ISO-17799: 10.3.3; FISCAM: AC-3.2]

**IA-10.b** BASIC CONTROL: Digital signatures that conform to FIPS 186-3 are used to sign information. Digital signature private keys are not used for any other purpose (e.g., key transport or key agreement), and are not escrowed or purposefully made known to any other party. The key owner is advised that use of the key will be construed as a binding legal signature, and applications make clear the significance of the act of signing with each signature. The application requires a clear separate act to signify the signature (such as clicking on an appropriately labeled box). The system maintains a detailed log of authentications and signatures. The Certification Authority (CA) is cross certified with the Federal Bridge CA at the medium or high level of assurance, or the certificate policy is determined to provide equivalent assurance.

**IA-10.e** ENHANCED CONTROL (Add to basic control):
Digital signature private keys are in the sole control of the signer, and are kept on a hardware cryptographic module that is validated at FIPS-140-2 level 2 or higher. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-10.s** STRONG CONTROL: To be defined.

**IA-11 AUTOMATIC INFORMATION SYSTEM IDENTIFICATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable identification of the information system being used or to which a connection is being made.

CONTROL MAPPING: [NIST 800-26:16.2.1, 16.2.4; FISCAM: AC-3.2; ISO-17799: 9.5.1]

**IA-11.b** BASIC CONTROL: Automatic information system identification is used to authenticate connections to specific locations and portable information system hardware.

**IA-11.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-11.s** STRONG CONTROL: To be defined.

### IA-12 REMOTE ACCESS IDENTIFICATION AND AUTHENTICATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable higher reliability in the identification and authentication of remote access users.

CONTROL MAPPING: [NIST 800-26: 16.2.4, 16.2.8; FISCAM: AC-1, AC-3.2; DCID 6/3: I&A3; CMS: 2.9.5, 2.9.6]

**IA-12.b** BASIC CONTROL: When remotely accessing via dialup authentication is provided through ID and password encryption for use over public telephone lines. Standard access is provided through a toll-free number and through local telephone numbers to local facilities.

**IA-12.e** ENHANCED CONTROL (Add to basic control):
Both access methods (toll free and local numbers) require a special (encrypted) modem for every applicable workstation and a smart card (microprocessor) for every remote user (See IA-7 Token-based Identification and Authentication). It also includes at least one of the following implementation features: (i) biometric identification, (ii) password, (iii) personal identification number (PIN), or (iv) telephone callback procedure. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-12.s** STRONG CONTROL: To be defined.

### IA-13 UNSUCCESSFUL LOGIN ATTEMPTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to take defined action in the face of multiple unsuccessful login attempts.

CONTROL MAPPING: [NIST 800-26: 15.1.14; FISCAM: AC-3.2; DCID 6/3: SessCtrl2-c, SessCtrl2-d; CMS: 2.9.5, 2.9.6]

**IA-13.b** BASIC CONTROL: For a given user, there is a limit of [*Assignment: number, typically three*] invalid information system access attempts that may occur over [*Assignment: time period (e.g., fifteen minutes)*]. When the maximum number of unsuccessful attempts is exceeded, the information system automatically [*Selection: locks the account/node until released by an administrator, locks the account/node for an* [*Assignment: time period (e.g., fifteen minutes)*], *delays next login prompt according to* [*Assignment: delay algorithm (e.g., the standard Unix algorithm that accomplishes successively longer delays with each subsequent failure)*]].

**IA-13.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**IA-13.s** STRONG CONTROL: To be defined.

**IA-14 IDENTIFIER MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user identifiers.

CONTROL MAPPING: [NIST 800-26: 15.1.8; FISCAM: AC-3.2; ISO-17799: 9.5.3; DCID 6/3: I&A1; CMS: 2.10.4]

**IA-14.b** BASIC CONTROL: Users of the information system are appropriately identified. Identification is unique to each user. Registration to receive a user identification (ID) is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the user ID is issued to the intended party. Inactive user Ids are disabled after [*Assignment: time period, for example, one year*].

**IA-14.e** ENHANCED CONTROL (Add to basic control):
Multiple, approved forms of individual identification such as documentary evidence or a combination of documents and biometrics are presented to the registration authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IA-14.s** STRONG CONTROL: To be defined.

**IA-15 AUTHENTICATOR MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage user authenticators.

CONTROL MAPPING: [ISO-17799: 9.2.3; DCID 6/3: I&A1; CMS: 2.9.3; FISCAM: AC-3.2]

**IA-15.b** BASIC CONTROL:

*Public Key Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor, and is done in person before a designated registration authority. Secure procedures ensure that the certificate is issued to the correct, identified party.

*Authenticator Selection, Content, Defaults and Protection*

Selection of passwords or other authentication devices (e.g., tokens, biometrics) is appropriate, based on FIPS Publication 199 security category of the information system. Initial authenticator content and administrative procedures for initial authenticator distribution are defined. Lost or compromised authenticators are addressed. Default authenticators are changed upon information system installation. Authenticators are protected to preserve confidentiality and integrity. Users maintain possession of their individual tokens, key cards, etc., do not loan or share these items with others, and report lost items immediately.

**IA-15.e** ENHANCED CONTROL (Add to basic control):

*Public Key Certificate Registration*

Multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A biometric, such as a photo or fingerprint is obtained as a part of the registration procedures and retained by the Registration Authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IA-15.s** STRONG CONTROL: To be defined.

**IA-16 PASSWORD MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that passwords meet specified requirements.

CONTROL MAPPING: [NIST 800-26: 15.1.3, 15.1.5, 15.1.7, 15.1.11; FISCAM: AC-3.2; ISO-17799: 9.2.3, 9.3.1; CMS: 2.9.2, 2.9.10]

**IA-16.b** BASIC CONTROL:

*Organization-issued Passwords*

Registration to receive a password is accomplished by a designated registration authority as determined by the organization, includes authorization by a supervisor or a responsible organization official, and is done by secure procedures that verify the identity of the user and ensure that the password is issued to the intended party. Users are instructed as to the proper methods of protecting their passwords.

*Organization-issued and User-determined Passwords*

For information systems employing password-based authentication, passwords are: (i) distributed securely; (ii) controlled by the assigned user and not subject to disclosure; (iii) prohibited from being embedded in programs; (iv) changed periodically every [*Assignment: time period, typically ninety days*]; (v) contain alphanumeric and special characters and are composed of representatives of at least three of the following character sets: upper case English, lower case English, numeric characters, and special characters (information systems with limited information input capabilities implement these measures to the extent possible.); (vi) have a minimum length of [*Assignment: value, minimum of eight characters*]; (vii) prohibited from reuse for a specified period of [*Assignment: number of generations, typically six*]; (viii) have an appropriate minimum life of [*Assignment: length of time, typically one day*]; (ix) not the same as the user ID; and (x) not names or words.

**IA-16.e** ENHANCED CONTROL (Add to basic control):

Multiple, approved forms of individual identification such as documentary evidence or a combination of documents and biometrics are presented to the registration authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**IA-16.s** STRONG CONTROL: To be defined.

## TECHNICAL CONTROLS

**FAMILY:** LOGICAL ACCESS CONTROL (AC)

### AC-1 REMOTE ACCESS RESTRICTIONS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide access protections for remote connections.

CONTROL MAPPING: [NIST 800-26: 16.2.1, 16.2.4, 16.2.8, 16.2.9, 16.3.2; FISCAM: AC-1, AC-3.2; ISO-17799: 8.5.1; DCID 6/3: I&A3, Integrty2, 7G.3.b, 7.G.3.c, 7.G.3.d; CMS: 2.2.17, 3.6.3; DOD 8500: EBRP-1, EBRU-1]

**AC-1.b** BASIC CONTROL: There are controls that restrict remote access to the information system.

*Protection of Remote Access - General*

Remote access to organizational information systems always uses encryption to protect the confidentiality of the session. All remote access is mediated through a managed access control point. Information regarding remote access mechanisms (e.g., dial-up connection telephone numbers) is protected.

*Remote Access for Privileged Functions*

Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to general security measures for remote access, additional protections such as a virtual private network with blocking mode enabled are implemented.

*Collaborative Computing*

Collaborative computing mechanisms are not remotely activated. Activation requires an explicit action by the workstation user (e.g., in the case of a desktop video teleconference, the user of the desktop is required to take an explicit action to turn on the camera and microphone, remote users are not allowed to activate a user's camera or microphone remotely). Peer-to-peer collaborative computing mechanisms between information systems ensure that only the information on the screen is observable to the remote user. Information located elsewhere on the workstation is not observable. The remote user is not able to modify or delete any information on the workstation. These restrictions also apply to any other information system to which the user's workstation is logically connected (e.g., any logically mounted disks). Collaborative computing mechanisms that provide video and/or audio conference capabilities provide some explicit indication that the video and audio mechanisms are operating.

*Public Access Information Systems*

For public access information systems, there are mechanisms implemented to protect the integrity of the information, the application, and the underlying system. These controls are resilient in the face of publicly known attacks.

*Dial-In Access to Information Systems*

Dial-in access to the information system is controlled and monitored. Mechanisms are implemented to limit the access achieved through dial-up, in accordance with organizational policy.

*Remote Terminal Access*

Where enforcement of information system security policy requires, mechanisms are implemented to restrict access through specific workstations or terminals.

**AC-1.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-1.s** STRONG CONTROL: To be defined.

**AC-2 LOGON NOTIFICATION MESSAGE**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide users with information about previous logons both successful and unsuccessful.

CONTROL MAPPING: [NIST 800-26: 16.2.13, FISCAM: AC-1, AC-3.2; ISO-17799: 12.1.4; DCID 6/3: SessCtrl1; CMS: 2.8.7, 10.8.3; DOD 8500: ECLO-2, ECWM-1]

**AC-2.b** BASIC CONTROL: Upon successful logon, the user is notified of the date and time of the user's last logon, the location of the user's last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon. A warning/notification message is displayed upon successful logon and before gaining system access. This message: (i) is approved and standardized; (ii) remains on the screen until explicit user action to remove it; (iii) warns all users that they have accessed a U.S. Government information system; (iv) provides appropriate privacy and security notices; (v) notifies the user that system usage may be monitored, recorded, and subject to audit; and (vi) notifies the user that use of the information system indicates (a) the consent of the user to such monitoring and recording and (b) that unauthorized use is prohibited and subject to criminal and civil penalties.

**AC-2.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-2.s** STRONG CONTROL: To be defined.

**AC-3 CONCURRENT SESSION CONTROL**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable control of the number of concurrent sessions on the information system for a given user.

CONTROL MAPPING: [ISO-17799: | DCID 6/3: SessCtrl2-a]

**AC-3.b** BASIC CONTROL: If the information system allows for multiple logon sessions for each user ID, the system provides a capability to control the number of logon sessions. The maximum number of concurrent sessions for any user is [*Assignment: number; (e.g., three)*].

**AC-3.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-3.s** STRONG CONTROL: To be defined.

**AC-4 SESSION LOCK**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable user-commanded locking of the information system session.

CONTROL MAPPING: [ISO-17799: 9.3.2 | DCID 6/3: ScrnLck; CMS: 1.13.1; DOD 8500: PESL-1]

**AC-4.b** BASIC CONTROL: Session-lock functionality is associated with each information system node (e.g., terminal, workstation, notebook computer). Upon user activation, a session-lock function prevents access to the node or to any session information. Once the session-lock is activated, access to the node requires knowledge of a unique authenticator. Session-lock is not a substitute for logging out.

**AC-4.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-4.s** STRONG CONTROL: To be defined.

**AC-5 SESSION INACTIVITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable enforcement of defined actions in the event of session inactivity.

CONTROL MAPPING: [NIST 800-26: 16.1.4, 16.2.6; FISCAM: AC-3.2; ISO-17799: 9.5.7; DCID 6/3: ScrnLck-a, SessCtrl2-b; CMS: 2.9.11, 7.3.5]

**AC-5.b** BASIC CONTROL: The information system detects [*Assignment: time period (e.g., fifteen minutes)*] of inactivity and blocks further access until the user reestablishes the connection using the proper identification and authentication procedures.

**AC-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-5.s** STRONG CONTROL: To be defined.

**AC-6 LIMITED CONNECTION TIME**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to limit the length of time given types of connections can be maintained.

CONTROL MAPPING: [ISO-17799: 9.5.8; DCID 6/3: SessCtrl2-b]

**AC-6.b** BASIC CONTROL: Mechanisms are implemented to limit the length of time a defined set of connections can be established. The defined set is: (i) [*Assignment: connection description/length of time*]; and (ii) [*Assignment: additional connection description/length of time*].

**AC-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-6.s** STRONG CONTROL: To be defined.

**AC-7 AUTOMATED MARKING AND LABELING**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to mark output and label information in storage, in process, and in transmission.

CONTROL MAPPING: [NIST 800-26: 16.1.6; FISCAM: AC-3.2; DCID 6/3: Marking, ParamTrans; DOD 8500: ECML-1]

**AC-7.b** BASIC CONTROL: Information systems that store, process, transmit, or display information in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in Federal policy and guidance documents. Markings and labels clearly reflect any special dissemination, handling, or distribution instructions. Internal security labels are an integral part of the electronic information or media. A means is provided for the information system to ensure that the labels a user associates with information provided to the system are consistent with the information that the user is allowed to access. Internal security labels and mark-

ings implement standard naming conventions. Documentation is maintained regarding the kind(s) of information allowed on each communications channel within the information system.

**AC-7.e** ENHANCED CONTROL (Add to basic control):
Automated marking mechanisms to ensure that either the user or the information system marks all information output from the system. Markings are retained with the information. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-7.s** STRONG CONTROL: To be defined.

### AC-8 AUTHORIZATION MANAGEMENT MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective assignment and management of access authorizations.

CONTROL MAPPING: [NIST 800-26: 16.1.2; FISCAM: AC-3.2; ISO-17799: 12.1.4; DCID 6/3: Access3, Access5; CMS: 2.9.12]

**AC-8.b** BASIC CONTROL: Authorization management mechanisms are implemented that effectively support the following access control capabilities: (i) [*Selection: one or more types of access control: role-based, identity-based*]; and (ii) [*Selection: one or more types of access control: discretionary, non-discretionary*]. Whenever the information system provides for disclosure of information deemed critical/sensitive by the organization (in accordance with FIPS Publication 199), an authorization mechanism is employed to query and receive consent for the disclosure of such information. The information system provides the capability for users (or processes acting on behalf of users) to determine the access authorizations granted to another user or to a communications channel.

**AC-8.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-8.s** STRONG CONTROL: To be defined.

### AC-9 ENFORCEMENT MECHANISMS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enforce the assigned authorizations for access to information or the information system and for controlling the flow of information.

CONTROL MAPPING: [NIST 800-26: 16.1.9; FISCAM: AC-3.2; ISO-17799: 9.4.1, 9.4.7, 9.6.1, 12.1.1, 12.1.4; DCID 6/3: Access4, Access5; DOD 8500: ECRC-1]

**AC-9.b** BASIC CONTROL: Information system access enforcement mechanisms (capable of including or excluding access to the granularity of a single user or user-role) enforce the assigned resource authorizations for each attempted access to information or information system. Information flow control enforcement mechanisms provide the granularity of information description and of source and destination description to adequately implement organizational policy.

*For discretionary access control enforcement*

Access is controlled between named users (or processes) and named objects (e.g., files and programs) in the information system. The enforcement mechanisms (e.g., self/group/public controls, access control lists, communities of interest, encryption) allow users to specify and control sharing of those objects by named individuals, or by defined groups of individuals, or by both, and provide controls to limit propagation of access rights. The enforcement mechanisms, either by explicit user

action or by default, protect objects from unauthorized access. These access controls are capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission is only assigned by authorized users.

*For non-discretionary access control enforcement*

A non-discretionary access control policy is enforced over all subjects and storage objects under its control (e.g., processes, files, segments, devices). These subjects and objects are assigned labels (implicitly or explicitly) that combine hierarchical levels and non-hierarchical categories; the labels are used as the basis for non-discretionary access control decisions.

*For flow control enforcement*

A flow control policy is enforced over information flows under its control. Information and source and destination objects may be assigned labels (implicitly or explicitly) that are used as the basis for non-discretionary flow control decisions. Additionally, flow control rules (e.g.,, router rules) may be used to enforce information flow policy both discretionary and non-discretionary.

**AC-9.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-9.s** STRONG CONTROL: To be defined.

### AC-10 AUTOMATED ACCOUNT CONTROLS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to manage inactive and special accounts.

CONTROL MAPPING: [NIST 800-26: 16.1.5; FISCAM: AC-3.1, AC-3.2; CMS: 2.10.5; DOD 8500: IAAC-1]

**AC-10.b** BASIC CONTROL: Emergency or temporary accounts are automatically terminated after [*Assignment: time period (e.g., thirty days)*]. Inactive accounts are automatically disabled after [*Assignment: time period (e.g., six months)*].

**AC-10.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AC-10.s** STRONG CONTROL: To be defined.

### AC-11 LEAST PRIVILEGE AND SEPARATION OF DUTIES

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to separate duties among individuals within the organization and limit authorizations to the minimum necessary to fulfill assigned duties.

CONTROL MAPPING: [NIST 800-26: 6.1.2, 6.1.3, 6.1.4, 17.1.5; FISCAM: AC-3.1, SD-1, SD-1.1, SD-1.2; ISO-17799: 8.1.4; DCID 6/3: Audit7, LeastPrv, Separation; CMS: 4.7.1, 4.7.6; DOD 8500: ECLP-1]

**AC-11.b** BASIC CONTROL:

*Least Privilege*

Each user or process is authorized the most restrictive set of privileges or accesses needed for the performance of authorized tasks.

*Separation of Duties*

The principle of separation of duties is enforced. Mission functions and distinct information system support functions are divided among different individuals and are performed by different individuals. Access authorizations are periodically reviewed for functions that should be separated to enhance security. Duties that should be separated to enhance security have been identified (e.g.,

security personnel who administer access control functions should not be those who administer the audit functions on the information system). Information system support functions are performed by different individuals (e.g., functions such system management, system design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, network security, database administration, network administration). As necessary to enhance security, mission-processing functions are distributed among different individuals. Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.

**AC-11.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AC-11.s** STRONG CONTROL: To be defined.

### AC-12 SUPERVISION AND REVIEW — ACCESS CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to supervise personnel and review their actions with respect to enforcement of access controls.

CONTROL MAPPING: [NIST 800-26: 17.1.6, 17.1.8; ISO-17799: 12.2.1; CMS: 1.10.2; FISCAM: AC-3.1]

**AC-12.b** BASIC CONTROL: Personnel (those enforcing controls and those who the controls are restricting) are provided adequate supervision and review, including each shift for computer operations. Supervisors routinely review user activity logs for inappropriate actions and investigate any abnormalities. Changes to security access authorizations are logged and periodically reviewed by appropriate organization officials independent of the security function. Unusual activity is investigated.

**AC-12.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AC-12.s** STRONG CONTROL: To be defined.

### AC-13 NON-DISCRETIONARY ACCESS CONTROL

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enable enforcement of non-discretionary access requirements.

CONTROL MAPPING: [DCID 6/3: Access2, Access5]

**AC-13.b** BASIC CONTROL: Non-discretionary access requirements are identified and appropriate authorizations implemented to enable the enforcement of these access requirements. Examples of non-discretionary requirements are: (i) limitations on release of private information; (ii) limitations on release of export-controlled information; and (iii) limitations on public release of information.

**AC-13.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AC-13.s** STRONG CONTROL: To be defined.

**AC-14 AUTHORIZATION PROCEDURES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system authorizations.

CONTROL MAPPING: [NIST 800-26: 15.1.4, 15.2.2; FISCAM: AC-2.1, AC_2.2, AC-3.1, AC-4; ISO-17799: 5.2.1, 9.2.2, 9.2.4; CMS: 1.4.7, 2.5.3, 2.7.2, 2.8.3, 2.8.4, 2.8.5, 2.8.6, 2.8.9, 2.9.4, 2.10.1, 2.10.2, 2.10.4, 7.1.1; DOD 8500: ECAN-1, PRNK-1]

**AC-14.b** BASIC CONTROL: Rules are in place for: (i) granting of access authorizations; (ii) determining initial rights of access to a terminal, transaction, program, process, or information; and (iii) determining the types of, and reasons for, modification to established rights of access, to a terminal, transaction, program, process or information.

*Granting of Access Rights*

Information system owners identify authorized users and their respective access authorizations. Emergency and temporary access authorizations to the information system are explicitly approved by designated organization officials, monitored, and removed as soon as no longer required. Where appropriate, access is authorized based on time and/or location. Security administrators set parameters in security software to provide access as authorized and restrict access that has not been authorized. This includes access to files, load libraries, batch operational procedures, source code libraries, security files and operating system files.

*Review of Access Rights*

Information system owners periodically review access authorizations for continuing appropriateness. Security managers review access authorizations and discuss any questionable authorizations with information system owners. Access to the information system is authorized only to individuals who: (i) have a valid need-to-know that is demonstrated by assigned official duties and satisfying of all personnel security criteria; or (ii) are otherwise to be granted access based upon intended system usage (e.g., a publicly accessible web site).

*Authorization Definitions*

Authorizations are defined and managed for: (i) mission-specific processing; (ii) program source library; (iii) system resources; (iv) support/technology management systems and/or tools; (v) system libraries; (vi) access to passwords/authentication services and directories; (vii) access authorizations for maintainers of information system resources, including those that are at remote locations; (viii) users who can dial into the information system from remote locations; and (ix) default permissions and rights.

*Miscellaneous*

Standardized naming conventions are used for information system components. Those routines that modify the status of a file are controlled. This means limiting and controlling the authority to catalog, scratch, and rename a file. Employees are discouraged from browsing files by making it clear that organizational policy prohibits it. Computer operators do not display user programs or circumvent security mechanisms, unless specifically authorized.

**AC-14.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AC-14.s** STRONG CONTROL: To be defined.

**AC-15 SYSTEM ACCOUNT MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage information system accounts.

CONTROL MAPPING: [NIST 800-26: 6.1.7, 15.1.1, 15.1.4, 15.1.5, 16.2.12; FISCAM: AC-2, AC-2.2, AC-3.1, AC-3.2, SP-4.1; ISO-17799: 9.2.1; DCID 6/3: AcctMan; CMS: 2.9.9, 2.10.4; DOD 8500: ECPA-1]

**AC-15.b** BASIC CONTROL: Comprehensive account management ensures that only authorized users can gain access to information systems. Account management includes: (i) identifying types of accounts (individual and group, conditions for group membership, associated privileges); (ii) establishing an account (i.e., required identification, approval, and documentation procedures); (iii) activating an account; (iv) modifying an account (e.g., disabling an account, changing privilege level, group memberships, authenticators); and (v) terminating an account.

*All Accounts*

Personnel files are matched with user accounts to ensure that terminated or transferred individuals do not retain information system access. The account manager is notified in a timely manner when information system users are terminated or transferred. Unnecessary accounts (defaults, guest accounts) are removed, disabled, or otherwise secured. Inactive accounts and accounts for terminated individuals are disabled or removed on a timely basis.

*Guest and Anonymous Accounts*

Guest and anonymous accounts on the information system are specifically authorized and monitored. Emergency or temporary accounts are appropriately controlled, including: (i) documented, approved by appropriate organization officials; (ii) securely communicated to the appropriate personnel; and (iii) automatically terminated after a predetermined period with a default of [*Assignment: time period (e.g., thirty days)*].

**AC-15.e** ENHANCED CONTROL (Add to basic control):

*Privileged Accounts*

All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). Privileged role assignments are tracked. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**AC-15.s** STRONG CONTROL: To be defined.

## TECHNICAL CONTROLS

**FAMILY:** ACCOUNTABILITY (INCLUDING AUDIT TRAILS) (AU)

### AU-1 USER ASSOCIATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the association of an individual user with the actions taken by that user.

CONTROL MAPPING: [NIST 800-26:16.1.1, 17.1.1; FISCAM: AC-3.2; DCID 6/3: Audit2-a, Audit5-a, Audit8-a, I&A2; CMS: 2.1.1]

**AU-1.b** BASIC CONTROL: Mechanisms are implemented to associate actions taken or attempted in the information system with the specific user responsible for that action.

**AU-1.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-1.s** STRONG CONTROL: To be defined.

### AU-2 CONTENT OF AUDIT RECORDS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to include specified information in audit records.

CONTROL MAPPING: [NIST 800-26: 17.1.1; DCID 6/3: Audit1, Audit4; CMS: 2.1.5; DOD 8500: ECAR-3, ECLC-1]

**AU-2.b** BASIC CONTROL: The audit trail includes sufficient information to establish what events occurred and who or what caused the events. For each security-relevant auditable event (as specified in AU-3), the audit record contains at least the following information: (i) date and time of the event; (ii) information system locale of the event; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

*For Information Release Actions*

Include: (i) identity of releaser; (ii) identity of recipient; (iii) identity of information released; (iv) device identifier (id) (e.g., port ID); (v) time and date of release; and (vi) modification or application of security labels.

*For Information Communications Actions*

Include: (i) identity of sender (e.g., person, information system); (ii) identity of recipient (e.g., IP address, host and user); device ID (e.g., port ID); and (iii) time and date of communication.

The following additional audit information is provided: [*Assignment: list of other information that the information system is able to include in the audit records*].

**AU-2.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-2.s** STRONG CONTROL: To be defined.

### AU-3 AUDITABLE EVENTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable the ability to generate an audit record for at least a defined set of events.

CONTROL MAPPING: [NIST 800-26: 16.1.10, 17.1.3, 17.1.5, 17.1.6, FISCAM AC-4; ISO-17799: 9.7.1 | DCID 6/3: Audit1, Audit6, Audit7, 7.B.2.h; CMS: 2.1.2, 2.1.6, 4.2.1, 7.3.1, 9.5.1; DOD 8500: ECAT-2]

**AU-3.b** BASIC CONTROL: The information system audit mechanisms are capable of generating an audit record for each of the following events: (i) start-up and shutdown of the audit functions; (ii) successful and unsuccessful logons and logoffs; (iii) successful and unsuccessful attempts to access security relevant files and utilities including user authentication information; (iv) operations performed to read, modify or destroy the audit information; (v) modifications to the audit configuration that occur while the audit functions are operating; (vi) actions taken due to exceeding of a threshold or audit storage failure; (vii) unsuccessful use of the user identification or authentication mechanisms including the identity provided; (viii) unsuccessful revocations of security attributes; (ix) modifications to the group of users that are part of a role; (x) key recovery requests and associated responses including who made the request and when; (xi) changes to the time; (xii) denial of access resulting from an excessive number of logon attempts; (xiii) blocking or blacklisting a user ID, terminal, or access port and the reason for the action; (xiv) detected replay attacks; (xv) rejections of new sessions based upon any limitation on the number of concurrent sessions; (xvi) other activities that modify, bypass, or negate security controls within the information system; (xvii) use of compilers, and (xviii) use of privileged accounts.

All accesses to information system software files are logged by automated logging facilities. Installation of all system software is logged to establish an audit trail/log and is reviewed by management. The use of system utilities is logged using access control software reports or job accounting information. Activities at the system console (either physical or logical consoles), and other system-level accesses by privileged users are logged.

*Mission-specific Processing Activity*

For example: (i) all transactions are logged as entered, along with the user ID of the individual entering the information; and (ii) overriding or bypassing information validation and editing is restricted to supervisors and then only in a limited number of acceptable circumstances. Every override is automatically logged by the application so that the action can be analyzed for appropriateness and correctness.

*Non-discretionary Access Control Events*

For example: (i) attempts to cause information flows contrary to policy; (ii) changes to user formal access permissions; (iii) changes in security labels; (iv) accesses or attempted accesses to objects or information whose labels are inconsistent with user privileges; (v) information downgrades and overrides; and (vi) identified events that may be used in the exploitation of covert channels.

The following additional events generate an audit record: [*Assignment: list of additional events*].

**AU-3.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-3.s** STRONG CONTROL: To be defined.

### AU-4 AUDIT PROCESSING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable meeting specified requirements for the audit system.

CONTROL MAPPING: [NIST 800-26: 17.1.4; ISO-17799: 9.73; CMS: 2.1.2; DOD 8500: ECTP-1]

**AU-4.b** BASIC CONTROL: Information system clocks are synchronized for accurate reading of auditable events. In the event of an audit failure or full audit trail, [*Assignment: action to be taken (e.g., shutdown information system, overwrite oldest audit records, or stop generating audit records)* ]. Online audit information from the information system is protected against unauthorized access, modification or deletion. Access to information system audit tools is protected to prevent possible misuse or compromise.

**AU-4.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-4.s** STRONG CONTROL: To be defined.

### AU-5 AUDIT REDUCTION AND REPORT GENERATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable effective human review of audit information and the generation of appropriate audit reports.

CONTROL MAPPING: [NIST 800-26: 17.1.2, 17.1.7; DCID 6/3: Audit3; DOD 8500: ECRG-1]

**AU-5.b** BASIC CONTROL: Tools are available for the review of audit records and for report generation from audit records. Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents.

**AU-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-5.s** STRONG CONTROL: To be defined.

### AU-6 NON-REPUDIATION

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against later claims by sender to not have transmitted a message or a receiver to not have received a message.

CONTROL MAPPING: [NIST 800-26; 17.1.1; ISO-17799: 10.3.4; DCID 6/3: Integrty3]

**AU-6.b** BASIC CONTROL: Mechanisms are implemented that enable a later determination whether a given individual sent a specific message and whether a given individual received a specific message.

**AU-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**AU-6.s** STRONG CONTROL: To be defined.

## TECHNICAL CONTROLS

**FAMILY:** SYSTEM AND COMMUNICATIONS PROTECTION (SP)

### SP-1 APPLICATION PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to isolate user interfaces from information system management functionality.

CONTROL MAPPING: [DOD 8500:DCPA-1; DCID 6/3: 7.B.5]

**SP-1.b** BASIC CONTROL: User interface services (e.g., web services) are physically or logically separated from information storage and management services (e.g., database management systems). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

**SP-1.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-1.s** STRONG CONTROL: To be defined.

### SP-2 INFORMATION SYSTEM PARTITIONING

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to separate security-relevant functionality from other information system functionality.

CONTROL MAPPING: [NIST 800-26: 16.1.3, 16.1.9; FISCAM: AC-3.2; DCID 6/3: SysAssur3-a, SysAssur4, SysIntgr2, 7.B.5; DOD 8500: DCSP-1]

**SP-2.b** BASIC CONTROL: Information system security functions are isolated from non-security functions by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform those security functions. The system maintains a separate execution domain (e.g., address space) for each executing process.

**SP-2.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-2.s** STRONG CONTROL: To be defined.

### SP-3 INFORMATION REMNANTS

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect against unauthorized information transfer via shared information system resources.

CONTROL MAPPING: [NIST 800-26: 3.2.12; FISCAM: AC-2, AC-3.4; DCID 6/3: ResrcCtrl]

**SP-3.b** BASIC CONTROL: No information, including encrypted representations of information, produced by a prior user's actions (or the actions of a process acting on behalf of a prior user) is available to any current user (or current process) that obtains access to a shared system resource that has been released back to the information system. There is no residual information from the shared resource.

**SP-3.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-3.s** STRONG CONTROL: To be defined.

**SP-4 DENIAL OF SERVICE PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to specifically protect against denial of service attacks.

CONTROL MAPPING: [DCID 6/3: DOS]

**SP-4.b** BASIC CONTROL: Mechanisms are in place to curtail or prevent well known, detectable, and preventable denial of service attacks. The attacks to be prevented are [*Assignment: list of attacks or pointer to source for current list*].

**SP-4.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-4.s** STRONG CONTROL: To be defined.

**SP-5 RESOURCE PRIORITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to limit use of information system resources by priority and by quota.

CONTROL MAPPING: [NIST 800-26: 11.2.7; DCID 6/3: Priority]

**SP-5.b** BASIC CONTROL: Mechanisms are implemented to provide for allocation of information system resources based upon priority and upon a quota. Mechanisms are implemented to enforce the information system resource allocations as appropriate for meeting system security needs.. Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

**SP-5.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-5.s** STRONG CONTROL: To be defined.

**SP-6 BOUNDARY PROTECTION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to proxy, screen, or filter communications at the authorization boundary of the information system.

CONTROL MAPPING: [NIST 800-26: 16.2.2, 16.2.7, 16.2.8, 16.2.9, 16.2.10, 16.2.11, 16.2.14; FISCAM: AC-1, AC-3.2; ISO-17799: 8.5.1, 9.4.7; DCID 6/3: Access4, Access5, 7.B.3.a(all), 7.B.3.b(all), 7.B.5, 7.F.1; CMS: 2.2.8, 10.8.4; DOD 8500: EBBD-3]

**SP-6.b** BASIC CONTROL:

*Boundary protection devices*

Protection mechanisms are implemented at the information system boundary and at layered or internal system boundaries, including, as appropriate, firewalls, gateways, proxies, routers and network intrusion detection systems.

*Protection Capabilities*

Controlled Release: Only traffic that is explicitly permitted (based on traffic review) is released from the boundary of the interconnected information system.

Encryption: Outgoing communication (including the body and attachment of the communication) are encrypted using FIPS 140-2 validated cryptography, as needed, with the appropriate level of encryption for the information, transmission medium, and destination information system.

Fail-secure: The operational failure of the boundary protection for the information system does not result in any unauthorized release of information outside of the system boundary. In the event of an operational failure of the boundary protection, no information external to the interconnected information system enters the information system.

The boundary protection of the information system is at least as strong as the boundary protection of the information system into which the information flows are directed.

Delivery: Incoming communications have an authorized user (and, as applicable, authorized addresses) as a destination.

Filtering: Communications protocols/services from outside the boundary of the interconnected information system are supported and filtered as appropriate to comply with security policy (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications).

Proxies: Protocol-mediation software (i.e., proxies) that is able to understand and take protective action based on application-level protocols and associated data streams (e.g., filtering FTP connections to deny the use of the *put* command, effectively prohibiting the ability to write to an anonymous FTP server) are supported by the information system, as appropriate.

Extensibility: Security support for the incorporation of additional system services (as they become available) is provided, where appropriate.

Platform Protection Requirements: The platform underlying the boundary protection mechanisms must be able to isolate and protect the boundary protection applications.

Information system nodes (e.g., workstations, notebook computers) with dial-up access generate a unique identifier code before connection to the information system is completed.

Non-discretionary policy enforcement: Required capability to implement policy when policy restricts information flows between information systems connected by the boundary protection device(s) and either of the systems is not considered trustworthy enough to maintain only allowed flows.

*Alternate Processing Site*

Information system boundary protections at the designated alternate site provide the same levels of protection as that of the primary site.

**SP-6.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-6.s** STRONG CONTROL: To be defined.

**SP-7 NETWORK SEGREGATION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable segregation of functionality and communications.

CONTROL MAPPING: [NIST 800-26: 16.2.10; ISO-17799: 8.5.1, 9.4.6; CMS: 10.8.1; FISCAM: AC-1]

**SP-7.b** BASIC CONTROL: Information system boundary hosts are appropriately isolated through controls such as segregation from the internal network. External servers are located external to a site's boundary protection (e.g., firewall) or are on a network separate from the site's intranet. All Internet access is through Internet access points that are under the management and control of the information system owner or organization and meets the organizational requirement that such contacts are isolated from other organization information systems by physical or technical means. Any connection to the Internet, or other external networks or information systems, occurs through a proxy, gateway, or firewall. Public wide area network connections between the organizational information systems and the Internet or other public or commercial wide area networks require an information protection network (IPN) that acts as the single point of entry into the site and defends the information system boundary or external connection(s).

**SP-7.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-7.s** STRONG CONTROL: To be defined.

**SP-8 TRANSMISSION INTEGRITY**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to protect the integrity of information being transmitted.

CONTROL MAPPING: [NIST 800-26: 11.2.1, 11.2.4, 11.2.9; ISO-17799: 8.5.1, 10.2.3, 10.3.3; DCID 6/3: Trans2]

**SP-8.b** BASIC CONTROL: Mechanisms are implemented to enable verification of the contents of a message to determine whether the contents have been changed in transit. Engineering practices such as parity checks and cyclical redundancy checks with respect to the integrity mechanisms of commercial off-the-shelf, government off-the-shelf, and custom developed solutions are implemented for incoming and outgoing information. Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of communication sessions.

**SP-8.e** ENHANCED CONTROL (Add to basic control):
Information is transmitted with FIPS Publication 140-2 validated cryptographic integrity controls such as message authentication codes (e.g., FIPS Publication 198 HMAC) or digital signatures (FIPS Publication 186-3) that ensure the authenticity and integrity of information and prevent hijacking of communications sessions. Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-8.s** STRONG CONTROL: To be defined.

**SP-9 NETWORK DISCONNECT**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to ensure that inactive network connections are terminated.

CONTROL MAPPING: [NIST 800-26:16.2.6, 16.2.14; FISCAM: AC-1, AC-3.2; ISO-17799: 8.5.1]

**SP-9.b** BASIC CONTROL: The network connection automatically disconnects at the end of a session or after being inactive for [*Assignment: time period (e.g., thirty minutes)*]. Where connectivity is not continuous, network connection automatically disconnects at the end of a session.

**SP-9.e** ENHANCED CONTROL (Add to basic control):

Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-9.s** STRONG CONTROL: To be defined.

**SP-10 INFORMATION TRANSMISSION**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to provide for the security of transmitted information.

CONTROL MAPPING: [NIST 800-26:16.2.4; FISCAM: AC-3.2; ISO-17799: 8.5.1; DCID 6/3: Trans1, Tran-Sep, 8.C.1; CMS: 2.2.8]

**SP-10.b** BASIC CONTROL: Where information confidentiality is required, information transmission implements at least one of the following: (i) information is transmitted only within an area approved for open storage of the information; (ii) information is transmitted via a protected distribution system; or (iii) information is transmitted using FIPS Publication 140-2 validated encryption. Dial-up lines, other than those that are protected with FIPS Publication 140-2 validated cryptography or protected distribution systems, are not used for gaining access to information system resources that process organizational information without specific written authorization for the system to operate in this manner. Mechanisms are implemented to detect or prevent the hijacking of a communication session (e.g., encrypted communication channels). Information transmissions of different FIPS Publication 199 security categories (for confidentiality) are segregated from each other (e.g., using encryption, physical separation). Security parameters (e.g., labels, markings) are reliably associated (either explicitly or implicitly) with information exchanged between information systems.

**SP-10.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-10.s** STRONG CONTROL: To be defined.

**SP-11 TRUSTED PATH**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable communication with security functionality between a user and the information system.

CONTROL MAPPING: [ISO-17799: 8.5.1, 9.4.2; DCID 6/3: I&A6]

**SP-11.b** BASIC CONTROL: A trusted communications path between the user and the security functionality of the system for login and authentication is implemented and supported. Communication via this trusted path is initiated exclusively by the user and is unmistakably distinguishable from other paths. In the case of communication between two or more information systems (e.g. client server architecture), bi-directional authentication between the two systems is implemented.

**SP-11.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-11.s** STRONG CONTROL: To be defined.

**SP-12 DURESS ALARM**

CONTROL OBJECTIVE: In accordance with organizational policy, automated mechanisms are in place and detailed supporting procedures are developed, documented, and effectively implemented to enable a user to indicate to the information system that actions are being taken due to coercion.

CONTROL MAPPING: [ISO-17799: 9.5.6]

**SP-12.b** BASIC CONTROL: Mechanisms are implemented that provide the user with the means of signaling coercion, enabling an effective response.

**SP-12.e** ENHANCED CONTROL (Add to basic control):
Supporting procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the mechanisms are properly configured and the procedures are being correctly applied and consistently followed.

**SP-12.s** STRONG CONTROL: To be defined.

**SP-13 CRYPTOGRAPHIC KEY MANAGEMENT**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to manage cryptographic keys.

CONTROL MAPPING: [NIST 800-26: 16.1.7, 16.1.8; ISO-17799: 10.3.5; DOD 8500: IAKM-2]

**SP-13.b** BASIC CONTROL: When encryption is used, documented procedures are being effectively implemented for key generation, distribution, storage, use, and destruction. Symmetric and asymmetric keys used to protect organizational information are generated in FIPS Publication 140-2 validated cryptographic modules and controlled and distributed using NIST-approved key management guidance. 128, 192, or 256-bit Advanced Encryption Standard (AES) encryption is used, with key agreement or key transport corresponding to the strength of the asymmetric key algorithms (See NIST key management guidance). Asymmetric keys are produced, controlled and distributed using an organization certificate authority (CA) cross-certified with the Federal Bridge CA at a level of medium or high or pre-placed keying material.

**SP-13.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SP-13.s** STRONG CONTROL: To be defined.

**SP-14 KEY ARCHIVE**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to archive keying material for encrypted information.

CONTROL MAPPING: [NIST 800-26: 16.1.8]

**SP-14.b** BASIC CONTROL: Keying material needed to recover encrypted stored information is archived in the custody of a designated key recovery custodian and is stored securely. Keys are stored so that an intruder who steals the encrypted information does not obtain the keying material needed to decrypt the information.

**SP-14.e** ENHANCED CONTROL (Add to basic control):
Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SP-14.s** STRONG CONTROL: To be defined.

**SP-15 PUBLIC KEY INFRASTRUCTURE CERTIFICATES**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to enhance the effectiveness of public key infrastructure.

CONTROL MAPPING: [FISCAM: AC-3.2]

**SP-15.b** BASIC CONTROL: All public key certificates used in the information system are issued in accordance with a defined certificate policy and certification practice statement.

*Certificate Registration*

Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party.

**SP-15.e** ENHANCED CONTROL (Add to basic control):

Registration to receive a public key certificate is done in person. Multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics must be presented to the registration authority. A secure process ensures that the certificate is issued to the correct, identified party. A biometric, such as a photo or fingerprint is obtained as a part of the registration process and retained by the Registration Authority. Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SP-15.s** STRONG CONTROL: To be defined.

**SP-16 USE OF ENCRYPTION**

CONTROL OBJECTIVE: In accordance with organizational policy, detailed procedures are developed, documented, and effectively implemented to ensure that when encryption is used, Federal policy requirements are met, to include use of FIPS Publication 140-2 validated cryptography.

CONTROL MAPPING: [NIST 800-26: 16.1.7, 16.1.8; ISO-17799: 8.5.1, 10.3.2, 10.3.3, 10.3.4, 12.1.6; DCID 6/3: Storage-d; DOD 8500: DCNR-1, ECCR-1, ECCR-2, ECCT-2, ENK-2]

**SP-16.b** BASIC CONTROL:

*Information at Rest (Encryption for confidentiality)*

When information on the information system is encrypted for confidentiality during storage, it is encrypted with FIPS Publication 140-2 validated cryptography.

*Information in Transit (Encryption for Confidentiality)*

Organizational information that is transmitted through a commercial or wireless network and kept confidential via encryption is encrypted using 128, 192, or 256-bit Advanced Encryption Standard (AES) implemented in FIPS Publication 140-2-validated cryptographic modules.

*Information in Transit (Encryption for Need-To-Know)*

Information in transit through a network at the same FIPS Publication 199 security category (for confidentiality), but which is kept separate for need-to-know reasons via encryption, is encrypted with FIPS Publication 140-2 validated cryptography.

*Non-repudiation*

FIPS Publication 140-2 validated cryptography (e.g., DOD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS Publication 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards are applied as they become available.

**SP-16.e** ENHANCED CONTROL (Add to basic control):

Procedures include checks to be performed and assigned responsibilities for conducting these checks to periodically ensure that the procedures are being correctly applied and consistently followed.

**SP-16.s** STRONG CONTROL: To be defined.