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

Special Publication 800-4A
(Draft)

Security Considerations in Federal Information Technology Procurements

A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials

Recommendations of the National Institute of Standards and Technology

Tim Grance
Joan Hash
Marc Stevens

THIS PAGE INTENTIONALLY LEFT BLANK.

NIST Special Publication 800-4A (Draft)

Security Considerations in Federal Information Technology Procurements

A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials

Tim Grance, Joan Hash, Marc Stevens

COMPUTER SECURITY

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

October 2002

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, Joan Hash and Tim Grance of the National Institute of Standards and Technology (NIST), and Marc Stevens of Booz Allen Hamilton, wish to thank their 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.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

Executive Summary

To meet the requirements of Office of Management and Budget (OMB) Circular A-130 and the Federal Acquisition Regulation (FAR), federal organizations must consider IT security in all phases of information resources management, including the acquisition phase.

Including IT security early in the acquisition process for an IT system will usually result in less expensive and more effective security than adding security to an operational system once it has entered service. The purpose of this guide, *Security Considerations in Federal Information Technology Procurements: A Guide for Procurement Initiators, Contracting Officers, and IT Security Officials*, is to present a framework for incorporating security into all phases of the acquisition process.

The five phases of the procurement lifecycle and the associated IT security steps that should be incorporated into each phase are:

- **Mission and Business Planning Phase–**
  - **Incorporate a Preliminary Sensitivity Assessment**–should result in a brief qualitative description of the basic security needs of the system.
- **Acquisition Planning Phase–**
  - **Integrity, Availability, and Confidentiality Requirements Analysis** –identify the protection requirements through an analysis of laws and regulations that define baseline security and consider functional and other security requirements.
  - **Sensitivity Assessment Update** –update the preliminary sensitivity assessment based on the results of the integrity, availability and confidentiality requirements.
  - **Analysis of the Level of Assurance Required**–address how much confidence is needed that that the IT security will work correctly and effectively. Assurance can be gained through many techniques including, among others, conformance testing and validation suites, Common Criteria, evaluations by government agencies, or evaluations by another vendor.
  - **Risk Assessment**–determine what types of controls will be cost effective and will form the basis for determining mandatory and desirable specifications.
  - **Certifier and Accreditor Review**–ensure a technically qualified person certifies that the security controls on the system, application or networks meet the requirements as required by OMB Circular A-130.
- **Acquisition Phase–**
  - **Specification and Statement of Work (SOW)**–develop specification and SOW based on the acquisition phase requirements analysis.
  - **Evaluation Proposals**–determine if an offer meets the minimum requirements described in the request for proposals (RFP) and conduct an assessment of the offeror's ability to successfully accomplish the prospective contract.
  - **Special Contract Requirements**–identify any special contract requirements. These are requirements not contained in the SOW that address rights, responsibilities, and remedies assigned to the parties of the contract.

- **Contract Performance Phase–**
    - **Inspection and Acceptance–**determine if the deliverables meet the specifications set forth in the contract. If so, the government accepts and pays for the deliverables as stipulated.
    - **Performance Measurement and Monitoring–**Review contract performance to ensure security has not degraded and that changes in the environment and system that result in new threats and vulnerabilities are recognized and appropriate safeguards are put in place.
- **Disposal and Contract Closeout–**
    - **Update the Security Plan**–ensure security plans evolve with the system.
    - **Archive Information**–retain information as necessary keeping in mind legal requirements and future technology changes that render the retrieval method obsolete.
    - **Sanitize Media**–ensure data is deleted, erased and written over as necessary.
    - **Dispose of Hardware and Software**–dispose of the hardware and software as directed by the information system security officer.

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

This document is a guideline to help agencies select and acquire cost-effective IT security controls by explaining how to include IT security requirements in IT system procurement and is intended for the use of procurement initiators (e.g., the user, program manager, or contracting officer's technical representative [COTR]), contracting officers, and IT security officials. It is not a substitute for organization procurement or security regulations, policy, and guidance. As always, close consultation with legal counsel and the contracting officer by the procurement initiators is essential.

Table of Contents

1. INTRODUCTION

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 United States Code (U.S.C.) 278 g-3 (a)(5). This document is not a guideline within the meaning of 15 U.S.C 278 g-3 (a)(3).

These guidelines are for use by federal organizations that process sensitive information. They are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III.

This document may be used by nongovernmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon 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, the Director of the OMB, or any other federal official.

1.2 Purpose

The need to provide protection for federal information technology (IT) systems has been present since computers were first used. Congress has passed several laws relevant to IT security, including the Computer Security Act of 1987 and the Information Technology Reform Act, also known as the Clinger-Cohen Act of 1996. The Office of Management and Budget (OMB) develops executive agency policy on IT security in accordance with existing law and Executive Order(s). Federal IT 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 IT acquisitions. To meet these policies and legal requirements, federal organizations must consider IT security in all phases of information resources management, including the acquisition phase.

Including IT security early in the acquisition process for an IT system will usually result in less expensive and more effective security than adding security to an operational system once it has entered service. The purpose of this guide is to present a framework for incorporating security into all phases of the acquisition process, from early planning to contract closeout and/or system disposal.

1.3 Scope

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

This document has two parts. The first part, included in Section 2.0, explains the integration of IT security into the IT system procurement process. The guide recommends that the following analyses be included in procurement documentation:

- Information sensitivity determination
- Analysis of integrity, availability, and confidentiality requirements
- Analysis of level of assurance required
- Risk assessment.

The second part of this guideline, Section 3.0, contains specifications and contract language for specific IT security features, assurances, and procedures that can be included in IT procurements.

NIST has prepared the following document to address IT security service issues.

- Guide to Information Technology Security Services, draft NIST Special Publication 800-34

The number and type of appropriate security controls may vary throughout a particular system's development and procurement life cycles. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls are all 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.

- Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30.

1.4 Audience

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

2. INCORPORATING IT SECURITY INTO THE PROCUREMENT CYCLE

To be most effective, IT security must be integrated into the procurement cycle from its inception. This guide focuses on the IT security components of the IT system procurement cycle. First, a description of the key security roles and responsibilities that are needed in most IT procurements is provided. Second, sufficient information about the procurement cycle is provided to allow a person not familiar with the procurement process to understand the relationship between IT security and procurement. However, this section does not provide an exhaustive description of the procurement process (See the Federal Acquisition Regulation (FAR) and organization specific policies and procedures for detailed IT system procurement information).

2.1 Key Roles and Responsibilities for Procurement Initiatives

Many participants can have a role in IT system procurements depending on the nature and scope of the system. The names for the roles and titles will vary in different organizations. Each participant does not necessarily work on every activity within a phase. The determination of which participants need to be consulted is as unique to the organization as the procurement. As with any acquisition, it is important to involve the IT Security Program Manager and Information System Security Officer as early as possible, preferably in the Mission and Business Planning stage.

2.1.1 Key Roles

A list of key IT roles is provided below. This list includes roles that are key in many procurements. In some small organizations, a single individual may hold multiple roles.

- **Chief Information Officer (CIO)** – senior official responsible for advising the organization head on the design, development, and implementation of information systems

- **Contracting Officer**[1] – person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings

- **Contracting Officer's Technical Representative (COTR)** – a qualified Government employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a particular contract

- **IT Investment Board (or equivalent)** – responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (section 5)

- **IT Security Program Manager** – responsible for developing enterprise standards for IT security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize IT security risks to the organization. IT 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 making certain that security management activities are conducted as required to meet the needs of the organization.

- **IT System Security Officer** – responsible for ensuring the security of an information system throughout its life cycle, from mission and business planning through disposal

[1] Federal Acquisition Regulation Section 2.101

- **Program Manager (owner of data) / Procurement Initiator** – represents programmatic interests during the acquisition process. The program manager, who has been involved in strategic planning initiatives of the procurement, plays an essential role in security and is intimately aware of functional system requirements.
- **Privacy Officer**[2] – responsible for ensuring that the services or system being procured complies with existing privacy policies regarding protection, dissemination (information sharing/exchange) and disclosure of information.

2.1.2 Other Participants

The list of roles in an IT procurement can grow with the complexity involved in acquiring and managing IT systems. It is vital that all members of the procurement team work together to ensure that a successful procurement is achieved. Since the system certifier and accreditor will be making critical decisions near the end of the procurement process, it is helpful to include them earlier in the procurement so that critical issues can be mitigated early. System users may assist in the procurement 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 information technology, configuration management, design/engineering, and facilities groups.

2.2 IT Security in the Procurement Cycle

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

Table 2-1 shows how security fits into the procurement cycle. The IT security steps in this section describe analyses and processes to be accomplished. These steps define a conceptual framework for IT security planning during the procurement cycle. 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 IT security acquisition specifications. Organizations can use other methodologies or modify the one presented here.

Table 2-2 is provided to assist system developers better understand the relationship between the procurement cycle and the five basic phases of the IT system life cycle:

- Initiation
- Development/acquisition
- Implementation
- Operation/maintenance
- Disposal.

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

This guide focuses on integrating IT security into the IT procurement cycle. For a more detailed description of security planning of IT systems, refer to SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Table 2-1. IT Security in the Procurement Cycle

	Mission and Business Planning	Acquisition Planning	Acquisition	Contract Performance	Disposal and Contract Closeout
PROCUREMENT CYCLE	- Needs Determination: • Perception of a Need • Linkage of Need to Mission and Performance Objectives • Assessment of Alternatives to Capital Assets	- Functional Statement of Need - Market Research - Feasibility Study - Requirements Analysis - Alternatives Analysis - Cost-Benefit Analysis - Software Conversion Study - Independent Government Cost Estimate - Risk Management[3] Plan - Acquisition Plan - Implementation Plan	- Statement of Work - Evaluation Plan - Review of Solicitation - Micro-purchases - Federal Supply Schedule Contracts - Government-wide Agency Contracts - Blanket Purchase Agreements - Invitation for Bids - Request for Proposals - Source Selection	- Performance measurement - Inspection and acceptance - Contract modifications - Performance failure	- Appropriateness of disposal - Exchange and sale - Internal organization screening - Transfer and donation - Contract closeout
SECURITY CONSIDERATIONS	- Preliminary Sensitivity Assessment	- Integrity, Availability, and Confidentiality Analysis - Sensitivity Assessment Update - Level of Assurance Analysis - Risk Assessment - Other Functional Groups Review - Certifier and Accreditor Review - Cyclical Nature of the Process - Other Planning Components	- Security Specifications and SOW Development - Proposal Evaluation - Special Contract Requirements Development	- Inspection and Acceptance - Performance Measurement and Monitoring	- Security Plan Update - Information Archival - Media Sanitization - Hardware and Software Disposal

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

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

<table>
<tr><th colspan="7">Procurement Lifecycle Phases</th></tr>
<tr><td>Mission and Business Planning</td><td colspan="2">Acquisition Planning</td><td>Acquisition</td><td colspan="2">Contract Performance</td><td>Disposal and Contract Closeout</td></tr>
<tr><td colspan="2">Initiation</td><td colspan="2">Development/ Acquisition</td><td>Implementation</td><td>Operation/ Maintenance</td><td>Disposal</td></tr>
<tr><td colspan="7">IT System Lifecycle Phases</td></tr>
</table>

2.2.1 Mission and Business Planning

The first phase in the procurement cycle is Mission and Business Planning. This section addresses the needs determination component of this phase.

2.2.1.1 Needs Determination

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

A need may have been determined from strategic or tactical planning. The following definitions are from the GSA publication, *Acquisition of Information Resources: Overview Guide*:

+ Strategic planning defines the major information resources activities and types of information required by the organization and produces a high-level strategy for pursuing the organization's information resource needs.

+ Tactical planning is the identification, scheduling, management, and control of tasks necessary to accomplish individual activities identified in the strategic plan.

Acquisition planning can begin only after an organization has determined that a need exists. 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 acquisition, the definition of the security requirement should begin with the preliminary sensitivity assessment.

2.2.1.2 Preliminary Sensitivity Assessment

The preliminary sensitivity assessment should result in a brief qualitative description of the basic security needs of the system. In practice, the need for IT 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, non-repudiation). Integrity can be examined from several perspectives. From a user's or application owner's perspective, integrity is a 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 sensitivity assessment should define the threat environment in which the product or system will operate. This sensitivity 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 IT security is defined in NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*.

This step does not require an elaborate sensitivity assessment scheme, but does require a determination of the significance of the systems. Legal implications, federal policy, organization policy, and the functional needs of the system help determine its sensitivity. Important factors that should be considered when assessing sensitivity include:

+ Importance of the system to the organization mission
+ Consequences of unauthorized modification, disclosure, or unavailability of the system or information it contains
+ Requirements to safeguard employee and citizen privacy.

2.2.2 Acquisition Planning

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

2.2.2.1 Requirements Analysis

Agencies establish and document requirements for IT system resources in the Acquisition Planning 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. It draws on and further develops the work performed during mission and business planning.

The following IT security steps should be included in a requirements analysis:

+ Analysis of integrity, availability, and confidentiality requirements
+ Updated sensitivity assessment
+ Analysis of the level of assurance required
+ Risk assessment
+ Review by other functional groups
+ Review by certifier and accreditor.

As stated above, these steps present a conceptual framework for IT security planning and should be used as a guide, example, or roadmap. Other ways to organize the steps needed in the IT security planning process are acceptable. Security requirements should be selected to address all the security objectives defined as a result of the preliminary sensitivity assessment. Therefore, a complete mapping of security requirements can be made to counter the numerous threats to security.

Although this section presents the IT security components of the requirements analysis in a sequential manner, the components can be completed in a different order. Security components of more complex systems will need to be done cyclically until all of the components work together. For smaller acquisitions, all of the components can be combined into one analysis. Figure 2-1 at the end of this section shows how the IT security components of the requirements analysis phase can interact.

2.2.2.2 Analysis of Integrity, Availability, and Confidentiality Requirements

The first step in the analysis is to identify the protection requirements. The analysis will build on the sensitivity assessment performed during the needs determination, but will be more in-depth and specific.

This process should include an analysis of laws and regulations such as the Privacy Act, Federal Manager's Financial Integrity Act, Computer Security Act, 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.

At this level, as opposed to the needs determination level, the analysis should be system specific. The legal, functional, and other IT security requirements should be stated in specific terms. For complex systems, more than one iteration of the requirement analysis components will be needed.

Because most systems have at least minimal integrity and availability requirements, care should be taken to address these areas clearly. IT security is more than confidentiality. Even systems with no confidentiality requirement need security to meet integrity and availability requirements.

2.2.2.3 Update Sensitivity Assessment

After completing the analysis of integrity, availability, and confidentiality requirements, the sensitivity assessment should be updated based on the results.

2.2.2.4 Analysis of the Level of Assurance Required

The correct and effective use of IT security controls is a fundamental building block of system security. 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.

Obtaining assurance can be quite difficult because assurance can be expensive and can be difficult to quantify. This analysis should address how much confidence is needed so that the IT security will work correctly and effectively. The analysis, which should be based on legal and functional requirements, will be used as the basis for determining how much and what kinds of assurance are required. This assurance analysis will lead directly to the evaluation plan, which will be developed in the solicitation phase. It can also be used to help determine appropriate acceptance criteria.

As with other aspects of security, the goal should be cost-effective security that meets the confidentiality, integrity, and availability requirements for protection of an organization's data. Absolute security is difficult to attain while preserving system usefulness and available resources. In each situation, there should be a balance between the benefits to mission performance from system security and the risks associated with operation of the system.

Many techniques exist for obtaining assurance. Some of these techniques are described below.

+ **Conformance Testing and Validation Suites.** Two major security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: (1) National Information Assurance Partnership (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) and (2) NIST Cryptographic Module Validation Program (CMVP).

  The NIAP CCEVS makes use of a network of private sector, accredited testing laboratories to independently evaluate a range of commercial products 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, and public key infrastructure components. The 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.

  The CMVP, also using independent, accredited, private-sector laboratories, focuses on conformance testing of cryptographic modules against Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, and related federal cryptographic algorithm standards. In both programs, a government body validates the results of the testing and evaluation processes to ensure that the security standards are being applied correctly and consistently.

+ **Common Criteria.** The Common Criteria (CC) uses security requirements, such as the evaluation assurance levels [EAL] to provide assurance based upon an evaluation (active investigation) of the IT product or 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.

+ **Evaluations by Government Agencies.** 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. Offerors should be asked to provide information about evaluations that they consider pertinent to their proposal.

+ **Evaluations by Independent Organizations.** CC Testing Laboratories (CCTLs) evaluate IT products against the CC. 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 successfully evaluated IT products and protection profiles on their respective validated products lists (VPL). The NIAP VPL can be accessed at http://niap.nist.gov. Government-evaluated protection profiles can be obtained at the following Web sites:

  – http://commoncriteria.org

  – http://niap.nist.gov

+ **Evaluations by Another Vendor.** Commercial organizations may offer product assurance testing and evaluations. These organizations may lack the independence of government and trade organization evaluations.

+ **Evaluations by Another Government.** Other governments, including several European governments, Canada, Australia, and New Zealand, can evaluate IT products for assurance, as the CCRA establishes a framework to allow recognition of certification and validation processes across international boundaries. The complete list of governments is available at http://niap.nist.gov.

+ **Accreditation of a System to Operate in a Similar Situation.** Once again, these accreditations are not 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. Since accreditation balances risk against benefits, the same product may be accredited for one environment but not for another.

+ **Self-Certification 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.

+ **Self-Certification 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.

2.2.2.5 Risk Assessment

This risk assessment during the acquisition planning 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. The risk assessment should be conducted before the approval of design specifications. In addition, a risk assessment can provide justification in case specifications are protested. This risk assessment will not necessarily be a large and complex document. The analysis, like other risk analyses, should consider assets, threats to the assets, potential vulnerabilities, and what can be done to reduce vulnerabilities. This risk assessment should take into consideration existing controls and their effectiveness. This risk assessment will require participation by the other functional groups.

This risk assessment will use input from the analysis of integrity, availability, and confidentiality requirements as the basis for determining the value of information assets and the impact of security failures. The selection of appropriate types of safeguards should take into consideration the results of the level of assurance analysis. The risk assessment, in turn, may point out deficiencies in the analysis of integrity, availability and confidentiality requirements or the level of assurance analysis by demonstrating the logical conclusion of the analyses.

Further information on the risk assessment process is contained within the risk management methodology as explained in NIST Special Publication 800-30, *Risk Management Guide on Information Technology Systems*.

2.2.2.6 Review by Other Functional Groups

Depending on the size and scope of the system, a team or group of participants from the functional groups described in the beginning of this chapter may be useful. Even for small systems, it may be helpful to get the assistance of the IT security staff. These functional groups should have insight into the integrity, availability, confidentiality and assurance requirements. Getting these groups involved early in the planning process is important because it may result in reduced life-cycle cost and it is easier to change requirements in the early stages. The IT security staff can:

+ Demonstrate that the security plan for this project 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

2.2.2.7 Review by Certifier and Accreditor

OMB Circular A-130, Appendix III requires that systems be approved for processing based on the validation of the safeguards. This process is referred to as accreditation. Technically qualified personnel certify that the security controls in a system, application or network meet the requirements. Accreditation is the decision to permit the system to operate for a specific purpose with specific sensitivities of data and is made by a senior management official (accreditor).

Because the accreditor is responsible for accepting the risk of operating the system, the accreditor can advise the acquisition team if the risks associated with eventual operation of the system appear to be unacceptable. 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 acquisition team and accreditor should also discuss what forms of assurance the accreditor needs to make a decision. This assurance can include system tests and other items that need to be addressed in the solicitation. The concept of assurance is further described in NIST Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition / Use of Tested / Evaluated Products*.

In addition, the procurement initiator and the accreditor should discuss how changes to the system and its environment will be addressed. The possibility of establishing a security working group should be discussed. Such a group can consist of various 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 draft NIST Special Publication 800-37, *Federal Guidelines for the Accreditation of Information Technology Systems*.

2.2.2.8 Cyclical Nature of the Process

The security steps in the requirements analysis portion of the Acquisition Planning phase may need to be performed cyclically. The steps interrelate and build on each other. Depending on the size and complexity of the system, these steps may be performed often as ideas become refined and focused. Figure 2-1 illustrates how the IT security steps of requirements analysis can work together.

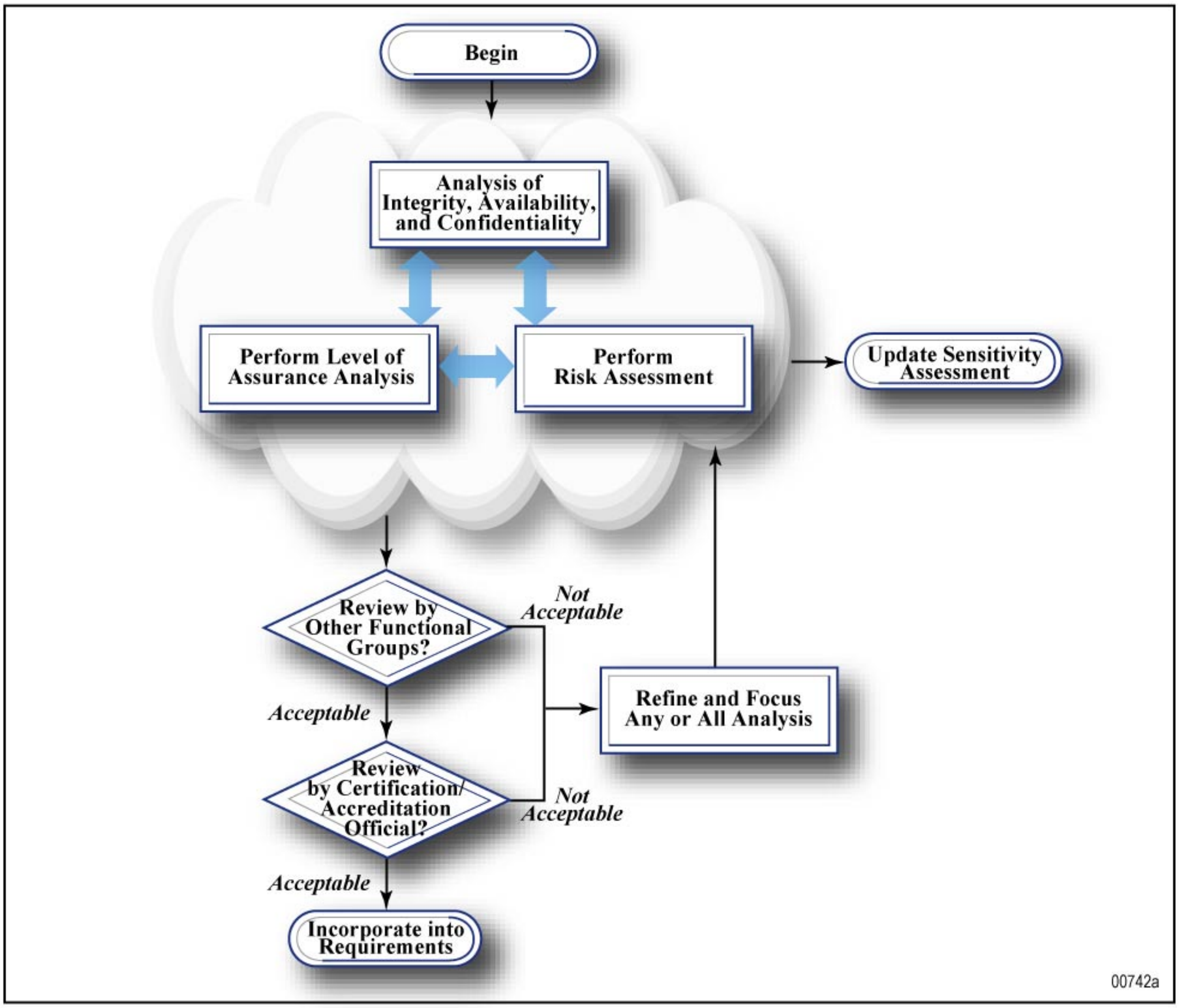
Begin
Analysis of Integrity, Availability, and Confidentiality
Perform Level of Assurance Analysis
Perform Risk Assessment
Update Sensitivity Assessment
Review by Other Functional Groups?
Not Acceptable
Acceptable
Refine and Focus Any or All Analysis
Review by Certification/ Accreditation Official?
Not Acceptable
Acceptable
Incorporate into Requirements
00742a

Figure 2-1. Flow Model for IT Security Components

2.2.2.9 Other Planning Components

Several other parts of the Acquisition Planning phase contribute to IT security:

- Feasibility Study
- System Cost-Benefit Analysis
- Software Conversion Study
- Alternatives Analysis
- IT Security Capital Planning
- Market Research

The Feasibility Study should also look at the IT security of the system. If security is not considered during the feasibility study, then it is possible? that a computer system might be acquired for which there is no practical cost-effective security solution.

The Cost-Benefit Analysis should use input from the planning phase risk assessment. If the analysis does not consider security, then it is possible for it to favor a system that will later require security upgrades (impact to system cost). Further, such a cost-benefit analysis could favor a system with unnecessary exposures to traumatic failures.

The Software Conversion Study, which examines the cost of reestablishing software on a new hardware or software base, should include the cost of reestablishing the desired degree of IT security on the new system and maintaining security during the transition.

The Alternatives Analysis should rate the alternatives against their ability to meet all the requirements, including IT security.

IT capital plans are developed when organization budget levels are insufficient to cover a proposed project. Most IT projects go through the capital planning process before the acquisition phase of the procurement cycle. In some cases, the capital plan is later revised and updated as actual cost data replaces initial projections. Additionally, a capital plan may be developed for a major modification to a system if the modification will result in a significant cost impact to the organization budget. Each organization should develop a process for allocating funding to security features and capabilities of the system.

The Market Research, which may include Requests for Comment (RFC) or Requests for Information (RFI), should include the IT security requirements.

At the end of the Acquisition Planning phase, the government will have determined the requirements and the best ways to achieve them. This effort will include a decision on whether a requirement can be met through acquisition or in-house development. Many systems combine these methods. Because this phase looks at the whole system, the IT security and other functional requirements should have been adequately addressed to allow acquisition of components while maintaining system integrity.

An investment justification and capital plan should be developed throughout the Acquisition Planning phase. The efforts performed in this phase will lead to the development of a funding request and subsequent submittal of the request to the organization's IT Investment Review Board. The approval can be used to ensure that the IT system procurement process incorporates a rational, risk-based approach to security planning.[4][5]

2.2.3 Acquisition

The third phase in the procurement cycle is the Acquisition phase. This covers the development and issuance of the RFPs and the receipt of proposals. All considerations surrounding the acquisition of the product or service must be addressed in this phase. This includes the description of what is being acquired; how it will be acquired; how it will be evaluated, tested, and accepted; and how the contract will be administered.

[4] In accordance with the Information Technology Reform Act, also known as the Clinger-Cohen Act

[5] OMB A-130 [8b1a (iv)] requires that as part of the agency IT capital plan, the agency must "demonstrate that IT projects and the [enterprise architecture] include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from NIST security guidance.

An RFP is designed to enable the government to make a best value decision based on an offeror's proposal. One of the strengths of the RFP process is the flexibility it provides the government and the 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 that allows for substantial creativity. Guidance on procurement alternatives should be obtained from the organization procurement office or the contracting officer.

This section explains some of the considerations for developing the IT security portion of a statement of work (SOW) or specification and provides general guidance about evaluation, testing, and acceptance of the IT security features. Because of the flexibility, it is impossible to address precise mapping of the IT security considerations into the uniform solicitation. The procurement initiator needs to decide how the IT security considerations will be met given the many options an RFP provides. The procurement initiator must therefore decide how a given feature, procedure, or assurance fits in the RFP. In addition, this guideline provides sample SOW language that may be tailored for an organization's specific needs.

2.2.3.1 Specifications and Statement of Work

The SOW or specification is based on the Acquisition Planning phase requirements analysis. This section describes two types of sources for IT security specifications: general specifications and federally mandated specifications. Security requirements can be included in the SOW in various ways, for example, in specifications, tasks, labor, work, or level of effort. The procurement initiator should concentrate on what is required and work with the contracting officer to determine how to ask for it.

General Specifications

Many sources of general IT security specifications exist, such as NIST guidance documents and guidance from other federal agencies, commercial sources, and trade organizations.

General IT security specifications should be reviewed for applicability to the system being procured. They may provide information about areas that were overlooked. They can also save time because they provide language that can be used directly in a SOW. 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 between 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 Acquisition Planning phase 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 required by law in the RFP. These are often referred to as directed specifications. All federal agencies must ensure that systems comply with applicable Federal Information Processing Standards (FIPS) publications. Agencies must also comply with OMB Circular A-130. Agencies may also require directed specifications, which are official policies issued with the concurrence of organization legal and procurement officials.

Directed specifications must be incorporated in an RFP if the system being acquired matches the criteria in the directed specification. It is very important to be aware of directed specifications. If specifications in an RFP conflict with directed specifications, a waiver must be obtained.

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

Government-developed Protection Profiles may also be considered as Federal security specifications for an RFP. For example, an RFP may require a network with an operating system that complies with the Protection Profile for Single Level Operating Systems in Environments Requiring Medium Robustness, Version 1.01.

The National Technology Transfer and Advancement Act of 1995 (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.[6]

It is incumbent on the procurement initiator to know what federally mandated specifications apply to the system(s) being procured. Many people erroneously believe that this is the responsibility of the contracting officer. These are technical issues and are, therefore, the responsibility of the procurement initiator.

2.2.3.2 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 phase, the procurement 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 procurement. IT 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 determine what the government considers most important.

Developing an Evaluation Plan

When evaluating IT 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 IT security features are true and that the offeror can provide the proposed services. Because IT security, like other aspects of computer

[6] 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)].

systems, is a complex and important subject, the offeror's assertions may not provide sufficient assurance. If the proposed products 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 procurement documentation. Appendix B further discusses assurance and presents ideas on how the government can obtain it. In addition, Section 4.4, Security Documentation, provides descriptions of documentation that can be used for assurance in the evaluation phase, such as the offeror's strategy for security.

How assurances are provided may determine the government's ability to adequately assess them. Security personnel should be sure that they are asking for the information they really need. If, after award, the government determines that more assurance is required, the government may be liable for additional costs.

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 evaluation and acceptance to effectively manage the security review and testing of proposals and deliverables.

Items to Consider in the Evaluation Plan

The remainder of this section presents ideas to help develop the IT 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 IT security can conflict with those that provide ease of use. The government must make it clear how offerors should propose different configurations and present conflicting options and tradeoffs. However, care should be taken to keep proposal size manageable to facilitate review and to keep down proposal preparation costs.

Testing is one method of determining if the proposed system or product can meet the IT 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 upon cost, technical, and procurement 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. The proposed use of products that have been evaluated under NIAP or the CCRA may lessen the amount of security testing required for a particular proposal. However, CC evaluations are typically accomplished at the individual product level in an intended environment. Any deviation from the CC test environment will have to be addressed through additional evaluations or testing.

Computer system testing, especially performance testing, should be performed with the IT security features enabled.

The more the procurement 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 knowledge learned by reading proposals cannot be used to modify the evaluation plan. It is worth the time to research what kind of alternatives could be offered so an evaluation scheme that reflects the true priorities of the government can be developed.

2.2.3.3 Special Contract Requirements

Some elements in an RFP are IT 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 nondisclosure of automated information obtained during the course of the contract is one example.

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

2.2.4 Contract Performance

Contract performance is the fourth phase of the IT procurement life cycle. An individual with extensive IT security expertise should take part in contract monitoring (i.e., COTR). This expert should be available to review contract performance measurement documentation, inspect IT security deliverables, and evaluate contract modifications.

Inspection and Acceptance. Acceptance refers to the government’s decision to accept, and therefore, pay for a deliverable. The government should be careful when accepting deliverables. Testing by the government or an independent validation and verification (IV&V) contractor to determine that the system does meet specifications can be very useful. This effort should include testing 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 specifications in the contract. 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 as there are many factors beyond the control of the vendor.]

Performance Measurement and Monitoring. The government should plan to review contractor performance to ensure that security has not degraded and that changes in the environment and system that result in new threats and vulnerabilities are recognized and appropriate safeguards put in place. A security working group can be effective in monitoring security in more complex contracts that involve more than simply the purchase of hardware.

After award, the government’s requirements should not change. If they do, 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 procurements. As noted in Section 1, Introduction, new security controls that are retrofitted to a system are seldom as effective as controls designed into the system.

2.2.5 Disposal and Contract Closeout

The final phase in the procurement life cycle is disposal and contract closeout. IT security issues for disposal and contract closeout should have been addressed when developing the solicitation. When IT systems are transferred, obsolete, or no longer usable, it is important to ensure that government resources and assets are protected. Four basic steps during this phase include:

+ **Update Security Plan**. Usually there is no definitive end to a system life cycle. 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 have relevance and be useful in developing the security plan for the follow-on system.

+ **Archive Information**. When archiving 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.

+ **Sanitize Media**. Protection of IT 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 different 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 through open-ended laboratory techniques. Several commercially available software utilities are available that can clear and purge information from an information system so that it cannot be later reconstructed.

  Degaussing, overwriting, and media destruction are some of the methods to purge information. Degaussing is a process whereby the magnetic media is erased. Overwriting is a process whereby unclassified data is written to storage locations previously containing sensitive data. Media may be destroyed by:

  – Destruction at an approved metal destruction facility (e.g., smelting, disintegration, or pulverization)

  – Incineration

  – Application of an abrasive substance to a magnetic disk.

+ **Disposal of Hardware and Software** –Hardware and software can be sold, given away, or discarded. The disposition of software should comply with license or other agreements with the developer. There is rarely a need to destroy hardware, except for some storage media containing classified information that cannot be sanitized without destruction. In the situations where 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 information system security officer should be consulted prior to disposing of the system.

3. SPECIFICATIONS, CLAUSES, AND TASKS

This chapter provides specifications, tasks, and clauses that can be used in RFPs to acquire IT security features, procedures, and assurances.[7],[8] 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 off-the-shelf products, purchase of integrated systems, development of applications, and other computer-related services.

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 IT security
2. Control of Hardware and Software
3. Control of Information/Data
4. Documentation
5. Legal Issues
6. Contract Administration, End of Task, Closeout
7. IT security Training
8. Personnel Security
9. Physical Security
10. IT 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 draft NIST Special Publication 800-35, *Guide to Information Technology Security Services*.

[7] 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.”

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

3.1 General IT 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 IT security administration, management, or support, the delineation of responsibilities should be clear, with a government employee retaining ultimate IT security program responsibility. OMB Circular A-76, *Performance of Commercial Activities*, provides additional detail regarding what positions are inherently governmental and should or should not be outsourced.

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

The following can be used to show the relationship between organization ownership of IT 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 IT security program as defined by (insert organization handbook, directives, manuals, etc.).*

3.2 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)>. No public domain, shareware, or freeware software shall be installed unless 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>. All additional hardware and software proposed for use, including upgrades, must be approved in advance and in writing by the contracting officer or COTR.*
>
> *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).*

2. *The contractor shall provide an impact analysis for proposed hardware and software changes that includes an assessment of possible new security vulnerabilities (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 a system or 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 multiuser 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/installed with the following message appearing before logon:*
>
> *(or)*
>
> *Contractor multiuser 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 user of the network shall have no reasonable expectation of privacy in the network?
- In the case of a non-government 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[9] 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 issue is requiring that the contractor provide continuity of support and IT 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 on 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*

[9] NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, provides examples of pre-logon warning banners.

> *fire, flood, or terrorist activity <modify to include threats to the system>. The plan shall, at a minimum -*
>
> - *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 emergency 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 can 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.*

3.3 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[10].

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]).

[10] 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 his/her 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 in order for 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 (or COTR). I agree that, whether or not a contract is awarded to me, I will keep all information in confidence.*

The following item is to prevent nondisclosable information from leaving the organization's control through such means as being stored on a hard drive 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.*

3.4 Security Documentation

Security documentation provides instruction 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, showing 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 what is being acquired. For instance, an approach, abstract, or outline of a Security Feature 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. Additionally, 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. Additionally, component Security Targets for CC evaluated products can serve as essential documentation for evaluated IT security components.

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

3.4.1 Proposal Documentation

3.4.1.1 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 will meet the security needs of the government. Offerors of off-the-shelf products should match the features of the packages to government specifications and address assurance. For complex system development efforts, this could 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.*
>
> *This plan will be included in any resulting contract for contractor compliance.*
>
> *Note: In system acquisitions where 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.*

3.4.1.2 Offeror's Internal Security Policy and Plan

Procurements 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.

3.4.2 Deliverable Documentation

3.4.2.1 Security Feature User's Guide

This guide is a description of the protection mechanisms provided by the system, guidelines on their use, and explanation of their interaction with one another. If a system is being procured, be sure to get both system-level documentation and product documentation.

3.4.2.2 System Administrator/Facility Manual

This manual, which is addressed to the system administrator, presents information about functions and privileges that should be controlled when running the system or facility in a secure manner. The procedures for examining and maintaining security features requested (such as audit record structures) should also be requested. The manual should describe the operator and administrator functions related to security, including changing the security characteristics of a user. It should provide guidelines regarding the consistent and effective use of the protection features of the system. It also should explain how they interact, and include warnings and privileges that need to be controlled in order to operate the system or facility in a secure manner. If a system is being procured, be sure to obtain system-level documentation and product documentation.

3.4.2.3 Test Documentation

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

3.4.2.4 Design Documentation

This documentation is a report that describes the manufacturer's or developer'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.

3.5 Legal Issues

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

+ **Security Violations** – It is possible for computer products to cause security violations, even if the products are functioning correctly. These violations could be caused by a product containing malicious code (i.e., virus or Trojan horse), bypassing operating system controls, or containing undocumented backdoors that bypass security. 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 IT 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.

  Agencies may wish to consider the use of warranties, liquidated damages, and other clauses in establishing the contractor's IT 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 IT security area is to provide incentive for the contractor 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.*

____

____

____

____

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

3.6 Contract Performance and Closeout

For complex contracts that include the development, implementation, or operation of a computer facility or application, a security control/review group can be used effectively to help maintain IT 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.

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 IT 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 for 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 no output will be retained by the contractor 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 IT security considerations include the return of the GFE in usable condition. This is especially important if a system will continue to operate under the government's or another contractor's control. The IT 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 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).*

3.7 IT Security Training and Awareness

An important goal of the Computer Security Act is to have all personnel involved in the management, use, and operation of federal systems trained in IT security awareness and accepted IT security practices. OMB Circular A-130, Appendix III, specifically requires federal agencies to provide for the mandatory periodic training in IT security awareness and accepted IT 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 draft NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" adequately addresses the security training requirement for the contractor. This can be tailored to include specific additional skills, training levels, or audience categories depending on the requirements of the organization. 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 draft NIST Special Publication 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 draft NIST Special Publication 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)*

3.8 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 that are required to perform each position. Personnel screening includes a range of implementations 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:

+ Review of employment forms completed by the contractor employee
+ Personal reference check
+ Credit check
+ Verification of employment for the last 2 years before current employment
+ Verification of education (high school or beyond) within the last 5 years that resulted in the awarding of a degree
+ Local police check in present county and state
+ Background check by private organization
+ National Agency Check with Local Agency Check and Credit Check (NACLC)
+ Single-Scope Background Investigation (SSBI) that includes verification of all previous places of employment.

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*
- *Failure to log off.*

In addition to background screenings, personnel security methods such as employee statements regarding conflict of interest may be used. Conflict of interest can include procurement 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 IT 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 in 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.

3.9 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.*

IT security should 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.*

3.10 IT Security Features in Systems

IT security features in systems refer to specific functions that can be incorporated into or those integral to the IT system. How security features are utilized 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 a procurement. This list is not exhaustive as 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 Special Publication 800-27 *Engineering Principles for Information Technology Security (A Baseline For Achieving Security June 2001).*

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 such as record or field controls and edit checks 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 procurement is to acquire off-the-shelf products, market surveys should be performed (in accordance with organization policy) to determine what features are currently available on 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 forthcoming draft NIST Special Publication 800-36, *Guide to Selecting Information Technology Security Products*.

Additional information on 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 IT security publications that provide additional information on some of these security features. Technical terms and concepts used in this section are explained in the glossary, Appendix B.

The term “system” is used loosely to mean any collection of components, hardware, software, firmware, and processes, etc. 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.

The controls described in this section are consistent with those specified in GAO Federal Information System Controls Audit Manual (FISCAM), Volume I, Financial Statement Audits, June 2001.

3.10.1 Identification and Authentication

Identification and authentication 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 user of the system. 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 risk. 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 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 (based on a number of incorrect password attempts).*

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. Authentication mechanisms 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 Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication* provides additional detail on the use of public key technology for advanced authentication.

3.10.2 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 belong to multiple roles, which provide the 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 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 both DAC and MAC types of enforcement should be based on a defined organization access control policy.

Organizations can help to 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, 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 by only 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.

3.10.3 Auditing

Auditing provides protection by enabling organizations to record meaningful actions within the system and to hold the user held 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 of the keys 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 prior to 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).

3.10.4 Cryptography

The NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal* Government provides a comprehensive reference for government use of cryptography. The purpose of this document is to provide guidance to Federal agencies on how to select cryptographic controls for protecting Sensitive Unclassified information. This Special Publication 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 exist four FIPS-approved symmetric algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, and Skipjack. The following FIPS describe or reference these four encryption algorithms:

+	AES	FIPS 197
+	DES[11]	FIPS 46-3
+	Triple DES	FIPS 46-3
+	Escrowed Encryption Standard	FIPS 185

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 3.10.4.5 below for further information on validations.

> *The cryptographic module and algorithm shall be validated by a Cryptographic Module Testing laboratory.*

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

[11] 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.

3.10.4.1 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 Message Authentication Code (MAC). The purpose of a Message Authentication Code (MAC) is to authenticate 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 HMACs. FIPS are available that describe the two MACs:

+	FIPS 113[12]	Computer Data Authentication (describes the MAC)
+	FIPS 198	HMAC - 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 Special Publication 800-38, Recommendation for Block Cipher Modes of Operation. These modes, when available, 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 and if they are equal then the information has not been altered.

3.10.4.2 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 IT 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 also verifies that information has not 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 document was signed by the owner of the public key 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 non-repudiation. 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), 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 CMT laboratories.

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

> *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.*

3.10.4.3 Key Management

Key management is extremely important because the security of any cryptographic system is dependent on the security provided to the cryptographic keys. In order 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 procurement 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.

3.10.4.4 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 changes in applicable standards and technology since the development of FIPS 140-1 as well as 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 procurement 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>.*

3.10.4.5 Cryptographic Validations

NIST currently provides cryptographic validation services through CMVP for FIPS 140-2, FIPS 197, FIPS 46-3, FIPS 81, FIPS 186-2, FIPS 180-1, and FIPS 185. The CMVP was established by NIST and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

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

After encryptions algorithms and modules are validated, NIST issues a validation certificate and adds the products to a 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 other standards and guidelines that relate to cryptography. A list of NIST security-related publications is available at http://crsc.nist.gov.

3.10.5 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 generally are not appropriate to verify the correctness of the software implementation. Depending upon 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.

3.10.6 System Architecture

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

> *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: The word "domain" refers to the protection environment in which a process is executing. Domain is sometimes also referred to as "context" or "address space."]

The procuring organization should be aware that over specifying the architecture for a system can preclude integrators from incorporating otherwise valid existing products. Over specifying can also eliminate lower cost alternatives, resulting in a more costly procurement. 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.

3.10.7 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. There are several accepted methods for sanitizing media: overwriting, degaussing, and destruction. Media sanitizing typically occurs in the closeout phase of procurement and is further addressed in section 3.6.

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 Procurement 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.	Procurement Contains standard RFP information.
B. Supplies or Services and Prices/Costs	List of Products/Services To Be Provided by Offeror	Procurement 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.	Procurement and Technical. Describes product/services to be produced.
D. Packaging and Marking	Shipping, Handling, and Storage Requirements. May Not Be Required for Service Contracts.	Procurement 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	Procurement 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 Down Time, Credits, Product Replacement, Variation in Quantity, Delivery and Installation Schedule, and Stop Work Orders.	Procurement 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, Financial Information	Procurement 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.	Procurement 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.	Procurement. Contains standard RFP information.
J. List of Attachments	Any Additional Procurement and Technical Information for Offeror.	Procurement 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.	Procurement. Standard RFP information.

RFP Section	Contents	Created By Technical and/or Procurement 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 Evaluation. Requires offerors to tell how they will/can meet the requirements described in Section C.	Procurement 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.	Procurement and Technical.

For further information, see FAR 15.406.

Appendix B—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 or not a facility or system meets the specified technical and performance standards.

Access control

Restrictions on the types of interactions between subjects (e.g., persons) and objects (e.g., files or data elements). Access can be further defined by types of access, such as read, write, modify, or execute. (Access control also includes physical access control.)

Access control label

A piece of information that represents the security level or sensitivity designation of data in an object or the access authorization of a subject.

Accreditation

Accreditation: the authorization and approval, granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets prespecified technical requirements for achieving adequate system security. (FIPS PUB 102, as updated by SP 800-26). See Certification (security).

Acquisition

Acquiring by contract with appropriated funds supplies or services by and for the use of the federal government through purchase or lease, whether the supplies or services are already in existence, or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when organization needs are established and includes the description of requirements to satisfy organization needs, solicitation and selection of sources, award of contract, contract financing, contract performance, contract administration and those technical and management function directly related to the process of fulfilling organization needs by contract. See Procurement.

Advanced Encryption Standard (AES)

A NIST-approved (FIPS 197) cryptographic algorithm that can be used to protect sensitive electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Assurance

A measure of confidence that the security features and architecture of an information technology (IT) system will meet the security requirements.

Authenticate

The process in which a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action.

Availability

The requirement for a system to be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used for only intended purposes.

Benchmark

A test of the capabilities of a proposed system using customized workloads.

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.

Certification (procurement)

A signed statement by an offeror.

Certification (security)

The technical evaluation that establishes the extent to which a computer system, application or network design and implementation meets a pre-specified set of security requirements. (FIPS PUB 102, as updated by SP 800-26). See Accreditation , System Security Evaluation.

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 too as off-the-shelf.

Common Criteria for Information Technology Security Evaluation

The three-part ISO/IEC international standard (IS 15408:1999) that describes security functional requirements, security assurance requirements, two constructs for expressing them (a Protection Profile and Security Target), and a model for determining them.

Common Criteria Testing Laboratory (CCTL)

Laboratory that has been accredited by the NIST National Voluntary Laboratory Accreditation Program and the National Information Assurance Partnership's Validation Body to conduct evaluations of IT security-capable products for conformance to the Common Criteria. See NIAP and NVLAP.

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.

Computer Security Act of 1987

A statute to provide for a computer standards program within the National Institute of Standards and Technology, to provide for government-wide IT security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems.

Confidentiality

The requirement for information to be protected from unauthorized disclosure.

Contingency planning

Plans to assure that users can continue to perform essential functions and that a reasonable continuity of data processing support is provided at all times. These plans can include emergency response, backup operation, and post-disaster recovery.

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 (CO)

A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

Contracting Officer's Technical Representative (COTR)

An individual to whom the Contracting Officer delegates certain contract responsibilities, usually related to technical direction and acceptance issues.

Deliverable

A product or service that is prepared for and delivered to the government under the terms of a contract.

Data Encryption Standard (DES)

An older cryptographic algorithm for protection of sensitive data, specified by FIPS PUB 46-3. Note: NIST no longer recommends that single DES be used. See Advanced Encryption Standard (AES).

Directed specification

A specification that must be included in statements of work based on federal law, policy, or regulation.

Discretionary access control (DAC)

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. See Access Control and Mandatory Access Control.

Domain

The unique context in which a program is operating.

Encryption

The use of cryptographic methods to transform intelligible data, called plaintext, into unintelligible form, called ciphertext.

Evaluation Assurance Level

A point on a scale defined in but not mandated by the Common Criteria for evaluating the assurance of Targets of Evaluation.

Features

Specifically, technical security features. The security-relevant functions, mechanisms, and characteristics of system hardware, firmware, and software. Technical security features are a subset of system security safeguards.

Federal Acquisition Regulation (FAR)

The regulation that codifies uniform acquisition policies and procedures for Executive agencies.

Federal Information Processing (FIP)

Refers to the resources and services used to process automated information, including telecommunications.

FIPS PUB

An acronym for Federal Information Processing Standards Publication. FIPS PUBs are issued by NIST after approval by the Secretary of Commerce. Some FIPS PUBs are mandatory for use in federal procurements.

Flowdown

The extension of prime contractor requirements to subcontractors.

Full and open competition

The consideration of all responsible sources in a procurement, as required by the Competition in Contracting Act.

GSBCA

General Services Board of Contract Appeals.

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.

Information Technology (IT) Security

The protection of automated data processing assets from harm. This includes the protection of data, hardware, firmware, and software. Harm is typically defined as a loss of integrity, availability, or confidentiality.

IV&V

Independent Verification and Validation.

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 can include one or more benchmark tests.

MAC

Message authentication code or mandatory access control.

Mandatory access control

A means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity. In a mandatory access control environment, users cannot pass their access rights to others without express concurrence of the access control authority. See Access Control and Discretionary Access Control.

Mandatory requirements

Those contractual conditions and technical specifications that are established by the government as being essential to meeting required needs.

Mechanism

Specifically, security mechanism. See Safeguard.

Multilabel

Having information with different sensitivities on one system. A multi-label secure system permits simultaneous access by users not authorized by the mandatory access authority to access all of the data and prevents unauthorized access. No hierarchy of sensitivity of information is implied by the term. See Multilevel.

Multilevel

Having information with various sensitivities on one system. A multilevel secure system permits simultaneous access by users not authorized by the mandatory access authority to access all of the data and prevents unauthorized access. This term is normally used to describe systems with hierarchical information sensitivities and situations in which the system is relied on to enforce a mandatory security policy. See Multilabel.

Needs determination

An assessment, performed as part of initial system planning, which looks at the needs of an organization that might be met through automation.

National Voluntary Laboratory Accreditation Program (NVLAP)

The U.S. accreditation authority for testing laboratories of all types. NVLAP accredits commercial IT security evaluation facilities operating in accordance with the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme. See Common Criteria Testing Laboratory (CCTL).

Object

A passive entity that contains or receives information. Access to an object implies access to the information it contains. Examples of objects are records, blocks, files, programs, video displays, printers, and network nodes.

Object reuse

The potential recovery and use of residual (e.g., deleted) data from a system resource such as a disk drive. Such data must be unrecoverably removed before reassignment and reuse of the resource.

Offeror

Any entity that responds to an RFP with a proposal. See Bidder.

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.

Procedure

Specifically, security procedure. A type of safeguard based on human actions (as opposed to technical features). These can be referred to as administrative safeguards.

Procurement

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.

Procurement initiator	The key person who represents the program office in formulating information resources requirements and managing presolicitation activities. Also called Program Manager or Sponsor. This person often becomes the COTR.
Procurement technical evaluation	The examination of proposals to determine technical acceptability and merit. This is part of the source selection process.
Product	A package of IT software, firmware, and/or hardware providing functionality designed for use or incorporation within a multiplicity of systems.
Product security evaluation	The examination of the security features of a product against a stated set of requirements or criteria , typically IS 15408, the Common Criteria. Product evaluations are typically performed in the setting of an accredited testing laboratory. See Common Criteria Testing Laboratory (CCTL).
Program manager	See Procurement Initiator.
Protection Profile	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs, defined by IS 15408-1, Common Criteria (CC) Part 1, and typically using security functional and assurance requirement sets from CC Parts 2 and 3.
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 Proposals (RFP)	A solicitation document used in negotiated acquisitions to communicate government requirements and to solicit proposals.
Request for Quotation (RFQ)	A solicitation document used in negotiated acquisitions to communicate government requirements and to solicit quotations.
Requirements analysis	A part of the acquisition cycle in which the requirements for a system are developed.
Responsible prospective contractor	To be responsible, a prospective contractor must meet the requirements of FAR 9.104-1, which include the ability to be able to perform the contract based on the financial, technical, organizational, ethical, and legal position of the contractor.

Responsive prospective contractor

To be responsive, a prospective contractor must comply in all material respects with the solicitation.

Restrictive specification

A detailed and precise description of an item(s) being acquired that needlessly limits competition (e.g., brand name without the words or equal).

Risk assessment

The process of examining assets, threats, and vulnerabilities in order to determine cost-effective security controls.

Role-based Access Control (RBAC)

A method for controlling access to system objects based on privileges defined in terms of the various roles exercised by users.

Safeguard

Any action, device, feature, mechanism, procedure, technique, or other measure that reduces the vulnerability of or threat to a system. Also called Controls or Countermeasures.

System security evaluation

The examination of the technical and non-technical security features of a computer system and other safeguards that establishes the extent to which a particular design and implementation meet a specified set of security requirements. See also Product Security Evaluation.

Security label

A piece of information that tells a system how to handle data. The label can be used to control access, specify protective measures, or indicate handling restrictions required by a security policy.

Security Target

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE (e.g., security-capable product), defined by IS 15408-1, Common Criteria (CC) Part 1, and typically using security functional and assurance requirement sets from CC Parts 2 and 3. See Protection Profile.

Sensitive information

Any information in which the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitivity assessment

An initial assessment of the general sensitivity of an organization function.

Single-label

A subset of a multilabel system in which only one type of labeled information is processed at a time.

Solicitation

An official government request for bids/proposals often publicized in the *Commerce Business Daily*.

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 services to be acquired.

Sponsor

See Procurement Initiator.

Statement of work

A statement of the technical specification in the RFP that describes the work or system required by the government.

Subject

An active entity, (usually a person, process, or device) that causes actions such as the flow of information.

Target of Evaluation (TOE)

An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. See Protection Profile and Security Target.

Threat

Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

Unauthorized access

Access to IT resources and services that unqualified users are not entitled to access.

Validated Products List

A publicly available document issued periodically by the NIAP Validation Body briefly describing:

1) every product that holds a currently valid validation certificate awarded by NIAP, and
2) every product validated or certified under the authority of another party for which the validation certificate has been recognized.

Vulnerability

Any weakness in a computer system, for example, in system security procedures, system design, implementation, internal controls, and physical environment.

Warner Amendment
10 USCA 2315.

Excludes certain systems from the requirements of Section 111 of the Federal Property and Administrative Services Act of 1949 (40 USC 795), including ADP equipment or services if the function, operation, or use of the equipment of services involves intelligence activities, involves cryptographic activities related to national security, involves the command and control of military forces, involves equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions except for equipment or services to be used for routine administrative and business application (including payroll, finance, logistics, and personnel management applications).

Appendix C—References

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

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

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

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

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

NSTISSP No. 11, January 2000, *National Information Assurance Acquisition Policy*, http://www.nstissc.gov/Assets/pdf/nstissp11.pdf

A Guide to Planning, Acquiring, and Managing Information Technology Systems, Version 1, General Services Administration, December 1998.

Public Law 100-235, *Computer Security Act of 1987*, Public Law 100-235.

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

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

OMB Circular A-76, *Performance of Commercial Activities*, 1999.

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/searchmanual.htm*, January 2001.

Appendix D—Frequently Asked Questions

1. **For whom is the guide intended?**
   NIST Special Publication 800-4, *Security Considerations in Federal Information Technology Procurements*, is intended for the use of procurement initiators (e.g., the end user, program manager, or contracting officer's technical representative [COTR]), contracting officers, and IT security officials.

2. **Why was this guide written?**
   Organizations must consider IT security in all phases of information resources management, including the acquisition phase (Federal agencies must do this to meet the requirements of OMB Circular A-130 and the Federal Acquisition Regulation [FAR]). The purpose of this guide is to present a framework for incorporating security into all phases of the acquisition process, from early planning to contract closeout and/or system disposal. Including IT security early in the acquisition process for an IT 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 IT security considerations factor into the procurement process?**

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

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

   The procurement life cycle has five phases

   + Mission and Business Planning
   + Acquisition planning
   + Acquisition
   + Contract Performance
   + Disposal and Contract Closeout

5. **Who are the key participants in the procurement life cycle of IT systems?**

   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, contracting officer's technical representative, IT investment board, IT security program manager, IT system security officer, program manager/procurement initiator, and privacy officer, among others.

6. **What is a sensitivity assessment?**
   A sensitivity assessment results in a brief qualitative description of the basic security needs of the system. In practice, the need for IT 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, non-repudiation). Developing a preliminary sensitivity assessment is the first IT security step in the first phase of the procurement lifecycle. The sensitivity assessment is then updated during the acquisition planning phase.

7. **What IT security steps are involved in the requirements analysis process?**

   The following IT security steps should be included in a requirements analysis:

   - Analysis of integrity, availability, and confidentiality requirements
   - Update sensitivity assessment
   - Analysis of the level of assurance required
   - Risk assessment
   - Review by other functional groups
   - Review by certifier and accreditor

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

   The process of identifying integrity, availability, and confidentiality requirements should include an analysis of laws and regulations such as the Privacy Act, Federal Manager's Financial Integrity Act, Computer Security Act, 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.

9. **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, among others, conformance testing and validation suites, Common Criteria, evaluations by government agencies, evaluations by independent organizations, evaluations by another vendor, and evaluations by another government.

10. **How does a risk assessment fit into the procurement process?**

    A risk assessment during the acquisition planning 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.

11. **Who should review the system procurement?**

    Functional groups, certifier, and accreditor should review the system procurement. Functional groups could consist of participants culled from the categories of key roles described in question 5. Even for small systems, it is helpful to get the assistance of the IT security staff. The functional groups should have insight into integrity, availability, confidentiality and assurance requirements.

    OMB Circular A-130 requires systems be approved for processing based on the validation of the safeguards. This approval comes from an accreditor. In the procurement review process, the accreditor can advise the acquisition team if the potential risk appears to be unacceptable. The accreditor should also discuss what forms of assurance is needed and how changes to the system will be addressed.

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

As part of the acquisition phase, the procurement 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 procurement. IT 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 IT security features are true and that the offeror can provide the proposed services.

13. What is inspection and acceptance?

Acceptance refers to the government's decision to 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.

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

After award, the change to government's requirements should be minimal. If they do, 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 procurements and new security controls that are retrofitted to a system are seldom as effective as controls designed into the system.

15. What IT security steps occur during the disposal and contract closeout phase?

There are four IT security steps in the final phase of the procurement lifecycle:

+ Update security plan

+ Archive information

+ Sanitize media

+ Dispose of hardware and software.