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

Special Publication 800-64 REV. 1

Security Considerations in the Information System Development Life Cycle

Recommendations of the National Institute of Standards and Technology

Tim Grance
Joan Hash
Marc Stevens

Revision Number	Date	Description of Revision
1	June 2004	The step 'Security Control Integration' in the Implementation Phase has been changed to read 'System Integration.' Rationale –the original NIST Special Publication (SP) 800-4 was an acquisition process focused guide. In that context, the information system was seen as a series of security controls in need of integration into an organization. As SP 800-64 evolved after the public comment period, it became focused on the System Development Life Cycle. In this context, the term 'Security Control Integration' was confusing because it conflicted with the 'Security Control Development' step. This change more accurately reflects the effort to integrate the system at the operational site. Specific changes: • Executive Summary (p. v) Updated to reflect 'System Integration' • Table 2-1 (p. 7) Changed Implementation column to reflect update • Section 2.3.3.2 (p.22) Changed paragraph to reflect update • Appendix E (p. E-4) Changed table to reflect update

NIST Special Publication 800-64 REV. 1

Security Considerations in the Information System Development Life Cycle

Tim Grance, Joan Hash, and Marc Stevens

C O M P U T E R S E C U R I T Y

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

June 2004

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

Technology Administration
Phillip J. Bond, Under Secretary for Technology

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

Acknowledgements

The authors, Tim Grance and Joan Hash of the National Institute of Standards and Technology (NIST), and Marc Stevens of Booz Allen Hamilton, wish to thank their many colleagues who reviewed drafts of this document and contributed to its technical content. We also gratefully acknowledge and appreciate the many comments we received from readers of the public and private sectors, whose valuable insights improved the quality and usefulness of this document. The authors would like to specifically acknowledge some key organizations whose extensive feedback substantially contributed to the development of the document. These organizations include: MITRE, Environmental Protection Agency, Department of Treasury, Social Security Administration, General Accounting Office, Internal Revenue Service, Corbett Technologies, National Archives and Records Administration, and the Tennessee Valley Authority. The authors would also like to acknowledge some key persons for their extensive review and comments: Ron Ross for his review on the certification and accreditation, Common Criteria, and assurance sections; Bill Burr, Tim Polk, Ron Tencati, and Annabelle Lee for their reviews of the cryptography section; Ramaswamy Chandramouli for his review of the access control section; Marianne Swanson, Gary Stoneburner, Curtis Barker, and Shirley Radack for their extensive and detailed review of the document; Marshall Abrams and Joseph Veoni of MITRE for providing insight into the use of the document for very large IT acquisitions; Harold Podell of the General Accounting Office for his assistance in clarifying the enterprise IT implications during IT acquisitions; and Alexis Feringa of Booz Allen Hamilton for her keen and insightful assistance throughout the development of the document.

EXECUTIVE SUMMARY

Including security early in the information system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to an operational system. This guide presents a framework for incorporating security into all phases of the SDLC process, from initiation to disposal. This document is a guide to help agencies select and acquire cost-effective security controls by explaining how to include information system security requirements in appropriate phases of the SDLC.

A general SDLC is discussed in this guide that includes the following phases: initiation, acquisition/development, implementation, operations/maintenance, and disposition. Each of these five phases includes a minimum set of security steps needed to effectively incorporate security into a system during its development. An organization will either use the general SDLC described in this document or will have developed a tailored SDLC that meets their specific needs. In either case, NIST recommends that organizations incorporate the associated IT security steps of this general SDLC into their development process:

- **Initiation Phase –**
  - **Security Categorization** – defines three levels (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). Security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.
  - **Preliminary Risk Assessment** – results in an initial description of the basic security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.
- **Acquisition / Development Phase –**
  - **Risk Assessment** – analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.
  - **Security Functional Requirements Analysis** – analysis of requirements that may include the following components: (1) system security environment, (i.e., enterprise information security policy and enterprise security architecture) and (2) security functional requirements
  - **Security Assurance Requirements Analysis** – analysis of requirements that address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and functional security requirements, will be used as the basis for determining how much and what kinds of assurance are required.
  - **Cost Considerations and Reporting** – determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training
  - **Security Planning** – 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 agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment,

security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones).

- **Security Control Development** – ensures that 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 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.

- **Developmental Security Test and Evaluation –** ensures that security controls developed for a new information system 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 operational controls.

- **Other Planning Components –** ensures that all necessary components of the development process are considered when incorporating security into the life cycle. These components include selection of the appropriate contract type, participation by all necessary functional groups within an organization, participation by the certifier and accreditor, and development and execution of necessary contracting plans and processes.

- **Implementation Phase –**

  - **Inspection and Acceptance** – ensures that the organization validates and verifies that the functionality described in the specification is included in the deliverables.

  - **System Integration** – ensures that the system is integrated at the operational site where the information system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.

  - **Security Certification** – ensures that the controls are effectively implemented through established verification techniques and procedures and gives organization officials confidence that the appropriate safeguards and countermeasures are in place to protect the organization's information system. Security certification also uncovers and describes the known vulnerabilities in the information system.

  - **Security Accreditation** – provides the necessary security authorization of an information system to process, store, or transmit information that is required. This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.

- **Operations / Maintenance Phase –**

  - **Configuration Management and Control** – ensures adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control 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.

  - **Continuous Monitoring** – ensures that controls continue to be effective in their application through periodic testing and evaluation. 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 agency officials is an essential activity of a comprehensive information security program.

- **Disposition Phase** –
  - **Information Preservation** – ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.
  - **Media Sanitization**– ensures that data is deleted, erased, and written over as necessary.
  - **Hardware and Software Disposal** – ensures that hardware and software is disposed of as directed by the information system security officer.

After discussing these phases and the information security steps in detail, the guide provides specifications, tasks, and clauses that can be used in an RFP to acquire information security features, procedures, and assurances.

Table of Contents

1. INTRODUCTION 1

1.1 Authority 1
1.2 Purpose 1
1.3 Scope 1
1.4 Audience 2

2. INCORPORATING SECURITY INTO THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE 3

2.1 Key Roles and Responsibilities for Development Initiatives 3
2.1.1 Key Roles 3
2.1.2 Other Participants 4
2.2 Expressing Security Properties 5
2.3 IT Security in the SDLC 6
2.3.1 Initiation 8
2.3.2 Acquisition / Development 10
2.3.3 Implementation 22
2.3.4 Operations and Maintenance 23
2.3.5 Disposition 24

Appendix A— Federal Government Request for Proposals A-1

Appendix B— Specifications, Clauses, and Tasks B-1

Appendix C— Glossary C-1

Appendix D— References D-1

Appendix E— Frequently Asked Questions E-1

1. INTRODUCTION

1.1 Authority

The National Institute of Standards and Technology (NIST) have 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 though attribution is desired 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.

1.2 Purpose

The need to provide protection for federal information systems has been present since computers were first used. Congress has passed several laws relevant to information system security, including the FISMA and the Information Technology Reform Act, also known as the Clinger-Cohen Act of 1996. The OMB develops executive agency policy on information system security in accordance with existing law and Executive order(s). Federal information system security policy is contained in OMB Circular A-130, Appendix III. OMB Circular A-130 and the Federal Acquisition Regulation (FAR) require security specifications for information system acquisitions. To meet these policies and legal requirements, federal organizations must consider information system security in all phases of information system management, including the acquisition phase.

Including information system security early in the acquisition process for an information system will usually result in less expensive and more effective security than adding security to an operational system. This guide presents a framework for incorporating security into all phases of the information system development life cycle (SDLC) process, from initiation to disposal.

1.3 Scope

This document is a guideline to help agencies select and acquire cost-effective security controls by explaining how to include information system security requirements in the SDLC. This document is **not** a substitute for organization acquisition or security regulations, policy, and guidance. It should be used in conjunction with these and other NIST documents. For more information regarding the fundamentals of information system security, refer to NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook.*

This document has two parts. The first part, Section 2, explains the integration of information security into the SDLC. Appendixes A and B contain resource material that can be used during the system acquisition process. Appendix A provides the standard format for a Request for Proposals and Appendix B contains specifications and contract language for specific information security measures that can be included in information system acquisitions.

NIST has prepared the following separate document to address information system security service issues: NIST SP 800-35, *Guide to Information Technology Security Services*. Performance based contracting has emerged, in many cases, as a preferred method of acquiring services. The following web site provides a comprehensive overview of the performance based contracting process:

http://oamweb.osec.doc.gov/pbsc/index.html

The number and types of appropriate security controls may vary throughout a particular SDLC and acquisition cycle. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission. One way to identify the ideal mix of management, operational, and technical security controls is with the risk management process. NIST has prepared the following document to address these issues: NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

This document uses the following words interchangeably: offeror, developer, manufacturer, and contractor. Each of these words refers to a commercial entity that participates at various times throughout a system development. The applicability of each word depends on the phase of the SDLC and the type of system being developed.

1.4 Audience

This document is intended for the use of acquisition initiators (e.g., user, program manager, or contracting officer's technical representative [COTR]), contracting officers, and information system security officials.

2. INCORPORATING SECURITY INTO THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE

To be most effective, information security must be integrated into the SDLC from its inception. This guide focuses on the information security components of the SDLC. First, a description of the key security roles and responsibilities that are needed in most information system developments is provided. Second, sufficient information about the SDLC is provided to allow a person who is unfamiliar with the SDLC process to understand the relationship between information security and the SDLC.

However, this guide does not provide an exhaustive description of the development and acquisition processes. (See the FAR and organization-specific policies and procedures for detailed information system acquisition information).

Many methods exist that can be used by an organization to effectively develop an information system. A traditional SDLC is called a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. Another SDLC method uses the prototyping model, which is often used to develop an understanding of system requirements without actually developing a final operational system. More complex systems require more iterative development models. More complex models have been developed and successfully used to address the evolving complexity of advanced and sometimes-large information system designs. Examples of these more complex models are the: spiral model, component assembly model, and concurrent development model.

The expected size and complexity of the system, development schedule, and length of a system's life will affect the choice of which SDLC model to use. In most cases, the choice of SDLC will be defined by an organization's acquisition policy.

This guide incorporates security into the SDLC using the linear sequential model as an example. Because this model is the simplest of the various models, it is an appropriate platform for this discussion. However, the concepts discussed in this section are applicable to any SDLC model.

2.1 Key Roles and Responsibilities for Development Initiatives

Many participants can have a role in information system developments depending on the nature and scope of the system. The names for the roles and titles will vary among organizations. Not every participant works on every activity within a phase. The determination of which participants need to be consulted in each phase is as unique to the organization as the development. With any development, it is important to involve the information security program manager and information system security officer (ISSO) as early as possible, preferably in the initiation phase.

2.1.1 Key Roles

A list of key roles is provided below. This list includes roles that are important to many information system acquisitions. In some small organizations, a single individual may hold multiple roles.

- **Chief Information Officer (CIO)** – The CIO is responsible for the organization's information system planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in acquiring the most efficient and effective information system to fit the organization's enterprise architecture.

- **Contracting Officer**[1] – The Contracting Officer is the person who has the authority to enter into, administer, and/or terminate contracts and make related determinations and findings
- **Contracting Officer's Technical Representative** – The COTR is a qualified employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a particular contract.
- **Information Technology Investment Board (or equivalent)** – The Information Technology (IT) Investment Board, or its equivalent, is responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (Section 5)
- **Information Security Program Manager** – The Information Security Program Manager is responsible for developing enterprise standards for information security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks to the organization. Information security program managers coordinate and perform system risk analyses, analyze risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions that help ensure mission accomplishment in the face of real-world threats. They also support senior management in ensuring that security management activities are conducted as required to meet the organization's needs.
- **Information System Security Officer** – The Information System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.
- **Program Manager (owner of data)/Acquisition Initiator/Program Official** – This person represents programmatic interests during the acquisition process. The program manager, who has been involved in strategic planning initiatives of the acquisition, plays an essential role in security and is, ideally, intimately aware of functional system requirements
- **Privacy Officer**[2] – responsible for ensuring that the services or system being procured meet existing privacy policies regarding protection, dissemination (information sharing and exchange) and information disclosure.
- **Legal Advisor/Contract Attorney** – responsible for advising the team on legal issues during the acquisition process.

2.1.2 Other Participants

The list of roles in an information system development can grow with the complexity involved in acquiring and managing information systems. It is vital that all development team members work together to ensure that a successful development is achieved. Because the system certifier and accreditor must make critical decisions throughout the development process, they should be included as early as possible in the process. System users may assist in the development by helping the program manager to determine the need, refine the requirements, and inspect and accept the delivered system. Participants may also include personnel who represent IT, configuration management, design and engineering, and facilities groups.

[1] Federal Acquisition Regulation Section 2.101

[2] In some organizations, there may not be a formal designation of a privacy officer. However, the responsibilities of the privacy officer may be incorporated as part of another role in the organization.

2.2 Expressing Security Properties

Articulation of the desired system security properties is necessary to integrating security into the SDLC depends on. When an organization determines a system's security properties, the security properties are referred to as "security requirements."

As explained below, the first phase in the SDLC is Initiation. During this phase, an organization determines its information security requirements. Often, the requirements are developed by successive refinement. The articulation of requirements starts at a high level of abstraction, often centered on the security objectives for the system. The high-level security requirements for the organization may include an information security policy and enterprise security architecture.

High-level requirements are the basis for more detailed functional requirements. Additional specificity is then added to the high-level security requirements.

> An enterprise security architecture is composed of a top-down set of identified trust modules that define network infrastructure domains and their countermeasures or mitigation. The prioritized risks for each of these levels enable the selection of the appropriate level of mitigation per module.
>
> Further, enterprise security architecture may implement layered protections and define common security services that can be implemented across a network, e.g., integrity (including nonrepudiation and authenticity), confidentiality, and availability requirements. Common security services also include access control and monitoring by intrusion detection systems and security information systems.

There are many ways to express high-level security requirements. One way to express these requirements is to use the concepts described in the Common Criteria for Information Technology Common Criteria Security Evaluation, International Organization for Standardization (ISO) 15408, known as the CC. The CC can provide a standard vocabulary and format for expressing the security requirements of a system. The specific document described in the CC to express security requirements for a product is the Protection Profile (PP)[3]. Although the intent of the CC is to use the PP to express product security requirements, the same concepts can be extended to express system security requirements. This extension of the CC has shown promise for large system developments. The concepts of the CC are extended[4] in this document to provide an example of how system security requirements can be developed, but the CC is just one of many methods that can be used to develop and express security requirements and specifications. An organization should use a process for expressing security requirements that is useful for that organization.

When an organization's requirements are developed during the Acquisition/Development phase, the organization's requirements regarding system performance are expressed as "specifications." Because the CC does not observe the subtle difference between specification and requirement, some modification is necessary.

Some large system developments use more sophisticated acquisition strategies on the assumption that large system acquisitions using classic linear strategies (as discussed in this document) have experienced

[3] The Common Criteria describes a protection profile as defining an implementation-independent set of security requirements and objectives for a category of products or systems, which meet similar consumers, needs for information security. A protection profile is intended to be reusable and to define requirements, which are known to be useful and effective in meeting the identified objectives.

[4] Certain aspects of the CC may not be extensible to the system environment. For instance, independent evaluations of a PP are not typically part of the acquisition process.

unsatisfactory results. Strategies such as the spiral model[5] are sometimes used in response to this challenge. Depending on the organization's needs, the security aspects of acquisition and system development could also follow similar models, strategies, and processes.

Because a SDLC can extend 20 years or more, different project personnel and supporting service providers will fulfill each role over the cycle. The security characteristics of the system will evolve over this system lifecycle, along with most other system characteristics. The system requirements documentation should be placed under configuration management as part of the total set of system documentation that evolves over the lifecycle.

2.3 IT Security in the SDLC

This section describes a number of steps that will help integrate IT security into the SDLC. This section explains each IT security step in each phase of the SDLC with the technical and security requirements being advanced together.

Table 2-1 shows how security fits into the SDLC. The security steps in this section describe analyses and processes to be accomplished. These steps define a conceptual framework for security planning during the SDLC. This framework should be used only as an example, not as a definitive methodology. The framework contains descriptions of a core set of planning considerations that will lead to the production of information security acquisition specifications. Organizations can use other methodologies or modify the one presented here. It is also important to note that certain critical security activities may be specifically performed by the organization acquiring the information system. For instance, certification and accreditation (C&A) is an activity performed by the organization integrating the information system into its operational environment. This activity can occur outside the bounds of the SDLC. In addition, an initial information security plan could be developed outside of the acquisition process. Other non-security activities include acceptance testing and installation.

The five basic phases of the SDLC as defined by NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems* are:

- Initiation
- Development/acquisition
- Implementation
- Operation/maintenance
- Disposition[6].

[5] Abrams, Marshall D., "Security Engineering in an Evolutionary Acquisition Environment," ACM, *Proceedings of New Security Paradigms Workshop*, 1998.

[6] In evolutionary acquisition strategies like the spiral model, this phase may not be present. With the spiral model, the life cycle acquisition management process is organized into a series of phases and decision points. The circular representation of this process conveys the idea that a mission need is defined and translated into an advantageous solution, which goes through a continuous loop of evolution and improvement until it is retired. New products should have open architecture, modular design, standard interfaces, and portable software so they can evolve over time as additional capability is needed and when obsolete components must be replaced.

Table 2-1. IT Security in the SDLC

	Initiation	Acquisition / Development	Implementation	Operations / Maintenance	Disposition
SDLC	- Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternatives to Capital Assets • Preparing for investment review and budgeting	- Functional Statement of Need - Market Research - Feasibility Study - Requirements Analysis - Alternatives Analysis - Cost-Benefit Analysis - Software Conversion Study - Cost Analysis - Risk Management[7] Plan - Acquisition Planning	- Installation - Inspection - Acceptance testing - Initial user training - Documentation	- Performance measurement - Contract modifications - Operations - Maintenance	- Appropriateness of disposal - Exchange and sale - Internal organization screening - Transfer and donation - Contract closeout
SECURITY CONSIDERATIONS	- Security Categorization - Preliminary Risk Assessment	- Risk Assessment - Security Functional Requirements Analysis - Security Assurance Requirements Analysis - Cost Considerations and Reporting - Security Planning - Security Control Development - Developmental Security Test and Evaluation - Other Planning Components	- Inspection and Acceptance - System Integration - Security Certification - Security Accreditation	- Configuration Management and Control - Continuous Monitoring	- Information Preservation - Media Sanitization - Hardware and Software Disposal

[7] Risk management in this context refers to risk associated with the development and not computer security or system technical risk.

Table 2-2 is intended to assist system developers to better understand the relationship between the acquisition cycle[8] and the five basic steps of the SDLC. A more detailed description of security planning of IT systems is presented in NIST SP 800-18.

Table 2-2. Relationship of Acquisition and IT System Development Phases

Acquisition Cycle Phases					
Mission and Business Planning	Acquisition Planning	Acquisition	Contract Performance		Disposal and Contract Closeout
Initiation	Acquisition / Development		Implementation	Operation/ Maintenance	Disposition
SDLC Phases					

The steps described in this guide present a conceptual framework for information security planning and should be used as a guide, an example, or a roadmap. Other ways to organize the steps needed in the information security planning process may be acceptable. Security requirements should be selected to address the security objectives defined as a result of the preliminary risk assessment. Therefore, a complete mapping of security requirements can be made to counter the numerous threats to security.

2.3.1 Initiation

The first phase in the SDLC is Initiation. This section addresses the needs determination component of this phase.

2.3.1.1 Needs Determination

Needs determination is an initial definition of a problem that might be solved through automation. Traditional components of the needs determination are establishing a basic system idea, preliminary requirements definition, feasibility assessment, technology assessment, and some form of approval to further investigate the problem.

The acquisition / development phase can begin only after an organization has determined that a need exists. A need may have been determined during strategic or tactical planning. The needs determination phase is at a very high level in terms of functionality. No specifics of a system are defined here. The idea for a new or substantially upgraded system and the feasibility of the idea are explored. During this early phase of the development, the definition of the security requirement should begin with the security categorization and preliminary risk assessment.

Needs determination is an analytical activity that evaluates the capacity of an organization's assets to satisfy existing and emerging demands. The security part of needs determination will result in a high-level description of the security controls in the proposed system and the assurance requirements. This material will be used to support the derivation of a cost estimate that addresses the entire life cycle. Total life-cycle costs, including implementation costs and in-service management costs, should be estimated. There may be a balance such that increased expenditures during acquisition may result in savings during system operation. The security implications of alternative architectures and technologies should be considered.

[8] GSA publication, A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1, December 1998.

Some of the considerations associated with needs determination may be security and acquisition sensitive and must be safeguarded appropriately. For example, threat analysis and efficacy of countermeasures should be safeguarded. In addition, certain enterprise security architecture and process specifics for multinode architectures should be safeguarded.

Investment analysis generates the information needed for determining the best overall solution for satisfying a mission need. Investment analysis is defined as the process of managing the enterprise information system portfolio and determining an appropriate investment strategy. For example, an appropriate investment strategy may be to optimize mission need within budget constraints. The intent of investment analysis is to not only define in functional and performance terms that the capability the agency must have to satisfy mission need, but also determine and baseline the best overall solution(s) and associated costs for achieving that capability.

Investment analysis is structured to translate mission need into high-level performance, assurance, and supportability requirements; conduct a thorough market analysis, alternatives analysis, and affordability assessment to determine the best solution for obtaining needed capability; and quantify the cost, schedule, performance, and benefit baselines for that solution. An investment analysis will help to define, in functional and performance terms, the capability that the agency must have to satisfy mission need, to determine and baseline the best overall solution(s) for achieving that capability, and to provide corresponding cost information. Information security needs should address the appropriate level of assurance, because this is a significant cost driver.

The system PP format can be used for presenting the results of the needs determination and requirements analysis. As the system PP concept becomes more recognized throughout the security community, improved communication among stakeholders can occur because a more standardized approach is in use. In particular, communication of security specifications to potential offerors can be greatly enhanced.

Further, a system PP acts as a record of the security analysis performed during this specification generation process. It provides a place to record the threats that are being considered, the security objectives that are being pursued, and the actual security specifications as they are created. Therefore, a system PP should be viewed as an evolving document that is not simply the "result" of the initial security analysis, but is the full record of the security analysis performed during the course of the specification generation process. Its creation is part of the initial analysis and its completion is realized when the full scope of the system is understood and specific security specifications are acknowledged. The completed security specification should be included by reference in the system Request for Proposal (RFP) or applicable acquisition document and later used in the risk management activity performed as part of the security C&A.

2.3.1.2 Security Categorization

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, provides a standardized approach for establishing security categories for an organization's information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the 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 (i.e., low, moderate, or high) of potential impact on organizations or individuals should there be a breach of security (a loss of confidentiality, integrity, or availability). The security categorization standards assist organizations in making the appropriate selection of security controls for their information systems.

2.3.1.3 Preliminary Risk Assessment

The preliminary risk assessment should result in a brief initial description of the basic security needs of the system. In practice, the need for information security protection is expressed in terms of the need for integrity, availability, and confidentiality and other security needs that may be applicable (e.g., accountability, nonrepudiation). Integrity can be examined from several perspectives. From a user's or application owner's perspective, integrity is the quality of data that is based on attributes such as accuracy and completeness. From a system's or operation's perspective, integrity is the quality of data that it is only changed in an authorized manner or that the system/software/process does what it is supposed to do and nothing more. Like integrity, availability also has a multipart definition. Availability is the state when data or a system is in the place needed by the user, at the time the user needs it, and in the form needed by the user. Confidentiality is the privacy, secrecy, or nondisclosure of information except to authorized individuals.

A preliminary risk assessment should define the threat environment in which the product or system will operate. This assessment is followed by an initial identification of required security controls that must be met to protect the product/system in the intended operational environment. The risk-based approach to information security is defined in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. A source for the derivation of required security controls is the forthcoming NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. This step does not require an elaborate assessment scheme.

2.3.2 Acquisition / Development

The second phase in the SDLC is Acquisition / Development. This section addresses one specific SDLC component (requirements analysis) and security considerations unique to this second phase.

Although this section presents the information security components of the requirements analysis in a sequential top-down manner, the order of completion is not necessarily fixed. Any starting point that is appropriate for the acquisition can lead to successful completion. Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

2.3.2.1 Requirements Analysis

Agencies establish and document requirements for information system resources in the Acquisition / Development phase by conducting a requirements analysis commensurate with the size and complexity of the need. The requirements analysis is an in-depth study of the need. The requirements analysis draws on and further develops the work performed during the Initiation phase.

2.3.2.2 Risk Assessment

The first step in analyzing the security functional requirements is to identify the protection requirements for the system through a formal risk assessment process. The analysis will build on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific.

The periodic assessment of risk to agency assets or operations resulting from the operation of an information system is an important activity required by FISMA. The risk assessment brings together important information for agency officials with regard to the protection of the information system and generates essential information required for the security plan. The risk assessment includes: (i) the identification of threats to and vulnerabilities in the information system; (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or

operations (including mission, functions, image, or reputation) should there be a threat exploitation of identified vulnerabilities; and (iii) the identification and analysis of security controls for the information system. Agencies should consult NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, or other similar publications for guidance on conducting risk assessments.

In addition to considering the security perspective of the system being acquired, organizations should also consider that the system might affect other systems to which it will be directly or indirectly connected. One way to incorporate the context is to have an enterprise security architecture. Without an enterprise perspective, the acquisition could be suboptimal, even to the extent of introducing vulnerabilities. If the enterprise context is not considered, there is a possibility that the system being acquired could compromise the other enterprise systems. The system being acquired may have a trust relationship with other enterprise systems, increasing the consequences of a compromise.

Each enterprise system should address several enterprise-wide security objectives:

- A specific enterprise system should not create vulnerabilities or unintended interdependencies in other enterprise systems.
- A specific enterprise system should not decrease the availability of other enterprise systems.
- The security posture of the set of all the enterprise systems should not be decreased because of this specific enterprise system.
- External domains not under enterprise control should be considered potentially hostile entities. The systems connected to such external domains must analyze and attempt to counter hostile actions originating from these domains.
- Security specifications should be appropriate for the given state of the system environment.
- Security specifications should be stated clearly to convey the desired functions and assurances to the enterprise system product team and the developers.
- Implemented specifications should sufficiently reduce the risks to the enterprise system and to the enterprise mission that the system supports.

The security risk assessment should be conducted before the approval of design specifications. In addition, a security risk assessment can provide justification for specifications. This risk assessment will not necessarily be a large and complex document. This security risk assessment should take into consideration existing controls and their effectiveness. This security risk assessment will require participation by people who are knowledgeable in the disciplines within the system domain (e.g., users, technology experts, operations experts, etc.).

The selection of appropriate types of safeguards or countermeasures should take into consideration the results of the security assurance requirements analysis. The security risk assessment, in turn, may identify deficiencies in the analysis of integrity, confidentiality, and availability requirements or the security assurance requirements analysis by demonstrating the logical conclusion of the analyses. The analysis should be iterated until consistency is achieved.

2.3.2.3 Security Functional Requirements Analysis

The security functional requirements analysis may include the two sources of system security requirements: (1) system security environment, (i.e., enterprise information security policy and enterprise security architecture) and (2) security functional requirements.

This process should include an analysis of laws and regulations, such as the Privacy Act, FISMA, OMB circulars, agency enabling acts, NIST Special Publications and FIPS, and other legislation and federal regulations, which define baseline security requirements. After a review of mandated requirements, agencies should consider functional and other security requirements.

The legal, functional, and other IT security requirements should be stated in specific terms. For complex systems, more than one iteration of the requirements analysis may be needed.

Because most systems have at least minimal integrity and availability requirements, care should be taken to clearly address these areas. Information security is more than confidentiality. Even systems with low confidentiality requirements need security to meet integrity and availability requirements.

2.3.2.4 Security Assurance Requirements Analysis

The correct and effective use of information security controls is a fundamental building block of information security. Assurance is the grounds for confidence that an entity will meet its security objectives. Assurance supports the confidence that the security controls being acquired will operate correctly and will be effective in the operational environment.

This analysis should address the developmental activities required and assurance evidence needed to produce the desired level of confidence that the information security will work correctly and effectively. The analysis, based on legal and security functional requirements, will be used as the basis for determining how much and what kinds of assurance are required. As with other aspects of security, the goal should be cost-effective assurance that meets the requirements for protection of an organization's information assets. In each situation, a balance should exist between the benefits to mission performance from system security and the risks associated with operation of the system.

Some methods of obtaining information about a system's quality through testing and evaluation include the following:

- **Common Criteria.** The CC uses security requirements, such as the evaluation assurance levels [EAL] to provide assurance based on an evaluation (active investigation) of the product or information system that is to be trusted. The assurance requirements can be found in Part 3 of the CC. The components prescribe specific developer action elements, content and presentation elements, and evaluator action elements.

  The National Information Assurance Partnership (NIAP) CC Evaluation and Validation Scheme (CCEVS) assesses the security features and assurances of commercial off-the-shelf (COTS) products. The NIAP CCEVS uses a network of private sector, accredited testing laboratories called CC Testing Laboratories (CCTL) to independently evaluate a range of commercial products against the CC in a variety of key technology areas. These include operating systems, database systems, firewalls, smart cards, biometrics devices, routers, gateways, browsers, middleware, virtual private networks (VPN), and public key infrastructure (PKI) components. These products are evaluated against a set of security requirements and specifications from the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, Common Criteria for IT Security Evaluation.

Member nations of the CC Recognition Arrangement (CCRA) have agreed to recognize the results of the evaluations performed in all member nations and to identify government-evaluated IT products and PPs on their respective validated products lists (VPL). The NIAP VPL can be accessed at:

- http://niap.nist.gov
- http://commoncriteria.org

- **Validation testing for Cryptographic Modules and Algorithms.** The NIST Cryptographic Module Validation Program (CMVP) uses independent, accredited, private-sector laboratories that perform conformance testing of cryptographic modules against Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and related federal cryptographic algorithm standards. NIST accredits these labs to ensure that the security standards are being applied correctly and consistently. In the case of cryptographic modules, when agencies have determined the need to protect information via cryptographic means they may only select CMVP validated cryptographic modules.

- **Third-Party Evaluations.** Government agencies evaluate products for use in their environments. These evaluations may or may not be published and are normally not considered to be endorsements by the agencies. Trade and professional organizations are possible sources of independent evaluations. Commercial organizations may offer product assurance testing and evaluations. When using third-party evaluations, the independence and objectivity of the evaluation should be considered. Offerors should be asked to provide information about evaluations that they consider pertinent to their proposal.

- **Accreditation of a System to Operate in a Similar Situation.** These accreditations are not usually published. It is important to ask offerors to supply the accreditation results. These, even more so than evaluations, are not usually endorsements. Accreditations are environment and system specific. Because accreditation balances risk against benefits, the same product may be accredited for one environment but not for another.

- **Test and Evaluation Following a Formal Procedure.** A vendor self-certification does not rely on the work of an impartial or independent reviewer. It is a vendor's technical evaluation of a system to see how well it meets an internally stated security requirement. Even though this method does not provide an impartial review, it can still provide some assurance. The certification report can be read to determine if the security requirement was defined and if a meaningful review was performed.

- **Test and Evaluation Under the Auspices and Review of an Independent Organization.** This method may be able to combine the lower cost and greater speed of a self-certification with the impartiality of an independent review. The review, however, may not be as thorough as a formal evaluation or testing process.

The concept of assurance is further described in NIST SP 800-23, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products.

2.3.2.5 Cost Considerations and Reporting

Most new acquisitions are evaluated in a department or agency's capital planning process—the systematic approach to managing the risks and returns of IT investments for a given mission. A key component of this process is determining how much the acquisition will cost over its life cycle. These costs include hardware, software, personnel, and training. Another critical area often overlooked is security.

The task of identifying costs attributable to security can be complex. The best input for this task comes from the risk management process. As previously described, the first step, risk assessment, results in recommended controls that will mitigate the identified vulnerabilities. In the second step, risk mitigation, organizations conduct a cost-benefit analysis on the recommended controls to determine whether they are cost effective given the likelihood of an incident and the potential impact. Once the controls are selected, the cost of each can be totaled for an overall security cost.[9]

To ensure that adequate attention is paid to security, OMB has included it as a specific line item in several separate budget reports. The first report is Exhibit 300, the Capital Asset Plan. This report is described in OMB Circular A-11, Part 3, "Planning, Budgeting, and Acquisition of Capital Assets," and is required for each new and ongoing major acquisition included in the agency's capital asset portfolio. Information security is a key component in this document; indeed, an entire section is devoted to demonstrating that security and privacy have been adequately considered. Specific security dollar amounts for the budgeted fiscal year must be included with the Exhibit 300 submissions. Criteria for determining whether a project requires an Exhibit 300 submission are provided in the circular.

Funding information is provided in the related Exhibit 53, "Agency Information Technology Investment Portfolio." Information regarding security costs must be provided in this exhibit in the form of a percentage of the overall funding.

Finally, the costs for security are aggregated into the agency's annual FISMA report, which is submitted each fall with the budget submission.

Including security at the beginning of the SDLC is often considered the most cost effective approach for two reasons: (1) it is usually more difficult to add functionality into a system after it has been built; and (2) it is frequently less expensive to include the preventive measures to deal with the cost of a security incident. Further information about this topic can be found in OMB Memorandum 00-07, "Incorporating and Funding Security in Information Systems Investments."[10][11]

2.3.2.6 Security Planning

FISMA requires agencies to have plans for information security programs to assure 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 required security controls (planned or in place) are fully documented. The security plan also provides a complete characterization or description of the information system. Attachments may include references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones[12]). Agencies should consult NIST Special Publication 800-18, *Guide for Developing Security Plans Information Technology Systems*, or other similar publications for guidance on creating security plans. Agencies should also consult NIST Special Publication 800-53, *Recommended*

[9] The cost of some security functionality will not be able to be determined as a discrete cost. These costs are the costs associated with built-in security elements or features of an application or service, such as password functionality. In addition, many applications or systems will rely upon the security provided by the network.

[10] http://www.whitehouse.gov/omb/memoranda/m00-07.html

[11] Additional information can be found at: http://csrc.nist.gov/roi/

[12] 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 milestone schedule are 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 milestone schedule prior to authorizing operation of the information system.

Security Controls for Federal Information Systems, (Initial public draft projected for publication, Fall 2003), and similar publications for guidance on selecting security controls.

2.3.2.7 Security Control Development

For new information systems, the security controls described in the respective security plans are designed, developed, and implemented. The security plans for information systems currently in operation may call for the development 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.

2.3.2.8 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 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.

2.3.2.9 Other Planning Components

Several other parts of the Acquisition / Development phase contribute to IT security.

- Type of Contract

  The type of contract (for example, firm fixed price, time and materials, cost plus fixed fee, etc.) can have significant security implications. The IT security technical experts developing the specifications and the contracting officer should work together to select the contract type that will be most advantageous to the organization.

- Review by Other Functional Groups

  Depending on the size and scope of the system, a team or group of participants from various functional groups (for example, legal, human resources, information security, physical security, etc.) may be useful. Even for small systems, it may be helpful to obtain assistance from the information security staff. These functional groups should have insight into the integrity, availability, confidentiality and assurance requirements. Involving these groups early in the planning process is important because it may result in reduced life-cycle costs, and it is easier to change requirements in the early stages. The information security staff can –

  - Demonstrate that the security plan for the system includes security controls that are consistent with the agency's IT architecture

  - Ensure that the security plan manages risks, protects privacy and confidentiality, and explains variance from NIST security guidance.

- Review by Certifier and Accreditor

  OMB Circular A-130, Appendix III, requires that systems be approved, or authorized, to process data in specific environments. Management and operational security controls should be employed to protect the system. Additionally, the technical security functional and assurance security

specifications must be contained in the contract with the developer. These security controls should be factored into the development of the technical specifications. The accreditor can take these assumptions[13] into account when deciding on the adequacy of the total set of security controls for reducing the residual risks to an acceptable level.

The management and operational security controls can sometimes be outside the scope of the contract. In particular, the developer obviously cannot be responsible for the organization's implementation of these security controls.

In contrast, C&A testing also includes management and operational security controls implemented by the organization. Determination of the efficacy of these organization-implemented security controls is part of C&A testing. C&A processes should confirm that the assumptions in the system security requirements have been implemented as assumed and that the total set of security controls are adequate to reduce the residual risks to an acceptable level. Acceptance testing of the security properties of the contractor-developed system is a prerequisite to security testing as part of the C&A process.

Because the accreditor is responsible for accepting the risk of operating the system, the accreditor can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the accreditor is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages.

The development team and the accreditor should also discuss the forms of evidence that the accreditor needs to make a decision. This evidence may include system test results and other data. In addition, the acquisition initiator and the accreditor should discuss how changes to the system and its environment would be addressed. The possibility of establishing a security working group should be discussed. Such a group may consist of personnel, such as users, program managers, and application sponsors; system, security, or database administrators; security officers or specialists, including the C&A representatives; and system or application analysts. Section 3.6, Contract Performance and Closeout, presents specifications for this group.

For further information about C&A, see the forthcoming NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems*.

- Cyclical Nature of the Process

  The security steps in the Acquisition / Development phase may need to be addressed cyclically. These steps interrelate and build on each other. Depending on the size and complexity of the system, these steps may be performed often as ideas are refined.

- Evaluation and Acceptance

  The system evaluation plan and appropriate acceptance criteria are developed in the Acquisition / Development phase. The solicitation should be designed for evaluation, which should include testing and analysis. Specifications should be written in a way to make it easy to clearly determine if the implemented system complies with the specification. In general, two separate activities require security testing – contract acceptance and C&A.

[13] One advantage of using the system PP format is that a well-defined place exists for assumptions about the system environment, including such management and operational security controls.

Contract acceptance usually addresses only the functional and assurance security specifications contained in the contract with the developer. C&A testing also includes management and operational security controls implemented by the organization. The existence and correct operation of controls, which may be assumed by the developer, may have been included as assumptions in the system security requirements. An adequate determination of the organization's security controls as implemented is part of C&A testing. Acceptance testing of the security properties of the developed system is a prerequisite to security testing under the C&A process.

- Request for Proposal Development

  An RFP enables the Government to make a best value decision based on an offeror's proposal. A strength of the RFP process is the flexibility it provides the Government and offeror to negotiate a contract that best meets the Government's needs.

  The Government can identify needed IT security features, procedures, and assurances in many ways. An RFP can be a flexible document. Guidance on acquisition alternatives should be obtained from the organization acquisition office or the contracting officer.

- Security Specifications and Statement of Work Development

  Specifications and the SOW are based on the requirements analysis. The specifications provide detail of what the system is supposed to do. Specifications should also be written independently of the implementation mechanisms, strategy, and design. In other words, the specifications should state *what* the system is to do, not *how*.

  The security functional requirements in a system PP based on the CC are excellent examples of security specifications. The choice of words in the PP as "functional requirements" should not be confusing; for contracting purposes, these are actually specifications.

  The developer's implementation of the system in conformance with the specifications can and should be tested. This implies that well written specifications are those that can be tested.

  The SOW details what the developer must do in the performance of the contract. Any deliverable that is not part of the system is specified in the SOW. Documentation developed under the contract, for example, is specified in the SOW. The security assurance requirements in a system PP based on the CC are excellent examples of SOW tasking. The security assurance requirements detail many aspects of processes the developer follows and what evidence must be provided to assure the organization that the processes have been conducted correctly and completely. The list of all deliverables that are not parts of the system is called the Contract Data Requirements List (CDRL). The specification of what a deliverable must contain is called the Data Item Description (DID). It is important that the security specifications in the SOW are instantiated in corresponding CDRLs and DIDs.[14]

  There is an exception to the general rule that security functional requirements map into security specifications. Selection of mechanisms to implement security functions may occur during the system operation life cycle rather than during proposal preparation. Such decisions may be deferred to the system operational life cycle to respond to changes in technology or the security environment. For example, the authentication mechanism may change from memorized reusable password to token to biometric technique during the life cycle. The acquiring organization may deal with selection of mechanisms to implement security functions during the system operation life cycle by tasking the

[14] The assurance requirements in the CC actually contain specifications that are suitable for incorporation in DIDs. These are titled "Content and presentation of evidence elements,".

developer in the SOW to perform a study and to recommend a mechanism or combination of mechanisms. The selection of the mechanism or combination of mechanisms remains the procuring organizations function.

Where possible, the organization should support interoperability by specifying mechanisms that comply with open standards at an appropriate level.

Experience has shown that if the specifications, SOW, CDRLs, and DIDs do not delineate the security properties of the system completely and unambiguously, then the system may not achieve the desired level of security.

The following sections describe two sources for information security specifications: general specifications and federally mandated specifications. The acquisition initiator should focus on what is required and work with the contracting officer to determine the best way to ask for it.

- General Specifications

  Many sources of general information security specifications are available and include NIST guidance documents and guidance from other federal agencies, commercial sources, and trade organizations.

  General information security specifications should be reviewed for applicability to the system being procured. These specifications may provide information about overlooked areas. They can also save time because they provide language that can be used directly. However, care should be taken when selecting features, procedures, and assurances from these sources. The items may be grouped in these documents based on interdependencies among the items. It is necessary to understand the features, procedures, assurances, and groupings before specifying them separately.

  Each specification must be justified from the requirements analysis, specifically from the risk assessment. Safeguards recommended by a general source should be considered, but they should not be included in an RFP if the risk assessment does not support them.

- Federally Mandated Specifications

  Agencies must also include additional specifications in the RFP, as required by law. These are often referred to as directed specifications. All federal agencies must ensure that systems comply with applicable FIPS publications. Agencies must also comply with OMB Circular A-130. Agencies may require directed specifications, which are official policies issued with the concurrence of organization's legal and acquisition officials.

  Directed specifications must be incorporated in an RFP or other applicable acquisition document if the system being acquired matches the criteria in the directed specification. It is very important to be aware of directed specifications.

  It is the acquiring agency's responsibility to incorporate applicable law, regulations, and policy in the RFP. In addition to mandates affecting the entire Executive Branch, each department and independent agency has its own set of directives, orders, and standards.

  Merely citing the requirements separately from technical specifications has proven to be inadequate. Leaving it up to the development contractor to interpret policy does not work. Rather,

relevant policy and guidance should be interpreted or at least referenced in the technical security specifications.

FIPS publications may be found at the NIST Computer Security Resource Center (http://csrc.nist.gov). Applicable OMB circulars, memorandums, and policy documents may be found at http://www.whitehouse.gov/omb.

When a single product is being acquired, a PP may be cited in an RFP. However, when product integration is required, it is not sufficient to merely cite these PPs. Additional specifications are necessary to address the security properties of the integrated system.[15]

The National Technology Transfer and Advancement Act of 1995 (Public Law [P.L.] 104-113) directs federal government departments and agencies to use, when practical, technical industry standards that are developed in voluntary-consensus-based standards bodies.[16]

It is incumbent on the acquisition initiator to know what federally mandated specifications apply to the system(s) being procured. Many people erroneously believe that the contracting officer is responsible for this effort. Because these are technical issues, the responsibility is that of the acquisition initiator.

- Proposal Evaluation

The proposal evaluation process determines if an offer meets the minimum requirements described in the RFP and assesses the offeror's ability to successfully accomplish the prospective contract. This effort involves a technical analysis of the merits of a proposal. As part of the Acquisition / Development phase, the acquisition initiator, working with the contracting officer, develops an evaluation plan to determine the basis for the evaluation and how it will be conducted. The evaluation itself is performed during the Source Selection phase of the acquisition. Information security should be addressed in the evaluation criteria to call attention to the importance of security to the Government. Offerors study the RFP (particularly, RFP Sections L and M) to understand what the Government considers most important.

- Developing an Evaluation Plan

When evaluating information security features, it can be difficult to assess if the offer meets the minimum requirements or can successfully accomplish the prospective contract. Therefore, offerors should provide assurance to the Government that hardware and software claims regarding information security features are true and that the offeror can provide the proposed services. Because information security, like other aspects of computer systems, is a complex and important subject, the offeror's assertions may not provide sufficient assurance. If the proposed products for use in the system have been evaluated under the NIAP or CC Recognition Arrangement, it will be easier to determine if the security features in an offeror's product meet the requirements stated in the acquisition documentation. In addition, Section 3.4, Security Documentation, provides descriptions of documentation that can be used for assurance in the evaluation phase, such as the offeror's strategy for security.

[15] In general, the organization will be acquiring integrated systems, and the citation of evaluated products conforming to single product PPs is insufficient. System PPs can be used to express security requirements, if appropriate.

[16] Information about voluntary industry standards is available from the National Standards Systems Network (NSSN). NSSN is a cooperative partnership between the American National Standards Institute (ANSI), U.S. private-sector standards organizations, government agencies, and international standards organizations (http://www.nssn.org)].

How assurances are provided may determine the Government's ability to adequately assess them. The SOW specifies Government's requirements on the development of the system, including the assurance requirements. Assurance specifications typically include documentation that will be examined by the Government. Such deliverables are identified by CDRLs. The form of the documentation is specified in a DID. After award, if the Government determines that more assurance is required, additional funding may be required to fully develop the system.

The determination of how the offerors will be required to provide assurance should be considered when developing the evaluation plan. This plan will be used to help develop RFP sections that provide instructions to the offerors and information about how the proposals will be evaluated and how source selection will be performed.

As part of this process, a determination of security acceptance testing should be made. It may be important to coordinate ST&E as part of acceptance as well as C&A to effectively manage the Government's efforts.

A certain amount of test and evaluation may occur as part of proposal evaluation. Benchmarking and functional demonstrations can be employed. Benchmarking has included stress testing (e.g., response time, throughput), which is similar to some security testing. Selecting the breadth and depth of such benchmarking is a business decision. Both the Government, as purchaser, and the offeror incur costs. Either party may decide that the costs are prohibitive. It may be possible to structure proposal evaluation to limit the number of proposals that receive intensive ST&E. For example, security functional demonstrations could be required of all offerors, whereas assurance and penetration testing could be applied to only the apparent selectee.

There are significant differences among ST&E of existing products, systems to be developed, and services. Organizations will have some uncertainty about the systems to be developed and services. One approach is to consider the failure to deliver the proposed security functions, assurances, and services as a breach of contract for which various legal remedies exist. The Government can structure the preaward functional demonstrations so that they provide meaningful and consistent results for evaluation purposes.

It is important that the threats to security and organizational security policy commitments be clearly articulated and that the proposed security measures be demonstrably sufficient for their intended purpose. Assurance should be based on an evaluation (active investigation) of the product or information system that is to be trusted. The validity of the documentation and of the resulting IT product or system should be measured by expert evaluators with increasing emphases on scope, depth, and rigor.

Assurance specifications can be taken from the CC, or written in a style that conforms to the CC examples, and incorporated in the SOW. A well-written specification is one that can be evaluated.

Architecture and design have a significant impact on vulnerabilities and testing. Good design includes testability as criteria. The cost of ST&E can be minimized by architecture and design that reduces the security impact of employing systems and services with unknown security properties, such as products that have not completed a CCEVS evaluation. Security architecture and design should employ techniques (e.g., encapsulation and isolation), and mechanisms (e.g., demilitarized zones and firewalls), to mitigate vulnerabilities and risks and the cost of ST&E.

Security architecture that integrates countermeasures should be considered. These countermeasures include point solutions for individual networks (e.g., firewalls and intrusion detection systems [IDS]);

security information management (SIM) systems; and (3) SIM integration with a secure network management (SNM) system.

- Items to Consider in the Evaluation Plan

  The remainder of this section presents ideas to help develop the information security portions of the evaluation plan. One important aspect of the evaluation plan is selecting evaluation team members. Section 3.2.3, Source Selection, discusses some of the roles and duties of the evaluation team.

  When the evaluation plan is developed, the alternatives may conflict with each other. For example, features that provide information security can conflict with those that provide ease of use. The Government should clarify how offerors propose different configurations and present conflicting options and tradeoffs. However, care should be taken to keep the size of the proposal manageable to facilitate review and to minimize proposal preparation costs.

  Testing is one method of determining if the proposed system or product can meet the information security requirements. Depending on the nature of the system, testing can be part of the proposal evaluation, in the form of live test demonstrations or benchmarks, or it can be part of post-award acceptance testing. During the evaluation process, testing can be used at different times, depending on cost, technical, and acquisition integrity considerations. Expensive tests should be kept to a minimum to help control offeror proposal preparation costs. Not only do expensive proposals limit competition, but also the costs are ultimately passed to the Government in higher contract costs. Guidance on testing alternatives should be obtained from the contracting officer. Use of products that have been evaluated under CMVP, NIAP or the CCRA may lessen the amount of security testing required for a particular proposal.[17]

  Information system testing, especially performance testing, should be performed with the information security features enabled.

  The more the acquisition initiator knows about the marketplace, the easier it is to develop an evaluation plan. However, proposals cannot be used for market research. The evaluation plan cannot be changed after the receipt of proposals. Additional information from other proposals cannot be used to modify the evaluation plan. It is worthwhile to investigate alternatives that could be offered to ensure the development of an evaluation scheme that reflects the true priorities of the Government.

- Special Contract Requirements

  Some elements in an RFP are information security-related but are not contained in the SOW or the evaluation criteria. These elements usually address rights, responsibilities, and remedies assigned to the parties of the contract. Often, such obligations survive the actual period of performance (POP) of the contract. Therefore, such elements are best addressed through specific contract clauses or requirements. The requirement for nondisclosure of automated information obtained during the course of the contract is one example.

  Chapter 4 addresses clauses and SOW items. The acquisition initiator must coordinate with the contracting officer about clauses to be added to an RFP.

[17] CC evaluations are typically accomplished at the individual product level in an intended environment. Deviation from the CC test environment should be addressed through additional evaluations or testing.

2.3.3 Implementation

Implementation is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the operational environment of the organization.

2.3.3.1 Inspection and Acceptance

Inspection and acceptance refers to the Government's decision to inspect and then accept and pay for a deliverable. The Government should take care when accepting deliverables. Testing by the Government or an independent validation and verification (IV&V) contractor to determine that the system does meet the specifications can be very useful. Testing should include the security of the system.

[**Note:** Official Government acceptance and approval to authorize processing (accreditation) are related, but different concepts. The Government normally accepts a deliverable that meets the contract specifications. The approval to authorize processing is a separate decision made based on the risks and advantages of the system as installed in an operational environment. It is incorrect to have the approval to authorize processing as one of the acceptance criteria because many factors are beyond the vendor's control.]

2.3.3.2 System Integration

System integration 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.

2.3.3.3 Security Certification

Prior to final system deployment, a security certification should be conducted to ensure that security controls established in response to security requirements are included as part of the system development process. In addition, periodic testing and evaluation of the security controls in an information system must be done 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 agency or by an independent third party on behalf of the agency to give agency officials confidence that the appropriate safeguards and countermeasures are in place to protect the agency's information system. In addition to security control effectiveness, security certification 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 accreditation decisions. Agencies should consult 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, Winter 2003-04), or other similar publications for guidance on the evaluation of security controls.

2.3.3.4 Security Accreditation

OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information.[18] This authorization (also known as security accreditation), granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed upon level of

[18] Security authorization is typically only one factor that ultimately goes into the agency decision to place the 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 agency's authorizing official.

assurance and an identified residual risk to agency assets or operations (including mission, functions, image, or reputation). The security accreditation 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 security accreditation decision on whether to authorize operation of the information system and to explicitly accept the residual risk to agency assets or operations.

2.3.4 Operations and Maintenance

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to an organization's needs. When modifications or changes are identified as necessary, the system may reenter another phase of the SDLC. Managing the configuration of the system and providing for a process of continuous monitoring are two key information security steps of this phase.

2.3.4.1 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 of the system. 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 accreditation. An effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. Configuration management and configuration control 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.

2.3.4.2 Continuous Monitoring

FISMA requires periodic and continuous testing and evaluation of the security controls in an information system to ensure that the controls are 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 agency officials are essential activities 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. Agencies should consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, (Initial public draft) or other similar publications[19] for guidance on the ongoing monitoring of security controls.

[19] For example, NIST SP 800-40, Procedures for Handling Security Patches and NIST SP 800-42, Guideline on Network Security Testing.

2.3.5 Disposition

Disposition, the final phase in the SDLC, provides for disposal and contract closeout of the system or contract in place. In general, more than one contract may have existed over the life of the system. For example, the acquiring organization may have chosen to operate and maintain the system using its own personnel, or it may have used another contract. Similarly, disposal may involve a unique contract.

Information security issues associated with disposal and contract closeout should be addressed explicitly. When information systems are transferred, obsolete, or no longer usable, it is important to ensure that government resources and assets are protected.

Usually, there is no definitive end to an SDLC. Systems evolve or transition to the next generation as a result of changing requirements or improvements in technology. Security plans should continually evolve with the system. Much of the environmental, management, and operational information should still be relevant and useful in developing the security plan for the follow-on system.

The disposition activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future if necessary. Particular emphasis is given to proper preservation of the data processed by the system, so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies, for potential future access.

Generally, a system owner should archive critical information, sanitize the media that stored the information, and then dispose of the hardware/software.

2.3.5.1 Information Preservation

When preserving information, organizations should consider the methods that will be required for retrieving information in the future. The technology used to retrieve the records may not be readily available in the future. Legal requirements for records retention should also be considered when disposing of systems.

2.3.5.2 Media Sanitization

Protection of information system hardware usually requires that residual magnetic or electrical representation of data be deleted, erased, or written over and that any system components with nonvolatile memory are erased. This residual information may allow data to be reconstructed, providing access to sensitive information by unauthorized individuals. The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide various levels of protection.

A distinction can be made between clearing information and purging information. Clearing information is removal of sensitive data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities.

Purging is the removal of data from a storage device at the end of a processing period in such a way that there is assurance, proportional to the sensitivity of the data, and that the data may not be reconstructed except through open-ended laboratory techniques. Several commercially available software utilities are available to clear and purge information from an information system so that it cannot be later reconstructed except by very sophisticated and expensive laboratory techniques.

Degaussing, overwriting, and media destruction are some of the methods for purging information. Degaussing is a process for erasing the magnetic media. Overwriting is a process for writing nonsensitive data in storage locations previously containing sensitive data. The following processes may destroy media:

- Destruction at an approved metal destruction facility (e.g., smelting, disintegration, or pulverization)
- Incineration
- Application of an abrasive substance to a magnetic disk.

2.3.5.3 Hardware and Software Disposal

Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposition of software should comply with license or other agreements with the developer and with government regulations. There is rarely a need to destroy hardware, except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations in which the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed. If there is doubt whether sensitive information remains on a system, the ISSO should be consulted before disposing of the system.

Appendix A—Federal Government Request for Proposals

Table A-1. Uniform Contract Format for Federal Government Requests for Proposals

RFP Section	Contents	Created by Technical and/or Acquisition Comments
A. Solicitation/Contract Form	Cover Sheet for RFP (SF 33 or SF 1443). Request for Quotations, use SF 18. If SF not used, details of issuing activity, proposal/quotation general information, and space for offeror/quoter information.	Acquisition contains standard RFP information.
B. Supplies or Services and Prices/Costs	List of Products/Services To Be Provided by Offeror.	Acquisition developed from other portions of RFP. Contains standard RFP information.
C. Description/Specifications/ Work Statement	Defines Scope of Contract and Requirements, Including Mandatory Specifications, Optional Features Services. Specification may be included as an Attachment/Section J.	Acquisition and Technical. Describes product or services to be produced.
D. Packaging and Marking	Shipping, Handling, and Storage Requirements. May Not Be Required for Service Contracts.	Acquisition and Technical. Standard RFP information with special technical requirements if necessary.
E. Inspection and Acceptance	Standards of Performance, Reliability Requirements, Acceptance, Benchmarks, Inspection, and Quality Assurance.	Acquisition and Technical. Determines how product or service is to be accepted and must perform. Contains standard RFP information with specific technical requirements.
F. Deliveries or Performance	Time, Place, and Method of Deliverables/Performance. Describes, for example, Liquidated Damages, Equipment Replacement, Field Modifications, Alternations, Maintenance Response Time and Downtime, Credits, Product Replacement, Variation in Quantity, Delivery and Installation Schedule, and Stop Work Orders.	Acquisition and Technical. Contains standard RFP information with special technical requirements.
G. Contract Administration Data	Contract Administration, Such as Authorities of Government Personnel, Required Reports, Holidays, Use of Government Property, and Financial Information.	Acquisition and usually Technical. Normally standard RFP information with special technical requirements.
H. Special Contract Requirements	Clauses Other Than Those Required By Law/Regulations, Including Warranties, Replacement Parts, Engineering Changes Recording Devices, Hardware/Software Monitors, Site Preparation, Financial Reporting, Transition Requirements, Handling of Data, and Security.	Acquisition and Technical. Normally standard RFP information with special technical requirements.
I. Contract Clauses	Clauses Required By Law/Regulations Not Otherwise Required for a Particular Section.	Acquisition. Contains standard RFP information.
J. List of Attachments	Any Additional Acquisition and Technical Information for Offeror.	Acquisition and Technical.
K. Representations, Certifications, and Other Statements of Offerors	All Statements Required of the Offeror by Law/ Regulation/Organization. Offeror Must Complete and Return with Proposal.	Acquisition. Standard RFP information.

RFP Section	Contents	Created by Technical and/or Acquisition Comments
L. Instructions, Conditions, and Notices to Offerors or quoters	Requirements for Proposals. Specifies the Plans, Approaches, References, and Other Information the Offeror Must Submit. Proposal Instruction. Requires offerors to tell how they will/can meet the requirements described in Section C.	Acquisition and Technical. Addresses how offeror should respond to SOW as set out in the evaluation criteria.
M. Evaluation Factors for Award	Describes how proposals will be evaluated and the criteria against which proposal will be evaluated. Also describes how a source will be selected.	Acquisition and Technical.

For further information, see FAR 15.406.

Appendix B—Specifications, Clauses, and Tasks

This section provides specifications, tasks, and clauses that can be used in an RFP or SOW[20] to acquire information security features, procedures, and assurances.[21,22] These specifications, tasks, or clauses are not mandatory, but are intended as a source of general specifications, as defined in Section 3.2.2. They are written for different types of acquisitions, including the purchase of COTS products, purchase of integrated systems, development of applications, and other computer-related services.

This guide does not provide an exhaustive description of every possible specification, task, or clause. Organizations should use the examples in this appendix as a baseline in developing unique acquisition language to meet the specific requirements of the development.

The specifications, tasks, and clauses are divided into 10 categories. Within each category, there may be specifications, tasks, and/or clauses as well as explanations, considerations, and/or prescriptions about their use. The specifications, tasks, and clauses are printed in *italics.* Explanations, considerations, and prescriptions are in Times New Roman typeface. These specifications, tasks, or clauses should be used carefully and should be tailored to meet individual circumstances. The categories are as follows:

1. General Information Security
2. Control of Hardware and Software
3. Control of Information and Data
4. Security Documentation
5. Legal Issues
6. Contract Performance and Closeout
7. Information Security Training and Awareness
8. Personnel Security
9. Physical Security
10. Information Security Features in Systems.

The categories above do not address the tasking language for specific security services, such as having a risk assessment performed or having contractors prepare security-planning documents. The tasking language for these types of services is provided in the NIST SP 800-35, *Guide to Information Technology Security Services*.

---

20 In performance-based contracting, the organization's SOW is replaced by the statement of objectives (SOO). The SOO defines what the procuring organization wants to procure but not how to achieve this goal. The provider's response will be in the form of an SOW. The language in this section can be used as a guide by an organization in evaluating a provider's response.

21 A word of caution on the use of subcontractors: ensure applicable computer security requirements and/or certifications placed on prime contractors are also reflected in subcontracts. This is called "flowdown."

22 The benefits of specifying compliance to an existing protection profile are that the individual security requirements need not be detailed in the RFP.

B.1 General Information Security

In keeping with OMB Circular A-130, Appendix III, security responsibility for a system must be assigned. This item should be included to clarify responsibility. If the contract calls for information security administration, management, or support, the delineation of responsibilities should be clear, with a government employee retaining ultimate information security program responsibility. OMB Circular A-76,[23] *Performance of Commercial Activities*, provides additional detail regarding what positions are inherently governmental and should or should not be outsourced.

> *The person responsible for information security for the system is <name>.*

The following shows the relationship between organization ownership of information system resources and contractor use. These clauses help establish clear lines of authority and responsibility.

> *The Government authorizes the use of <organization> computer resources (list specific resources if appropriate) for contractor performance of the effort required by the statement of work of this contract.*
>
> *The contractor shall comply with the requirements of the organization information security program as defined by (insert organization handbook, directives, manuals, etc.).*

B.2 Control of Hardware and Software

The Government should consider who can introduce hardware and software onto the system and under what circumstances.

Introduction and Change of Software. To reduce the chance of viruses and other forms of malicious code, illegal use of licensed software, and software that may open security vulnerabilities (such as operating system utilities or untested software updates), organizations should consider restricting contractors by using the following types of specifications and tasks. These specifications and tasks could be used when the contractor is providing a service, such as running or maintaining a government computer system.

> *Only licensed software and in-house developed and authorized code (including government and contractor developed) shall be used on <system name(s)>. Public domain, shareware, or freeware software shall only be installed after prior written approval is obtained from the contracting officer or COTR.*

The previous specification is fairly restrictive. The alternatives that follow can be used to modify the specification.

> *The only hardware and software that shall be used on <system name(s)> is <listed here or specify section>. The contracting officer or COTR must approve all additional hardware and software proposed for use, including upgrades, in advance and in writing.*
>
> *Alternatives:*
>
> 1. *The contractor shall provide a list of software and hardware changes _____ working days in advance of installing (or other time or performance period).*

[23] http://www.whitehouse.gov/omb/circulars/a076/a076.html

2. *The contractor shall provide test environment analysis for proposed hardware and software and state the security vulnerabilities that were addressed (include other assessment items required) _____ working days in advance of installing.*

3. *The contractor shall provide proposed hardware and software for testing _____ working days in advance of loading.*

4. *The contractor shall provide proof of license for new software.*

5. *The contractor shall maintain a list of hardware, firmware, and software changes throughout the contract. The contractor shall provide this list to the Government (specify time frame and/or at the end of the contract).*

If the contractor is using its own software, then the following specification can be used to help protect the Government from buying products developed with stolen software.

The contractor shall provide proof of license for all software used to perform under this contract.

The following clauses are reprinted from FAR 52.239-1, Privacy or Security Safeguards.

FAR 39.106, Contract Clause, prescribes that these clauses, or variations of them, be used in solicitations and contracts requiring security of IT systems or for the design, development, or operation of records using commercial IT services or support services. Clause (a), which addresses ownership of and rights to developed software, should be coordinated with the contracting officer or legal counsel.

(a) The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of government data, the contractor shall afford the Government access to the contractor's facilities, installation, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

One option to modify these clauses is to add a task related to clause (c):

The contractor shall provide an analysis of the new threat, hazard, or vulnerability and recommend possible fixes or safeguards.

The following two clauses address other issues in the use of government hardware and software by a contractor providing services. The Government should include all restrictions such as single site licensing, proper use to maintain warranties, proprietary code, or special considerations.

Under no circumstances is a contractor permitted to make any use of organization computer equipment or supplies for purposes other than performance on this contract.

The following items of government-furnished equipment or software have the following licensing or use restrictions: <provide list>.

The special needs to protect desktop and portable computers should be addressed. Desktop and portable IT security options include security hardware and software, locks, removable hard drives, and antivirus software. Consider if these are needed when desktop computers are acquired or if contractors will be using desktop computers.

The contractor shall not allow its employees to access files that contain employee's passwords.

Consider configuring multi-user systems with a warning message. Pre-logon warning messages can deter unauthorized use, increase IT security awareness, and provide a legal basis for prosecuting unauthorized access. Warning messages can also be used on contractor systems processing federal information.

The system(s) shall be delivered and installed with the following message appearing before logon:

(or)

Contractor multi-user systems used to process data under this contract shall use the following pre-logon warning message:

The Department of Justice manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* describes six considerations when developing a pre-logon warning banner:

- Does the banner state that use of the network constitutes consent to monitoring?
- Does the banner state that use of the network constitutes consent to the retrieval and disclosure of information stored on the network?
- In the case of a government network, does the banner state that a network user shall have no reasonable expectation of privacy in the network?
- In the case of a nongovernment network, does the banner make clear that the network system administrator(s) may consent to a law enforcement search?
- Does the banner contain express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring?
- Does the banner require users to "click through" or otherwise acknowledge the banner before using the network?

One example[24] of a banner is provided:

WARNING**WARNING**WARNING

This is a <organization> computer system. <Organization> computer systems are provided for the processing of Official U.S. Government information only. All data contained on <organization> computer systems is owned by the <organization> may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crime found on <organization> computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, OR CAPTURING and DISCLOSURE.

WARNING**WARNING**WARNING

Another requirement is that the contractor should provide continuity of support and information system contingency plans for government general support systems and major applications, or for contractor systems that process government data. The following statement addresses continuity of support for a mission-essential network, but it can be tailored for other types of systems. To use this clause, the offerors must have sufficient information to be able to postulate the types of emergencies that could occur. It may be necessary to provide additional detailed specifications about these needs to give offerors and evaluators enough information to prepare and review cost estimates and to make objective evaluations.

Add to Section C:

After contract award, the contractor shall deliver a draft continuity of support plan for the system being acquired for organization approval within 90 days of receiving the organization approval and/or guidance on the preliminary plan. The final continuity of support plan shall be delivered 90 days after receiving organization approval and/or guidance on the draft plan. The plan shall be reviewed periodically and updated annually by the Contractor to ensure the accuracy and timeliness of the contents. Recommended updates and revision based on this review shall be submitted to the organization for approval _____ working days prior to incorporation in the plan.

Summary:

- *Preliminary plan submitted with proposal*
- *Draft plan submitted ____working days after organization comment on preliminary plan*
- *Final plan submitted ____ working days after organization comment on draft plan.*

The continuity of support plan shall detail the taking of appropriate and timely action to protect system assets from damage or misappropriation in the event of the threat of a disaster or emergency. The emphasis shall be on avoiding or mitigating the damage caused by such things as fire, flood, or terrorist activity <modify to include threats to the system>. The plan shall, at a minimum --

[24] NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, provides examples of pre-logon warning banners.

- *Include a risk assessment*
- *Include a business impact assessment*
- *Identify essential functions or critical processes, components, and the relationship of critical workload to variables, such as time to recovery*
- *Identify activities that can be suspended temporarily*
- *Identify alternate procedures*
- *Identity action(s) to be taken to mitigate threats.*

> *The continuity of support plan shall detail the taking of appropriate and timely action to return assets to use after damage, destruction, alteration, or misappropriation. The system recovery portion of the plan shall include at a minimum -*

- *Basic strategy for recovery*
- *Specifications for restoration procedures by component and subsystem priority*
- *Testing procedures during redundant operations*
- *Specific responsibilities for incident response.*

> *The continuity of support plan shall state how the plan shall be tested and how often the tests shall be done. Annual testing is required as a minimum, and some tests should be done without advance notice.*

As part of continuity of support and contingency planning, organizations should consider how long the system could remain operable.

> *In the event the system or any component is rendered permanently inoperative, the contractor shall deliver a replacement within <time frame> from the date of request.*
>
> *In the event the system or any component is unavailable for use as a result of maintenance or repair or other reasons for a period of more than <time frame>, or in the event that it is reasonably anticipated that maintenance will exceed <time frame>, the contractor shall make a loaner or replacement available within <time frame>.*

If an alternate site is required for system recovery, and/or the contractor maintains the alternate site, the contractor shall provide –

- *Technical specifications of alternate site*
- *Technical specifications of alternate equipment*
- *Telecommunications requirements*
- *Risk assessment of alternate site.*

In the event recovery of the system at the alternate site is required, the contractor shall make available the alternate site within <timeframe>, for at least <minimum timeframe> and at most <maximum timeframe>.

System recovery should be tested at the alternate site at least annually. A physical security risk assessment should be conducted at least annually to ensure that the facility meets technical and security requirements.

Add to RFP Section L:

As part of the proposal, the offeror shall submit a preliminary continuity of support plan to address the planned reaction to threatened or actual emergencies. Provisions for testing the plan, at the option of the organization, must be included in the proposal.

The offeror shall describe how the proposed architecture, technical capabilities, and organization will protect the system during emergency situations. The plan should state what priority the organization will have in terms of services, replacement hardware, use of alternate site, etc. Examples of how these resources will be used during an emergency are required.

The offeror shall describe external emergency management interface arrangements that will be used with subcontractors if necessary.

The organization is concerned that service may be degraded in a network environment in which systems and network components are shared with others. If the offeror proposes such a shared environment, the offeror must address the following issues:

- *Protection of access for critical organization users*
- *Protection of network access ports from saturation caused by other traffic that may be using the same network access ports*
- *Provision of alternative access and facilities for critical users during periods of overload.*

B.3 Control of Information and Data

Contractors may be required to work with information or data that the organization has designated as subject to nondisclosure. Clauses should be used to prevent the contractor from disclosing the information during the course of the contract and after it has terminated. It is important to work with the contracting officer to ensure that nondisclosure is adequately addressed for both situations.[25]

Any <list type of or all> information made available in any format shall be used only for carrying out the provisions of this contract. Information contained in such material shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an authorized officer or employee of the contractor shall require written approval of the contracting officer (or contracting officer's technical representative [COTR]).

[25] The following contract clauses may be tailored to be applicable during the course of the contract and after it has terminated.

Any <list type of> information shall be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output shall be given the same level of protection as required for the source material.

If it is necessary to disclose <type of> information to perform under the contract, the contractor shall request written authorization from the contracting officer (or COTR) to make such necessary disclosure.

- *Except as provided elsewhere in this contract, the contractor shall not disclose <type of information> except to the individual specified in this contract.*
- *Only those disclosures specifically authorized in writing by the contracting officer (or COTR) may be made, and only when it is clearly shown by the contractor that such disclosures are essential to successfully perform under this contract.*
- *Should the contractor or one of their employees make any unauthorized disclosure(s) of confidential information, the terms of the Default clause (FAR 52.249-8), incorporated herein by reference, may be invoked, and the contractor will be considered to be in breach of this contract.*

If nondisclosable information is released to prospective offerors to enable them to prepare proposals, the following clause can be used during the release of information.

I hereby certify that I will not disclose (type of information) unless authorized in writing by the contracting officer. I agree that, whether or not a contract is awarded to me, I will keep all information in confidence.

The following item can be used to prevent nondisclosable information from leaving the organization's control such as through storage on a hard drive that is sent out for maintenance.

The contractor shall ensure that <list type of> information shall not be released outside the control of the organization <or specific organization office>, including release for maintenance or replacement purposes, without the written consent of the contracting officer or COTR.

B.4 Security Documentation

Security documentation provides instructions for users about the use of the system's security features. Security documentation also supports a demonstration of meeting the requirement. The items below are divided into proposal and deliverable documentation. Documentation that shows that a requirement has been understood will be received as part of the proposal and will be used to evaluate the offeror. Instructional documentation will be received as a deliverable after contract award. Documentation, such as test reports that show that the contractor has successfully met the security requirement will normally be received as a deliverable after contract award.

Different types of documents can be required depending on the nature of the acquisition. For example, an approach, abstract, or outline of security features in the system User's Guide can be included in the proposal with the final version as a deliverable. In the proposal phase, the document would be used to evaluate the offeror's understanding of the security requirement and ability to meet the requirement. As a deliverable, the document would become instructional documentation. The documentation that is

requested with the proposal should be used to evaluate the offer, but should not constitute a requirement that the offeror prepare deliverables before award.

Component-level documentation may not be sufficient to adequately document a system. System-level documentation should describe the system security requirement and how it has been implemented. In addition, the operating system, application, and security system documentation should be combined with descriptions of the interrelationships among applications, operating system and utilities in its operational environment to form a complete system-level description. Component documentation will generally be off-the-shelf from the component vendor. The contractor will prepare specific system documentation during systems development. In addition, component security targets for CC-evaluated products can be used as essential documentation for evaluated IT security components. Published CC Protection Profiles may also be used to provide technical specifications for system components or may be adapted to provide system-level specifications.

It may be necessary to provide additional detailed specifications, including content and delivery schedule, to give offerors and evaluators enough information to prepare and review cost estimates and to make objective evaluations.

B.4.1 Proposal Documentation

B.4.1.1 Offeror's Strategy for Security

This strategy should be commensurate with the size and complexity of the system. All systems acquisitions should request some form of offeror security strategy. In this strategy, the offeror should state how the product or service would meet the Government's security needs. Offerors of COTS products should match the features of the packages to government specifications and address assurance. For complex system development efforts, this might include a plan for incorporating and assuring security throughout the development. An example of a clause requesting such a plan follows.

> *The offeror shall provide a plan that describes its IT security program. The plan shall address the security measures and program safeguards, which will be provided to ensure that all information systems and resources acquired and utilized in the performance of the contract by contractor and subcontractor personnel:*

- *Operate effectively and accurately*
- *Are protected from unauthorized alteration, disclosure, or misuse of information processed, stored, or transmitted*
- *Can maintain the continuity of IT support for organization missions, programs, and function*
- *Incorporate management, operational, and technical controls sufficient to provide cost-effective assurance of the system's integrity and accuracy*
- *Have appropriate technical, personnel, administrative, environmental, and access safeguards*
- *Notify offeree of any and all vulnerabilities found.*

> *This plan will be included in any resulting contract for contractor compliance.*

Note: In system acquisitions in which multiple CC-evaluated products are planned, but not currently available (or evaluated), it may be appropriate to require the offeror to establish a CC Management Plan, to ensure the availability of CC-evaluated products in the delivered system.[26]

B.4.1.2 Offeror's Internal Security Policy and Plan

Acquisitions that include contract services can ask for this type of assurance document. Depending on the scope of the acquisition, this may include copies of the offeror's applicable information security, personnel security, and physical security policies.

B.4.2 Deliverable Documentation

B.4.2.1 Test Documentation

This documentation is a report that describes the test plan, the test procedures showing how the security features and controls were tested, and the results of the security features and controls of functional testing.

B.4.2.2 Design Documentation

This documentation is a report that describes the offeror's philosophy of security controls and explains how these controls are designed into the system. This report can be the post-contract award counterpart of the offeror's strategy for security; it describes how the strategy was implemented in the system design. The report can also include an informal or formal description of a security policy model and an explanation of how the system enforces the security policy. For systems requiring very high security assurance, formal description languages and mathematical modeling also may be included.

B.5 Legal Issues

The contracting officer and legal department should be consulted about legal issues. This section addresses some issues that the acquisition initiator may want to discuss with organization acquisition and legal staff.

- **Security Violations** – It is possible for computer products to cause security violations, even if the products are functioning correctly. For example, a product containing malicious code (i.e., virus or Trojan horse), bypassing operating system controls, or containing undocumented backdoors that bypass security could cause these security violations. Some manufacturers include backdoors so they can assist customers.
- **Allocation of Contractual Risk and Responsibility** – The FAR contains general clauses that define the respective responsibilities and allocate risks among the parties to a government contract. However, additional clauses may be needed to fully address specific information security requirements. Such clauses, for example, may address guarantees, warranties, or liquidated damages. The specific wording of such clauses may vary from one solicitation to another because they are a function of the particular need for data integrity, confidentiality, or availability and the nature of the system being protected.

[26] NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, describes the concept of assurance and a number of different methods and alternatives of obtaining assurance. Products should be acquired and used appropriate to their risk environment and the cost-effective selection of security measures. When selecting products, the threat/risk environment, cost-effectiveness, assurance level, and security functional specifications should be considered, as appropriate.

Agencies may wish to consider the use of warranties, liquidated damages, and other clauses in establishing the contractor's information security-related responsibilities in contracts. Such clauses, when properly crafted, will provide incentive to the contractor to ensure that its products and services meet the security requirements of the contract. Such clauses, when poorly drafted or overly broad, can unnecessarily increase contract costs, limit competition, complicate contract administration, and increase litigation risk. These clauses must be prepared in conjunction with existing FAR clauses.

- Warranties provide a means to require the contractor to fix products after they have been accepted. A warranty is an agreement by the contractor that it will be liable for meeting the contract specifications for a stated period of time after acceptance. (See FAR 46.7 and 52.246-17 through 20.)

- Liquidated damages provide a means for the contractor to compensate the Government for losses that result from contract delays or other problems. The purpose of liquidated damages clauses and other clauses fixing the contractor's performance responsibilities in the information security area is to provide incentive for the contractor to take reasonable steps to ensure that the product does only what it is intended to do and nothing more. For example, the product should be free from malicious code. If the product results in poor security, the contractor can be required to pay for damages. Because the goal is to acquire secure systems, the extent of the liquidated damages clause (or other such clause) should be commensurate with the anticipated risks and damage to the Government. A specific maximum dollar value can be placed on the damages, or other means can be used to limit the contractor's liability. (See FAR 11.5.)

  [Note: These are not penalties. If a security violation occurs, but does not result in any loss, the contractor should not be responsible for any liability or liquidated damage.]

The following are examples of integrity statements that may be modified to form a warranty, guarantee, or liquidated damage clause. The examples are not intended to be used together and should be modified for the operating environment. There are no examples of customized enforcement clauses (the specific warranty, guarantee, or liquidated damage) because they must be developed with the contracting officer and legal counsel. (FAR 52.246-17 through 20 contain FAR standard warranties.)

- The subject product performs in accordance with all specifications, certifications, and representations reflected in the documentation provided in Addendum 1 except as reflected below:

  _____

  _____

  _____

  _____

- The installation instructions provided with the subject product, if properly followed, shall result in the creation and modification of only those objects listed below:

  _____

  _____

  _____

_____

- The subject product (hardware or software) shall not interact with any other component (hardware, software, or firmware) of the system onto which it is being installed to perform any function not described in the documentation listed below:

  _____

  _____

  _____

  _____

- The instructions provided for removing the subject product from any system onto which it has been properly installed, shall, if properly followed, release back to the system every object used to store the subject product on the system.

- Other than the exceptions listed below, the subject product contains no undocumented functions and no undocumented methods for gaining access to this software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

  _____

  _____

  _____

  _____

- The subject product does not interfere or bypass the system security software [[insert name(s) of security software]. The program code performs only request validation checking and enforces the action that the system security software indicates should be taken. This processing is performed for all users. Any exceptions are listed below:

  _____

  _____

  _____

  _____

- **Flaw remediation** – Flaw remediation is the process of tracking and correcting security flaws by the contractor.

  - The contractor shall document the flaw remediation procedures.

- The contractor shall establish a procedure for accepting and acting upon reports of security flaws and requests for corrections to those flaws.

- The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the system.

- The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

- The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

- The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to the Government.

- The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to the Government.

  Caution is required on the sequence of external reporting of security flaws before the corrections are tested. Potential attackers should not be informed of uncorrected security flaws.

- The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

- **Government Patents and Ownership** – Government patents and ownership of developed software and systems are another important consideration that should be discussed with the contracting officer and legal staff and clearly delineated in RFP and contract text.

B.6 Contract Performance and Closeout

For complex contracts that include the development, implementation, or operation of a computer facility or application, a review group that has security experts can be used effectively to help maintain information security. The group can be composed of a combination of government and contractor personnel. Depending on the operational environment, the group can be used for the following:

- Information exchange
- Configuration management
- C&A issues
- Analysis of security requirements
- Identification of new threats and vulnerabilities
- Identification of changes to the system that affect security
- Recommendation of solutions to security problems as they occur
- Recommendation of tradeoffs between security and other functional requirements.
- Physical and electronic access policy for contractors

- Escrow of source code to purchaser.

The following examples define a security working group used to support an operational system.

> *The contractor shall provide <number and type of> personnel for a security control/review group. This group will address security problems, help provide for the maintenance of certification or accreditation under the control of <government person responsible for information security of system>, report security problems, and make security recommendations.*

The contractor can be made responsible for the administration and support of the group.

> *The contractor shall schedule meetings <time frame>, arrange for (or provide) a room, and record minutes. These minutes will be submitted to the COTR within <time frame> after the meeting. The meetings shall be held <time frame> commencing <time frame> after contract award and continue throughout the period of performance (or other ending time).*

One issue to be resolved in contract closeout is the return or destruction of government data and information. Because information can be easily copied, the return of originals does not fully address the destruction of the information. This issue only needs to be addressed when the Government is processing information on a contractor facility or computer. Be sure that official organization records or information are not destroyed before a copy of the information has been received by the organization (if needed).

> *The contractor certifies that the data processed during the performance of this contract shall be purged from all data storage components of its computer facility, and the contractor will retain no output after such time as the contract is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any organization data remaining in any storage component will be safeguarded to prevent unauthorized disclosures. (Insert schedule.)*

Government-furnished equipment (GFE), including hardware and software, should be returned in accordance with normal procedures. Special information security considerations include the return of the GFE in usable condition. This is especially important if a system continues to operate under the Government's or another contractor's control. The information security can be transferred by having passwords reset by the Government or by having the contractor turn in the passwords. The delineation of security responsibilities during transition should be addressed. No specific language is provided because of the diversity and individuality of systems.

> *Returned software shall be certified to be in its original form.*

Another item to be considered is the contractor's computer accounts on government-owned systems. Accounts no longer needed by the contractor should be terminated to protect government resources (i.e., computer time) and to prevent malicious activity by unauthorized users.

> *When a contractor employee no longer requires access to the system (if the employee leaves the company or the contract), the contractor shall notify the COTR within <time frame>. At contract completion or termination, the contractor shall provide a status list of all users and shall note if any users still require access to the system to perform work under another contract. Any group accounts or other means of gaining access to the system also shall be listed, including maintenance accounts and security bypasses.*
>
> *If a contractor employee is fired or leaves the contract or company under adverse conditions, the contractor shall notify the COTR before the employee is removed. If the removal is unplanned,*

the contractor shall notify the COTR immediately after dismissing the employee. This action will allow the Government to terminate his/her access.

When an employee leaves at contract closeout, it is sometimes important to dispose of computer files and accounts. Often, only the person who created or used the files has sufficient knowledge to dispose of them. If the contractor will be handling official organization records, it is important that disposition be made in accordance with organization records management instructions.

When an employee leaves the contract, the contractor project manager shall ensure that all files are disposed of by transfer to another user, archive, destruction, etc. The contractor project manager shall report (or certify) disposition in (time frame such as in a monthly report or within <time frame> of the employee leaving).

B.7 Information Security Training and Awareness

An important goal of the FISMA is to assure that all personnel involved in the management, use, and operation of federal systems trained in information security awareness and accepted information security practices. OMB Circular A-130, Appendix III, specifically requires federal agencies to provide for the mandatory periodic training in information security awareness and accepted information security practice for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This effort includes contractors and employees of the organization.

The following can be used in the cases where the organization determines that NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* adequately addresses the security training requirement for the contractor. This guidance can be tailored to include specific additional skills, training levels, or audience categories depending on the organization's requirements. A time frame should be specified for when the contractor personnel must have received the training. The use of training certifications should be discussed with the contracting officer.

The contractor shall, at a minimum, certify that all contractor personnel involved in the management, use, and operation of (name of) system(s) who perform work under the subject effort shall have received training appropriate to their assignment as defined in NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

Each contractor employee proposed for the effort shall be identified. The contractor shall certify each as having received IT security training, as defined in NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program."

Additional or refresher training shall be performed within <time period>. Certification of this training shall be provided to the contracting officer no later than <time period> after the training has occurred.

The following are examples of tailoring the training specification.

In addition, all contractor personnel involved in the administration of the access control package shall have received training on the package equivalent to <amount> hours of classroom instruction or <amount> hours of job experience using the package.

The contractor system security personnel shall have received training in the operations of the system that includes a systemic overview, security features, known vulnerabilities and threats, and security evaluation methodologies.

The following can be used when the acquisition organization has specific training minimums that are available to the prospective offerors. The second paragraph may be added as an Instruction to Offerors.

The contractor shall, at a minimum, certify that any personnel who perform work under the subject effort shall have received security awareness and skills training that is equivalent to that received by government personnel at <location>.

It is the responsibility of the prospective offeror to obtain the organization guidelines for this training prior to the submission of a proposal under this solicitation at <address and point of contact>. (Alternate: The organization guidelines can be included as an attachment to the RFP.)

B.8 Personnel Security

Requiring personnel screening of contractor or subcontractor employees as a condition for physical or computer systems access is a recommended safeguard. Each position should be reviewed and designated a level of risk. The level of risk should have a type of screening appropriate to the personnel who are required to perform each position. Personnel screening includes implementations ranging from minimal checks to complete background investigations. The extent of screening is dependent on program or system criticality and function, information sensitivity, system exposure, and the implementation of other management, operational, and technical controls.

The following considerations are important for all contracts:

- Types of informational access requirements that exist under the contract
- Types of screenings required for each type of access
- Review of the screenings before access is granted
- Personnel that will review the screening to determine access privileges
- Responsibility for paying for screenings
- Timing of submission of names and supporting information
- Types of screening (from other government agencies) that can be substituted
- Methods for reported on or certified screening results to the contracting officer.

Different personnel screenings could also be required for different types or levels of access. There are many kinds of screenings. The list below includes forms of possible screenings[27]:

- Review of employment forms completed by the contractor employee
- Personal reference check

[27] This document does not address personnel security requirements for classified access to information. However, reviewing guidance relating to classified access can assist the reader in understanding unique circumstances that may require additional personnel security measures. Two of these documents include: Executive Order 12968, "Access to Classified Information," August 2, 1995 and Executive Order 12958, "Classified National Security Information," April 17, 1995.

- Credit check
- Verification of employment for the last 2 years before current employment
- Verification of education (degree obtained, accreditation status, date of degree, etc)
- Local police check in present county and state
- Background check by private organization
- Government background investigation.

Access to the Government's resources is a privilege that should be revoked if a contractor employee becomes a threat to the system.

> *The Government may remove access privileges for contractor personnel for unauthorized, negligent, or inappropriate and willful actions. These may include the following:*
>
> - Unauthorized use of the system
> - Introduction of malicious software
> - Unauthorized modification or disclosure of the system or data
> - Unauthorized sharing or disclosure of passwords

In addition to background screenings, personnel security methods, such as employee statements regarding conflict of interest, may be used. Conflict of interest may include acquisition integrity certifications, financial disclosure, or reports on outside activity. Be sure to specify what is required, when the form(s) must be completed, and what access decision(s) are based on the form.

If the organization has a computer systems user agreement that states user information security responsibilities (such as safeguarding passwords), it is appropriate to require that contractor personnel sign the agreement before computer systems access is granted. The following clause can be modified to be more stringent (such as organization receipt of agreement before access is granted).

> *The contractor shall insure that all contractor personnel sign the user agreement prior to having access to organization systems.*

- Care must be taken when addressing contractor personnel. The Government cannot engage in personal services contracts unless specifically authorized by statute (see OMB Circular A-76). Personal services contracts are those in which the Government has an employer-employee relationship with contractor staff. See Part 37 of the FAR, "Service Contracting." Requiring contractor personnel to be screened as a condition for employment under the contract might suggest an employer-employee relationship. However, requiring screening of contractors as a condition for access to government resources is different. It does not imply an employer-employee relationship because the Government is responsible for retaining control of its resources. Although the distinction above may seem minor, it can be essential during a contract. It is important that the distinction be understood to avoid personal services contracts while protecting government resources.

B.9 Physical Security

The following types of clauses can be used for contracts when work will be performed at the contractor location.

Physical security for computer systems can help prevent theft, tampering, and destruction.

> *The contractor shall provide physical security for <list components or systems> other than those in organization-controlled space and for information being transmitted across <list networks>. Physical security measures to be implemented include protecting the following:*
>
> - *Location (e.g., access to hardware, software, and data)*
> - *Hardware*
> - *Software and data.*
>
> *The contractor shall identify <name of system or components> equipment that will be in nonorganization-controlled areas. Methods for physically protecting these systems shall be provided by the Contractor. The protection shall be against damage, unauthorized access, alteration, modification, and destruction, whether by act of nature, accident, or intrusion.*

Information security can be integrated into existing organization clauses for preaward site surveys instead of using this clause, where applicable.

> *When it is determined that a preaward site survey is necessary in order to verify that the security of a facility is adequate, the contracting officer shall notify the offeror that such a survey will be necessary and coordinate with the offeror as necessary. No contract for services or supplies will be awarded until the survey is completed. The recommendations of the <office performing survey>, as appropriate, will be a significant factor in the determination of responsibility.*

B.10 Information Security Features in Systems

Information security features in systems[28] refer to specific functions that can be incorporated into or those integral to the information system. How security features are used in any given information system or network is dependent on a variety of factors, including the operating environment, the sensitivity of the data processed or transmitted by the system, the requirements for availability, and other risk factors. This section addresses several security controls that could be considered during the Acquisition Planning and Acquisition phases of the acquisition life cycle. This list is not exhaustive because there are many different controls that can be applied to a system to achieve the desired level of security. Some of these additional security controls are described in SP 800-27, *Engineering Principles for Information Technology Security (A Baseline For Achieving Security)*. SP 800-53, *Recommended Security Controls for Federal Information Systems*, will establish a set of standardized, minimum-security controls for information systems addressing low, moderate, and high levels of concern for confidentiality, integrity, and availability.

[28] The term "system" is used loosely to mean any collection of components, hardware, software, firmware, and processes. The use of a more specific term is recommended. Terms such as "the offeror's solution" for integration efforts, "the product" for a component buy, "application system," "operating system," or specific references to parts of the system architecture (e.g., "trusted computing base") are a few examples.

For many systems, a combination of features will be used, some of which are incorporated in the operating system and application. For example, additional access controls are commonly incorporated at the application level. File access may still be performed by the operating system. Many different security architectures are possible. Security features should work together in the system environment and the documentation and testing should address the coordinated approach for the security architecture that is selected.

The features described in this section are a combination of basic security controls and some advanced controls. The controls should be described in functional specifications. Individual tailoring to specific environments will probably be required. If the purpose of the acquisition is to acquire off-the-shelf products, market surveys should be performed (in accordance with organization policy) to determine what features are available in the commercial market. Modifying security features of off-the-shelf products can be expensive. For more information on specific products related to each security feature below, refer to the NIST SP 800-36, *Guide to Selecting Information Technology Security Products*.

Additional information about the uses of these features can be obtained from NIST, commercial standards bodies, and organization security officials. The NIST Computer Security Resource Center (http://csrc.nist.gov) catalogues the NIST information security publications that provide additional information about some of these security features. Technical terms and concepts used in this section are explained in the glossary, Appendix C.

B.10.1 Identification and Authentication

Identification and authentication (I&A) are basic building blocks of security features in systems. For many systems, every user-initiated activity within the computer system (e.g., accessing or printing a file, sending a message) should be attributable to a system user. The identification is normally performed when the user logs on to the system. User authentication has been typically performed by the use of passwords; however, system planners and security officials should seek to incorporate the strongest practical authentication technologies commensurate with system risks. To enforce accountability and access control, all users must identify and authenticate themselves to the system.

The system shall:

- *Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to mediate*
- *Be able to maintain authentication data that includes information for verifying the claimed identity of individual users (e.g., passwords)*
- *Protect authentication data so that it cannot be accessed by any unauthorized user*
- *Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user*
- *Raise alarms when attempts are made to guess the authentication data either inadvertently or deliberately).*

The type of user authentication mechanism may need to be specified. These authentication mechanisms can be based on three categories of information: something the user knows, such as a password; something the user possesses, such as a token; and some physical characteristic (biometric) of the user, such as a fingerprint. Authentication methods employing a token or biometric can provide a significantly

higher level of security than passwords alone. Multi-factor authentication mechanisms, such as those involving tokens and biometric data are considered strong authentication mechanisms and considered to be advanced authentication technologies. In addition, cryptography plays a key role in advanced authentication technologies to provide strong user authentication mechanisms (like tokens), server authentication (using digital certificates), and data authentication (using digital signatures). NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,* provides additional detail about the use of public key technology for advanced authentication.

B.10.2 Access Control

Access control ensures that all access to resources is authorized where necessary. Access control protects confidentiality and integrity and supports the principles of legitimate use, least privilege, and separation of duty. Access control measures for computer systems focus on assurances that sufficient management, operational, and technical controls are implemented to protect sensitive data and system or network components commensurate with risk. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses.

Access control systems grant access to information system resources to authorized users, programs, processes, or other systems. Access control can be enforced solely by the application, by the operating system, or by a combination of both.

Access control mechanisms can be user-centric (based on credentials or access rights associated with a user) or resource centric (based on access control lists that detail the access rights of various users on a particular information resource). In addition to associating access rights with a user (based on the user's identity), access rights can also be associated with roles (as in role-based access control [RBAC]), groups, or any other appropriate attribute associated with users.

RBAC has emerged as a promising feature of many database management, security management, and network operating system products. RBAC products allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role; a user may have multiple roles, which provide an appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without limiting them to the "all or nothing" tradition of an access control list.

Access control enforcement based on access rights (also called permissions or privileges) associated with a user/role/group is called Discretionary Access Control (DAC). In addition, there are systems that could enforce access control based on labels (Mandatory Access Control [MAC]) associated with a user (called clearance levels) and resources (called sensitivity levels). The required access control data for DAC and MAC types of enforcement should be based on a defined organization access control policy.

Organizations can help protect their data by controlling who can use an application, database record, or file. Particular attention should be paid to controlling who is allowed to enable or disable the security features or to change user privileges.

Users should ensure that secure applications sufficiently manage access to the data that they maintain. The access control process includes any or all of the following: knowing who is attempting access, mediating access according to some processing rules, auditing user actions, and managing where or how data is sent.

[**Note:** The term "access control" also refers to physical controls. This section addresses the logical access provided by the computer system.]

> *The system shall use identification and authorization data to determine user access to information. The system shall be able to define and control access between subjects and objects in the computer system. The enforcement mechanism (e.g., self/group public controls, access control lists, and roles) shall allow users to specify and control sharing of those objects by other users, or defined groups of users, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be 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 shall be assigned only by authorized users.*

If the system being acquired is to be delivered with access controls established, then the Government must provide a security policy, definition of data objects, and lists of access classes, access types, and accesses (who can do what) to the data objects.

B.10.3 Auditing

Auditing provides protection by enabling organizations to record meaningful actions within the system and to hold the user accountable for each action. Auditing can occur at the operating system level or within a database or application. The recorded audit data can assist the system security officer in determining who is responsible for a problem or how a problem was caused. Audit data can be used to deter users from attempting to exceed their authorizations and to achieve individual accountability. One key to accountability in computer and network systems is the recording and analysis of effective audit trail information.

Some system designers provide for the auditing of specific events with mechanisms that cannot be turned off by the operator or system security officer. More commonly, system designers supply audit capabilities that can be turned on or off at the discretion of the operator or system security officer, thus allowing each local site to "tune" its auditing. A number of tradeoffs must be made in deciding what is to be audited and how often and should be considered before the acquisition of the system.

A government management official should be responsible for selecting which events have the potential to be audited and, after system acquisition, which events are recorded in the audit trail. The official must also specify how long audit information is to be retained and on what media. These decisions should be based on how the audit data will be used. Audit thresholds and events should also be reviewed during the C&A process.

The following is a three-part specification for auditing that should be modified for the type of system being procured. The first part of the specification defines the auditing function.

> *The system shall be able to create, maintain, and protect from modification or unauthorized access or destruction of an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.*

The second part of this specification lists what types of events need to be auditable. This list should be modified to include security events relevant to the system function and environment.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers and other security relevant events. The system shall also be able to audit any override of human-readable output markings.

The third part of this audit specification is a description of the audit record. This list should be modified to include only those data elements relevant to the system function and environment.

For each recorded event, the audit record shall be able to identify the date and time of the event, user, type of event, and success or failure of the event. For identification and authentication events, the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events, the audit record shall include the name of the object and the object's label. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity and/or object label.

The audit system should raise alarms whenever a threshold is reached with respect to an auditing system resource (disk space in audit log volume) or when auditing has been turned off (either inadvertently or deliberately).

B.10.4 Cryptography

The NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government,* provides a comprehensive reference for government use of cryptography. This document provides guidance to federal agencies regarding the selection of cryptographic controls for protecting Sensitive Unclassified information. This SP describes the cryptographic selection process as containing one or more of the following steps:

- Perform risk assessment to identify the assets that must be protected, vulnerabilities of the system, and threats that might exploit the vulnerabilities.
- Identify security regulations and policies that are applicable to the system
- Specify the cryptographic security requirements
- Specify the security services that will address the needs identified in the above steps.

Currently, there are four FIPS-approved symmetric algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, and the Escrowed Encryption Standard, "Skipjack." The following FIPS describe or reference these four encryption algorithms:

- AES FIPS 197
- DES[29] FIPS 46-3
- Triple DES FIPS 46-3
- Escrowed Encryption Standard FIPS 185

[29] NIST does not anticipate reaffirming single DES in FIPS 46-4, since its 56-bit key is now vulnerable to key-exhaustion attacks. Applications that use DES should be converted to AES or Triple DES as soon as practical. NIST recommends that new applications select AES encryption.

NIST provides a validation service for cryptographic modules containing approved algorithms. Validations for conformance are required for ALL encryption algorithms and cryptographic modules. See Section B.10.4.5, Cryptographic Validations, for further information on validations.

> *An accredited cryptographic module testing laboratory shall test the cryptographic module and algorithm against all applicable FIPS requirements.*

Data authentication, digital signatures, key management, security of cryptographic modules, and cryptographic validations are important issues that should be considered in specifying cryptographic implementation. These issues are further discussed in the sections below. Agencies should also consider other technical variables such as throughput, system interfaces, and data format. In addition, products that implement the selected encryption algorithm may need to be customized for a particular environment.

B.10.4.1 Data Authentication

Provisions for data authentication should be considered when an agency determines that authentication of the source of data and detection of intentional modifications of data is essential. One method for data authentication is through the use of a MAC. A MAC authenticates both the source of a message and its integrity without the use of any additional mechanisms. MACs can be based on FIPS-approved encryption algorithms such as those above or they can be based on cryptographic hash functions. MACs based on cryptographic hash functions are known as Keyed-Hash Message Authentication Code (HMAC). FIPS are available that describe the two MACs:

- FIPS 113[30] Computer Data Authentication (describes the MAC)
- FIPS 198 Keyed-Hash Message Authentication Code (describes the HMAC)

NIST anticipates the development of future message authentication modes that may be used with the AES algorithm to be included in future releases of NIST SP 800-38, *Recommendation for Block Cipher Modes of Operation*. When available, these modes may also be used for message authentication.

Applying the cryptographic algorithm, a MAC is calculated on and appended to information. To verify that the information has not been modified at some later time, the MAC is recalculated on the information. The new MAC is compared with the MAC that was generated previously. If they are equal, then the information has not been altered.

B.10.4.2 Digital Signature

A digital signature can be used to detect unauthorized modifications to data and to authenticate the identity of the signatory. This capability can be used in information systems anywhere a signature is required. For example, a signature may be needed on an electronic letter, form, or electronic mail (e-mail) message. Like the handwritten signature, the digital signature can be used to identify the originator or signer of electronic information. Unlike its written counterpart, the digital signature can also verify that information has been altered after it was electronically signed.

A digital signature is generated using public key cryptography. Documents in a computer system are electronically signed by applying the originator's private key to a hash of the document. The resulting digital signature and document are usually stored or transmitted together. The signature can be verified using the public key of the signer. If the signature verifies properly, the receiver has confidence that the

[30] Note: FIPS PUB 113 may be implemented in hardware, software, firmware, or any combination thereof.

owner of the public key signed the document and that the message has not been altered after it was signed. Because private keys are known to only their owner, it is also possible to verify the signer of the information to any third party. A digital signature, therefore, provides two distinct security services: non-repudiation and message integrity. Identifying that electronic information was actually signed by the claimed originator to a third party provides nonrepudiation. Determining that information was not altered after it was signed provides message integrity. FIPS 186-2, *Digital Signature Standard (DSS)*, addresses three FIPS-approved algorithms for generating and verifying digital signatures: Digital Signature Algorithm (DSA); Rivest, Shamir, and Adleman (RSA); and Elliptic Curve DSA (ECDSA).

Testing requirements and validation lists are available for DSA, RSA, and ECDSA implementations and can be found at http://csrc.nist.gov/cryptval/dss.htm. These algorithms are also tested and validated by one of the Cryptographic Module Testing (CMT) laboratories.

> *The FIPS-approved public key-based digital signature capability provided by <the system or specific part of the system as defined in the statement of work> shall be validated by a CMT laboratory.*

B.10.4.3 Key Management

Key management is extremely important because the security of any cryptographic system is dependent on the security provided to the cryptographic keys. For a cryptographic system to work effectively, keys must be generated, distributed, used, and destroyed securely. NIST is preparing specific key management standards and recommendations; however, they are now available only in draft form and not yet in a state suitable for inclusion in acquisition specifications. Pending completion of the NIST key management guidance, agencies may use commercially available methods and algorithms, which typically employ public key methods.

Key management can be a complex issue for large or diverse systems. Any key management system should meet the system's specific needs.

B.10.4.4 Security of Cryptographic Modules

The security of cryptographic modules refers to the secure design, implementation, and use of a cryptographic module. The security of cryptographic modules is important because cryptography is often relied on as the exclusive means of protecting data when the data is outside the control of the system. The protection of the data is, therefore, reliant on the correct operation of the cryptographic module. The confidence that a module is operating correctly is referred to as assurance.

FIPS PUB 140-2, *Security Requirements for Cryptographic Modules,* establishes the physical and logical security requirements for the design and manufacture of cryptographic modules used to protect sensitive unclassified information. FIPS 140-2 supersedes FIPS 140-1 and incorporates not only changes in applicable standards and technology since the development of FIPS 140-1, but also changes that are based on comments received from the vendor, laboratory, and user communities.

FIPS PUB 140-2 defines four levels of security, with Level 1 being the lowest and Level 4 being the highest. Based on the level of assurance required that is determined during the security requirements phase, an appropriate overall FIPS PUB 140-2 level should be identified. NIST may be able to provide additional information, which can help agencies identify the appropriate level. The identification of the overall security level should be specified in the acquisition package.

Currently, agencies must require that cryptographic modules used to protect sensitive, unclassified information have been validated under the CMVP, ensuring that they have been tested and validated to conform to FIPS 140-2. NIST maintains a list of validated modules at http://csrc.nist.gov/cryptval/.

> *Cryptographic modules provided by <the system or specific part of the system as defined in the statement of work> shall be validated under the Cryptographic Module Validation Program to conform to FIPS 140-2, Level <insert level>.*

B.10.4.5 Cryptographic Validations

NIST provides cryptographic validation services through CMVP for FIPS 140-2, FIPS 197, FIPS 46-3, FIPS 81, FIPS 186-2, FIPS 180-2, and FIPS 185. NIST and the Communications Security Establishment (CSE) of the Government of Canada established the CMVP in July 1995. NIST's National Voluntary Laboratory Accreditation Program (NVLAP) accredits the third-party laboratories that conduct tests under the CMVP.

Validations are no longer performed for the MAC standards, but the standards remain in effect.

After encryption algorithms and modules are validated, NIST issues a validation certificate and adds the products to the appropriate validation list. Validation lists are available from NIST. Manufacturers, integrators, and offerors must use BOTH encryption algorithms and modules that have been validated to claim that their products are FIPS compliant. The offeror should be able to identify the validated implementation used in the product by supplying a copy of the validation certificates.

NIST has issued other standards and guidelines that relate to cryptography. A list of NIST security-related publications is available at http://crsc.nist.gov.

B.10.5 System Integrity

The Government can use commercial products with diagnostic capability to validate the correctness of the hardware and firmware operations. However, such diagnostic offerings are not usually appropriate for verifying the correctness of the software implementation. Depending on the level of system risk, there are a number of ways that the correctness of software operation can be ensured.

> *Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the system.*

Some vendors are using cryptographic techniques to verify the integrity of their software. These techniques can be used to ensure that software received, or has in storage, the same software as the "master" copy of the software maintained by the vendor.

B.10.6 System Architecture

The use of advanced system architectures can provide assurance that the security features are correctly and effectively implemented. High-security architectures are not commonly used in commercial products and they tend to be significantly more costly. Accordingly, their specification in acquisition will need to be justified by perceived system risk.

In addition, the procuring organization should be aware that over specifying the architecture for a system could preclude integrators from incorporating otherwise valid existing products. Over specifying can also eliminate lower cost alternatives, resulting in a more costly acquisition. This over specification is a

common problem that is usually not cost effective. From a security perspective, over specification can actually make adequate information control more difficult.

> *The mechanisms within the application that enforce access control and other security functions shall be continuously protected against tampering and/or unauthorized changes.*
>
> *The security-relevant software shall maintain a domain for its own execution that protects its security mechanisms from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the system may be a defined subset of the subjects and objects in the computer system. The system shall maintain process isolation through the provision of distinct address spaces under its control. The system shall isolate the resources to be protected so they are controlled by the access control and auditing requirements.*

[Note: "Domain" refers to the protection environment in which a process is executing. Domain is sometimes also referred to as "context" or "address space."]

B.10.7 Media Sanitizing

With the more prevalent use of increasingly sophisticated encryption systems, an attacker wishing to gain access to an organization' sensitive data is forced to look elsewhere for information. One avenue of attack is the recovery of supposedly deleted data from media or memory. This residual data may allow unauthorized individuals to reconstruct and thereby gain access to sensitive information. Media sanitization can be used to thwart this attack by ensuring that deleted data are completely removed from the system or media.

When storage media are transferred, become obsolete, or are no longer usable as a result of damage, it is important to ensure that residual magnetic, optical, or electrical representation of data that has been deleted is no longer recoverable. Sanitization is the process of removing data from storage media, such that there is reasonable assurance, in proportion to the sensitivity of the data, that the data may not be retrieved and reconstructed. Once the media are sanitized, it should be impossible or extremely difficult and time-consuming to retrieve the data. Several accepted methods exist for sanitizing media: overwriting, degaussing, and destruction. Media sanitizing, which typically occurs in the closeout phase of acquisition, is further addressed in Section 3.6, Contract Performance and Closeout.

Appendix C—Glossary

Acceptance	The act of an authorized representative of the Government by which the Government, for itself or as agent of another, assumes control or ownership of existing identified supplies tendered or approves specific services rendered as partial or complete performance of the contract. It is the final determination whether, a facility or system meets the specified technical and performance standards.
Acquisition	Includes all stages of the process of acquiring property or services, beginning with the process for determining the need for the property or services and ending with contract completion and closeout.
Acquisition initiator	The key person who represents the program office in formulating information technology requirements and managing presolicitation activities.
Acquisition technical evaluation	The examination of proposals to determine technical acceptability and merit. This is part of the source selection process.
Best and Final Offer	An opportunity for offerors in the competitive range to submit final proposals.
Bidder	Any entity that responds to an invitation for bids with a bid. See Offeror.
Clinger-Cohen Act of 1996	Also known as Information Technology Management Reform Act. A statute that substantially revised the way that IT resources are managed and procured, including a requirement that each agency design and implement a process for maximizing the value and assessing and managing the risks of IT investments.
Closeout	Includes all final contract activities (e.g., ensuring completion of all requirements, making final payment).
Commercial off-the-shelf (COTS)	Software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.
CC	Common Criteria
Competition in Contracting Act (CICA) of 1984	A statute that made several revisions to federal contracting, including requiring that specifications be developed in an unrestricted manner to obtain full and open competition.
Contract administration	Government management of a contract to ensure that the Government receives the quality of products and services specified in the contract within established costs and schedules.
Contracting Officer	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative	An individual to whom the CO delegates certain contract administration responsibilities, usually related to technical direction and acceptance issues.
CDRL	Contract Deliverable Requirements List
DID	Data Item Description
Deliverable	A product or service that is prepared for and delivered to the Government under the terms of a contract.
Directed specification	A specification that must be included in Statements of Work (SOW) based on federal law, policy, or regulation.
Federal Acquisition Regulation (FAR)	The regulation that codifies uniform acquisition policies and procedures for Executive agencies.
FIPS PUB	An acronym for Federal Information Processing Standards Publication. FIPS publications (PUB) are issued by NIST after approval by the Secretary of Commerce. Some FIPS PUBs are mandatory for use in federal acquisitions.
Flowdown	The extension of prime contractor requirements to subcontractors.
Full and open competition	The consideration of all responsible sources in an acquisition, as required by the Competition in Contracting Act.
ISSO	Information System Security Officer
Information Technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes computers, ancillary equipment, software, firmware, similar procedures, services, and related resources.
Invitation for Bid (IFB)	A solicitation document used when contracting by sealed bids.
Latent defects	Defects that exist at the time of acceptance but are not discoverable by a reasonable inspection.
Liquidated damages	Compensation to the Government for damages that result from the contractor failing to deliver supplies or perform services. (See FAR 12.2 and 52.212-4).
Live test demonstrations (LTD)	The demonstration of capability or period of time during which a government user requires an offeror to perform certain user-witnessed activities. These may include one or more benchmark tests.
Mandatory requirements	Those contractual conditions and technical specifications that are established by the Government as being essential to meeting required needs.
NIAP	National Information Assurance Partnership

Offeror	Any entity that responds to an RFP with a proposal. See Bidder.
POP	Period of Performance
Preaward survey	An evaluation by a surveying activity of a prospective contractor's capability to perform a proposed contract.
Presolicitation	The period preceding release of a solicitation that includes preparation of documentation required by federal regulations.
PP	Protection Profile
Protest	A written objection by an interested party to a solicitation for a proposed contract for the acquisition of supplies or services, or a written objection by an interested party to a proposed award, or the award of such a contract.
Request for Comment (RFC)	An announcement requesting industry comment on a proposed system or other acquisition.
Request for Information (RFI)	An announcement requesting information from industry in regard to a planned acquisition and, in some cases, requesting corporate capability information.
Request for Proposal (RFP)	A formal solicitation document used in negotiated acquisitions normally exceeding $100,000 to communicate government requirements and to solicit proposals.
Request for Quotation (RFQ)	A less formal solicitation document used in negotiated acquisitions valued at $100,000 or less to communicate government requirements and to solicit quotations.
Restrictive specification	A detailed and precise description of an item(s) being acquired that can limit competition (e.g., a desirable feature that is not required nor available from more than one source brand name without the words or equal).
Solicitation	An official government request for bids and proposals often publicized in the *Fed Biz Opps (http://www.fedbizopps.gov)*.
Source selection	The process of evaluating proposals and determining which offeror will be selected for contract award.
Specification	A description of the technical requirements for a material, product, or service. Specifications should state only the Government's actual minimum needs and be designed to promote full and open competition, with due regard for the nature of the supplies or services to be acquired.
Statement of Work	A statement of the technical specification in the RFP that describes the material, product, service or system required by the Government.

Appendix D—References

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, November 1999.

NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication,* October 2000.

NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline For Achieving Security),* June 2001.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

NIST SP 800-35, *Guide to Information Technology Security Services,* October 2003.

NIST SP 800-36, *Guide to Selecting Information Technology Security Products,* October 2003.

NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems,* draft.

NIST SP 800-38B, *Recommendation for Block Cipher Modes of Operation: the RMAC Authentication Mode.*

NIST SP 800-40, *Procedures for Handling Security Patches,* September 2002.

NIST SP 800-42*, Guideline on Network Security Testing,* October 2003.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* draft.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* draft.

NIST SP 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems,* draft.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels (draft).*

NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process (draft)*.

NIST Interagency Report (NISTIR) 6462, *CSPP Guidance for COTS Security Protection Profiles*, December 1999.

Clinger-Cohen Act, 40 United States Code (U.S.C.) 1401 and following, 1996.

Computer Security Act of 1987, Public Law (P.L.) 100-235.

Federal Information Security Management Act of 2002, 44 U.S.C. Chapter 35, Subchapter III. 2002.

Federal Acquisition Regulation (FAR), Department of Defense, General Services Administration (GSA) and National Aeronautics and Space Administration.

Federal Information Processing Standard (FIPS) 46-3, *Data Encryption Standard (DES)*, October 1999.

FIPS 81, *DES Modes of Operation*, December 1980.

FIPS 113, *Computer Data Authentication*, May 1985.

FIPS 140-2, *Security Requirements for Cryptographic Modules,* June 2001.

FIPS 180-2, *Secure Hash Standard (SHS)*, August 2002.

FIPS 185, *Escrowed Encryption Standard*, February 1994.

FIPS 186-2, *Digital Signature Standard (DSS)*, January 2000.

FIPS 197, *Advanced Encryption Standard*, November 2001.

FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

FIPS 199, Standards *for Security Categorization of Federal Information and Information Systems*, final public draft (December 2003).

GSA publication, A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1, December 1998.

International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) International Standard 15408:1999 (parts 1 through 3), *Common Criteria for Information Technology Security Evaluation*, August 1999.

National Technology Transfer and Advancement Act of 1995 (P.L. 104-113).

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, January 2000, *National Information Assurance Acquisition Policy*, http://www.nstissc.gov/Assets/pdf/nstissp_11.pdf

Office of Management and Budget (OMB) Circular A-130*, Management of Federal Information Resources*, Office of Management and Budget, November 2000.

OMB Circular A-76, *Performance of Commercial Activities*, May 2003.

Paperwork Reduction Act of 1995, as amended, (44 U.S.C. 3501 (10) and 3506).

United States Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, http://www.cybercrime.gov/s&smanual2002.htm*, January 2001.

Section 781 of title 50, U.S.C.

Section 831 through 835 of title 50, U.S.C.

Section 552a of Title 5, U.S.C.

Pressman, Roger S. *Software Engineering: A Practitioner's Approach.* 4th Edition. New York: McGraw-Hill, 1997.

Appendix E—Frequently Asked Questions

1. **For whom is the guide intended?**
   NIST SP 800-64 REV. 1, *Security Considerations in the Information System Development Life Cycle*, is intended for the use of acquisition initiators (e.g., the end user, program manager, or contracting officer's technical representative (COTR), contracting officers, and information technology (IT) security officials.

2. **Why was this guide written?**
   Organizations must consider information security in all phases of information resources management, including the acquisition phase. Federal agencies must do this to meet the requirements of Office of Management and Budget (OMB) Circular A-130 and the Federal Acquisition Regulation [FAR]. This guide presents a framework for incorporating security into all phases of the SDLC, from initiation to system disposition. Including information security early in the SDLC for an information system will usually result in less expensive and more effective security than adding security to an operational system once it has entered service.

3. **When should information security considerations factor into the SDLC?**

   Each phase of the SDLC needs to factor in IT security considerations. The longer a program manager waits in the SDLC to incorporate a security control, the more costly this control will be.

4. **What is the acquisition life cycle?**

   The SDLC has five phases:

   - Initiation
   - Acquisition / Development
   - Implementation
   - Operations / Maintenance
   - Disposition.

5. **Who are the key participants in the SDLC?**

   The list and titles of participants will vary depending on the nature and scope of the system and organization; however, key roles include the chief information officer (CIO), contracting officer, COTR, IT investment board (or equivalent), information security program manager, information system security officer, program manager (owner of data)/acquisition initiator, and legal advisor/contract attorney, among others.

6. **How does one identify the protection requirements?**

   The process of identifying functional and other security requirements should include an analysis of laws and regulations such as the Privacy Act, Federal Manager's Financial Integrity Act, Federal Information Security Management of 2002, OMB circulars, agency enabling acts, and other legislation and federal regulations, which define baseline security requirements. After a review of mandated requirements, agencies should consider functional and other security requirements.

7. What is assurance and how does one get it?

Assurance is the degree to which the purchaser of a system knows that the security features and procedures being acquired will operate correctly and will be effective in the purchaser's environment. An analysis to determine the level of assurance will need to be performed to determine the level of assurance that is necessary. Many techniques exist for obtaining assurance, including, conformance testing and validation suites, Common Criteria, evaluations by government agencies, evaluations by independent organizations, evaluations by another vendor, and evaluations by another Government.

8. How does a risk assessment fit into the SDLC?

A risk assessment during the Acquisition / Development phase is a critical step. It is used to determine what types of controls will be cost effective and will form the basis for determining mandatory and desirable specifications for the system.

9. How should an organization evaluate the IT security components of proposals?

As part of the acquisition phase, the acquisition initiator, working with the contracting officer, develops an evaluation plan to determine the basis for the evaluation and how it will be conducted. The evaluation itself is performed during the source selection phase of the acquisition. Information security should be addressed in the evaluation criteria so that offerors will know that it is important to the Government. The evaluation plan will determine how offerors will be required to provide assurance that the hardware and software claims regarding information security features are true and that the offeror can provide the proposed services.

10. What is inspection and acceptance?

Acceptance refers to the Government's decision to inspect, then accept, and therefore, pay for a deliverable. When inspecting deliverables for acceptance, the Government should be careful. Testing by the Government or an independent validation and verification contractor to determine that the system does meet specifications can be very useful. This effort should include testing the security of the system.

11. What happens if the requirements change during contract performance?

After award, changes to the Government's requirements should be minimal. If changes occur, there are mechanisms to modify the contract to accommodate some changes. However, these modifications can be very costly. In addition, some changes may require separate acquisitions and new security controls that are retrofitted to a system are seldom as effective as controls designed into the system.

12. What information security steps occur during the disposition phase?

There are three IT security steps in the final phase of the acquisition life cycle:

- Preserve information
- Sanitize media
- Dispose of hardware and software.

13. Are there other NIST publications that can assist me in incorporating security into the SDLC?

There are some NIST publications that have a direct correlation to the security considerations of table 2-1 of this guide. Other NIST publications can be used as a companion but don't address a specific consideration directly. The table below provides a mapping between security considerations and NIST publications, if one is available.

Security Consideration	NIST Publication
Security Categorization	FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System* NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categorization Levels*
Risk Assessment	NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
Security Functional Requirements Analysis	NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook* NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government* NIST SP 800-27 *Engineering Principles for Information Technology Security (A Baseline For Achieving Security)* NIST SP 800-33, *Underlying Technical Models for Information Technology Security* NISTIR 6462, *CSPP Guidance for COTS Security Protection Profiles*
Security Assurance Requirements Analysis	NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*
Cost Considerations and Reporting	NIST SP 800-55, *Security Metrics Guide for Information Technology Systems* NIST SP 800-65, *Integrating Security into the Capital Planning and Investment ControlProcess*
Security Planning	NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*
Security Control Development	NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*

Security Consideration	NIST Publication
Developmental Security Test and Evaluation	NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems* NIST SP 800-42, *Guideline on Network Security Testing* NIST SP 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*
Other Planning Components	NIST SP 800-35, *Guide to Information Technology Security Services* NIST SP 800-36, *Guide to Selecting Information Technology Security Products*
Inspection and Acceptance	NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*
System Integration	NIST SP 800-43, *Systems Administration Guidance for Windows 2000 Professional* NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices* NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*
Security Certification and Accreditation	NIST SP 800-37, *Guidelines for the Security Certification and Accreditation of Federal Information Systems*
Continuous Monitoring	NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems* NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems* NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* NIST SP 800-55, *Security Metrics Guide for Information Technology Systems* NIST SP 800-61, *Computer Security Incident Handling Guide*