Effectively Integrating Information Technology (IT) Security into the Acquisition Process

TABLE OF CONTENTS

Section 1: Getting Started

Purpose

This course is designed to familiarize you with the IT security requirements that must be considered during the acquisition process.

Objectives

After successful completion of this course you will be able to:

- Recognize the legal and practical reasons for considering IT security during the acquisition process
- Identify specific security considerations in each phase of the acquisition life cycle
- Integrate IT security language into procurement documents
- Ensure that contractors comply with DOC and/or Bureau security standards and other industry security practices

Definition of IT Security

IT security is about protecting information assets by effectively managing risks. How much protection depends on the risk and magnitude of harm that could result if the data were lost, misused, disclosed, or modified. To view DOC's IT Security Program Policy click here[1]

IT Resources

IT resources are: computers, networks, telecommunications systems, applications, information, data and any associated service.

Vulnerabilities and Threats	Risks are managed by evaluating: • Vulnerabilities • Threats
Definition of Vulnerabilities	Vulnerabilities are weaknesses in a system, software, application that could be exploited to compromise security processes or a control that protect the system and the information it stores, processes, or transmits.
Definition of Threats	Threats are catalysts of impending danger or harm. They are perceived as potential dangers and are events or circumstances, whether internal or external, that has the potential to cause harm to a system or to its associated applications or information.
External Threats	External parties may attempt to access IT systems without authorization and cause harm to theft of systems or information.
Examples of External Threats	Examples of external threats include: • hackers • crackers • thieves
Internal Threats	Internal parties may intentionally or unintentionally alter, disclose, lose, or destroy information or system processing capabilities.
Examples of Internal Threats	Examples of internal threats include: • disgruntled authorized users • careless authorized users • internal unauthorized users
Natural Disasters	Natural disasters (storms, floods, fire, etc.) that may cause physical harm or unavailability of IT resources are also classified as internal threats

Section 1: Getting Started, Continued

Components	The IT Security Program includes: • a set of policies • guidance for ensuring the protection of IT resources from harm. **Note:** To view DOC's IT Security Program click here[2]
Policy Safeguard Measures	DOC's IT security policy helps minimize vulnerabilities and ward off threats. • This policy provides guidance on the implementation of security controls within DOC. Without the appropriate safeguards and security control measures in place, DOC IT systems could be vulnerable to threats and harm resulting from misused, lost or stolen data. • The policy is reviewed annually by the IT Security Program Manager
Harm	Harm is the loss of integrity, availability, or confidentiality of DOC's IT resources.
Integrity	Integrity is the ability to ensure that information and software are protected from error or unauthorized modification.
Availability	Availability is the ability to ensure that resources are accessible when and where needed
Confidentiality	Confidentiality is the ability to ensure that information is disclosed only to those who have a valid need to possess it.

Section 2: The Framework

Laws

The following laws provide the framework for establishing Departmental security programs for the protection of federal information systems.

- Competition in Contracting Act of 1984-CICA
- Federal Information Security Management Act of 2002 (FISMA)
- Government Paperwork Elimination Act-GPEA

Competition in Contracting Act of 1984 CICA

CICA is a public law enacted by Congress for the purpose of increasing the number of Federal Government procurements conducted under the principles of full and fair competition, as apposed to contracts that are issued under noncompetitive arrangements such as "sole source" or "set aside" awards.

Federal Information Security Management Act of 2002 FISMA

Requires Federal Agencies to implement a comprehensive IT security program and monitor the security of all information systems. From an enforcement perspective, the law requires every agency to provide a risk assessment determination and report of the security needs of its systems. These reports must be included in every agency budget request. For more information on a risk assessment determination 1, consult section 3.1 of the DOC IT Security Program Policy.

FISMA enforces accountability and requires each agency to examine the adequacy and effectiveness of information security policies, procedures and practices in plans and reports. It directs agencies to report findings of significant deficiencies in policies, procedures and practices.

Government Paperwork Elimination Act-GPEA

GPEA requires Federal agencies to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives.

GPEA Acts

There are four acts belonging to GPEA:

- Clinger-Cohen Act of 1996
- Paperwork Reduction Act of 1995
- Privacy Act of 1974

Clinger-Cohen Act of 1996

The Clinger-Cohen Act of 1996 is also known as the IT Management Reform Act (ITMRA), requires agencies to appoint Chief Information Officers and to use business process reengineering and performance measures to ensure effective IT procurement and implementation.

Paperwork Reduction Act of 1995

The Paperwork Reduction Act of 1995 requires federal agencies to be accountable for reducing the burden of federal paperwork requirements. The goals of the Act are to:

- Minimize paperwork burden imposed on the American public
- Ensure maximum utility and quality of federal information
- Ensure the use of information technology to improve Government performance
- Improve the federal government's accountability for managing information collection activities.

Privacy Act of 1974

The Privacy Act establishes provisions to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invitations of personal information about them. The law:

- Restricts disclosure of personally identifiable records maintained by agencies
- Gives individuals the right to obtain information held on them by the Federal government
- Allows individuals the right to seek amendments of agency records maintained on them if the records are NOT accurate, relevant, timely, or complete.
- Levies civil and criminal penalties for violation of the provisions of the Act.

Section 2: The Framework

Regulations

The following regulations specify detailed procedures to ensure uniform implementation of IT security laws within DOC.

Federal Acquisition Regulation (FAR)

Federal Acquisition Regulation (FAR)
The FAR is a federal regulation that is established for the codification and publication of uniform acquisition policies and procedures to be implemented by all executive agencies.

Commerce Acquisition Regulation (CAR)

Commerce Acquisition Regulation (CAR)
The CAR is a federal regulation that is established by the Department of Commerce to implement and supplement the FAR within the Department of Commerce. The CAR is intended to supplement and implement the FAR without paraphrasing or duplicating FAR language. The CAR should be read in conjunction with the FAR.

Policies

The following policies provide guidance to Agencies to help to ensure that proper security controls are considered when establishing IT security programs.

OMB Circular A-130, Appendix III
Establishes a minimum set of controls that agencies must include in IT security programs; assigns agency responsibilities for the security of IT; and links agency IT security programs to agency management controls that define the roles and responsibilities of individuals acquiring, using, and managing IT systems.

Also requires that a single individual be assigned operational responsibility for IT security. The individual must be knowledgeable about the IT resources used and how to secure them. For major applications, the assigned individual must be able to give special management attention to the security of the application.

Section 3: Major Players: Key Roles

Introduction	Major players in the process of integrating IT security into the acquisition process and their key roles are addressed in this section.
Chief Information Officer (CIO)	The CIO is the department or bureau level senior official designated for ensuring that the organization's programs make full and appropriate use of information technology enabling the Department to carry out its mission better, with improved products and services at the lowest cost. High priority is given to IT Security, so as to ensure the integrity of the department's systems and data and products and services based on these data and to ensure continuity of operations.
Contracting Officer (CO)	The CO is a federal procurement official that possesses a formal written certificate of appointment from the Head of Contracting Activity, or designee, that authorizes him/her to contractually obligate the Federal Government as set forth in the FAR Subpart 1.6.
Contracting Officer Representative (COR)	The COR as defined by CAM Chapter 1301.67, COR Certification Program, a COR is a Federal Government employee that has been formally appointed by a CO, in writing, to serve as the CO's technical representative on a designated contract or order subject to the limitations set forth in their appointment letter. The COR plays a key role in ensuring that security requirements are identified during the post-award phases of the acquisition process. The COR ensures security requirements are addressed throughout design reviews, tested during implementation and operational phases, and maintained during the disposal process.
Division/ Bureau IT Security Program Manager or IT Security Officer	The Division/Bureau IT Security Program Manager or IT Security Officer is responsible for maintaining a division or bureau's IT security risks to the organization. IT security program managers and IT Security Officers track operating unit weaknesses reported under self-assessments and external reviews and track implementation of corrective actions; and identify resource requirements, including funds, personnel, and contractors, needed to manage the IT security program. 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 and IT security officers track e-bureau IT security programs.

Continued on next page

Section 3: Major Players: Key Roles, Continued

DOC IT Security Program Manager	The IT Security Program Manager is a solitary and specific role defined by FISMA section 301, subsection 3544. No other office in the department fills this role.
Information Technology Review Board (ITRB)	The ITRB reviews and evaluates the Department's information technology capital investments ensuring that proposed investments contribute to the Department's strategic vision and mission requirements, employ sound IT investment methodologies, comply with Departmental systems architectures, and provide the highest return on the investment or acceptable project risk. The ITRB reviews system security plans, expenditures for security requirements, as well as security risks.
Procurement Initiator	The term Procurement Initiator is synonymous with the term Requisitioner. A Procurement Initiator is a Federal Government employee that represents programmatic interests during the pre-award phase of the acquisition process and is responsible for initiating a requisition for a particular procurement need for products and/or services. The Procurement Initiator is involved in strategic planning initiatives of the procurement, plays an essential role in security and is intimately aware of functional system requirements. The Procurement Initiator is generally appointed the COTR after contract award.
Privacy Officer	The privacy officer is responsible for ensuring that services or systems being procured complies with existing privacy **laws and** policies regarding protection, **maintenance**, dissemination (information sharing/exchange) and disclosure of information.

Continued on next page

Section 3: Major Players: Key Roles, Continued

Program Manager	The person who manages a group of related activities performed within a definable time period to meet a specific set of objectives whose value is independent. The related activities involve a series of undertakings, i.e. contract actions, that continue over a period of time (normally years), which are designed to pursue or are in support of a focused scientific, business, technical, or statutory or regulatory goal, and which are characterized by: design, development and operations of systems; relatively high funding levels; firm schedules; and firm scientific, business, technical, or statutory or regulatory objectives. The program manager is usually the system owner and may be the procurement initiator.
Technical Evaluation Team	The team assembled by the Procurement Initiator, responsible for reviewing, analyzing, rating and ranking offers or quotes in response to a request for offers or quotations.

Section 4: Effective Integration: Procurement and System Life Cycles

Phases of the procurement cycle.

The following five phases of the procurement life cycle must address IT security requirements:

- PHASE 1: Mission/Business Planning – The process through which an organization determines its needs and how those needs can be met through the acquisition process.

- PHASE 2: Acquisition Planning -The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition.

- PHASE 3: Acquisition- The process of acquiring by contract of supplies or services for the use of the Federal Government. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contract(s).

- PHASE 4: Contract Performance -The period where a contractor supplies goods and/or services conforming to the specifications of the solicitation and award. During this phase the Government exercises oversight in order to ensure that the Government receives the quality of products and services specified in the contract within established costs and schedules.

- PHASE 5: Contract Closeout - Includes all final contract activities for ensuring completion of all requirements and making final payment.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

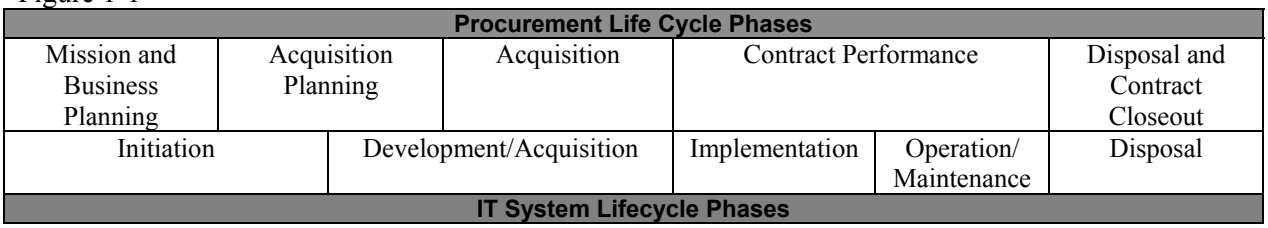
Figure 1-1 Life Cycles

The following figure 1-1 portrays how the two life cycles relate. All 5 phases in the procurement life cycle must address IT security requirements:

- Mission/Business Planning
- Acquisition Planning
- Acquisition
- Contract Performance

Contract Closeout

Figure 1-1



Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Overview

The actions outlined in the table describe analyses and processes to be performed by the major players in the process of security integration in the acquisition life cycle. The steps define a framework for security planning during the process. The framework should be used as an example, not as a definitive methodology.

Figure 1-2 Life Cycles and Security

Figure 1-2 describes the security considerations that must be addressed during each phase of the procurement life cycle. The table also highlights tasks to be accomplished during each phase of the procurement and system life cycles.

Figure 1-2

	Mission and Business Planning	Acquisition Planning	Acquisition	Contract Performance	Disposal and Contract Closeout
PROCUREMENT CYCLE	• The perception of a Need emerges • Program office and procurement initiator partner with the Contracting Office to development a *Needs Determination*, which includes: - System Idea - Preliminary Requirements Definition; and - Approval • Linkage of the Need to Mission and Performance Objectives Occurs during this Phase • Assessment of Alternatives to Capital Assets is conducted	• Program office and procurement initiator partner with the Contracting Office to: - Develop a *Functional Statement of Need* - Perform *Market Research* - Conduct a Feasibility Study - Performance a Requirements Analysis - Develop an Independent Government Cost Estimate; and - Funding is secured • ITRB Review is completed • Contracting Office prepares an Acquisition Plan	• Statement of Work (SOW) (Including Quality Assurance Plan) is Developed • Offer or Quotation Evaluation Plan is Developed including: - Non Disclosure/ Confidentiality Agreements • Internal contracting office review of Solicitation is performed • Request for Offers or Quotations is released to prospective offerors • Source Selection is performed • Contract is Awarded	• Contractor Performance is measured • Inspection and acceptance occurs • Contract Modifications are considered and/or issued • Performance Failures addressed	• Appropriateness of disposal procedures are addressed • Exchange and sale considered • Internal organization screening conducted • Transfer and donation considered • Contract Closeout activities completed

	Mission and Business Planning	Acquisition Planning	Acquisition	Contract Performance	Disposal and Contract Closeout
SECURITY CONSIDERATIONS	• Preliminary Sensitivity Assessment is developed • Interconnectivity Requirements are Considered	• Integrity, Availability, and Confidentiality Analysis is conducted • Sensitivity Assessment is Updated • Level of Assurance Analysis is conducted • Risk Assessment is performed • For IT systems or major applications, development of the security plans as required by FISMA • Other Functional Groups Review Conducted • Certifier and Accredit or Review Conducted • Cyclical Nature of the Process – Because the steps in this phase interrelate and build on each other the security steps in this may need to be addressed cyclically.	• Security Specification are included as the SOW is being developed • Assignment of Contract Security Risk or Sensitivity Level is done • Personnel Security Requirements and Background Checks are planned • Offer or Quotation Evaluation of security requirements • Special Security Related Contract Requirements are Developed • Security Plan is Updated • Risk Assessment is Updated	• Inspection and acceptance occurs based on security tests • Performance Measurement and Monitoring occurs • Review of security at contactor facility conducted • Reviews of contractor compliance with IT contract and IT security requirements are completed • Risk Assessment is Updated	• Security Plan is Updated • Information Archival is performed • Media Sanitization is performed • Hardware and Software Disposal occurs • Risk Assessment is Updated • Security clearance debriefing and nondisclosure agreement briefing conducted

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 1: Mission and Business Planning

Introduction	Mission/Business Planning results in a needs determination.
Stages of the Need Assessment	The stages of the need assessment are: • A basic system idea • Preliminary requirements definition, and • Approval
Needs Determination	Needs determination defines the problem to be resolved through the procurement process. The needs determination is an initial definition of a problem that could be solved through automation. The needs determination is very high-level in terms of functionality. No system specifics are defined in this phase. The idea for a new or substantially upgraded system and the feasibility of the idea and alternatives are explored.
Stages of the Preliminary System Security Plan	The stages of the preliminary system security plan are: • Establish the need • Link the need to performance objectives • Address alternatives • Address interconnectivity
Preliminary System Security Plan	The needs determination for IT systems and applications should result in a preliminary system security plan compliant with NIST Special Publication 800-18. To view this document click here[3].

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles, Continued Continued

Phase 1: Mission and Business Planning

Procurement Initiator

The procurement initiator should:

- Conduct a preliminary sensitivity assessment in accordance with Federal Information Processing Standard 199.

Obtain a unique system identifier number by contacting the bureau's Office of the Chief Information Office (OCIO), which is used by the OCIO to track the system in the IT system inventory and in budget documentation**.**

Results of a preliminary sensitivity assessment

The preliminary sensitivity assessment:

- Identifies potential threats and **security controls**[a] necessary to protect **classified**[b] and **sensitive**[c] information
- Identifies potential privacy
- Contains a preliminary security analysis commensurate with the scope and complexity of the program objective intended to be supported by the proposed procurement
- Results in a preliminary **security sensitivity determination** [d]

Note: *(For more information on **bold** terms see footnote♦)*

♦ Security controls, include cryptography and auditing, are covered in the IT Security Controls In Systems section of this training module.

[b]Executive Order 12958, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy based on an Executive Order of Act of Congress. A system is considered "classified" if it is used, intentionally or accidentally, to electronically process, store, or transmit national security "Confidential," "Secret," or "Top Secret" data or information.

[c]The Computer Security Act of 1987 (P.L. 100-235) provides the following definition for sensitive information: "…any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

[d] Sensitivity depends on the mission. For example, if the agency/operating unit mission were financial in nature, availability sensitivity would probably be high. As a guide, the following ranges are provided to assist in your determination of information sensitivity. A determination of medium level would apply if the data does not fit in either the low or high level.

- Confidentiality: low confidentiality applies to publicly available information; whereas high confidentiality would apply to classified national security information.
- Integrity: low integrity applies to data that has no impact to the DOC mission; high integrity reflects that Public Law requires data protection.
- Availability: Low availability indicates the data could be unavailable for more than XX hours/days without significant mission impairment; high availability requires the data to be restored within XX hours/days of the loss or damage to the system to ensure mission continuity. The timeframe established by the number of hours/days must be determined by each Agency.
- Criticality: Low criticality indicates that data is non-mission critical but business essential; medium criticality indicates data that is mission critical; high criticality indicates data is a paramount concern and critical to carrying out a national mission.

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 2: Acquisition Planning

Introduction	Acquisition planning results in a requirement analysis that specifically addresses security consideration. Funding the requirement also takes place during this phase.
Requirement Analysis	The requirements analysis is an in-depth study of the need and the initial beginnings of the Statement of Work (SOW). The requirements analysis draws on and further develops the work performed during mission/business planning by incorporating market research, any results from analysis of alternatives, and incorporates a risk assessment that addresses confidentiality, integrity, and availability, as well as the criticality of the system to the Department's mission.
The CO and the Procurement Initiator	The CO and Procurement Initiator are jointly responsible for: • Conducting market research, including consideration of socioeconomic programs, and • Planning the acquisition in accordance with FAR Part 7[4].
The CO	The CO should: • Include security requirements in any Requests for Comments or Request for Information. • Consider the needs determination and requirements analysis in the acquisition plan.
Project Team	The Procurement Initiator anticipated COTR, Contracting Officer and Program Manager comprise the project team that is responsible for considering IT security when funding the requirement by completing a Capital Asset Plan and Business Case as required by OMB Circular A-11, Section 300[5]. • May be required to present the Capital Asset and Business Case to the ITRB when requested.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 2: Acquisition Planning, Continued

The Capital Asset Plan and Business Case

The Capital Asset Plan and Business Case:

- should demonstrate that the proposed use of IT dollars is aligned with strategic plans,
- support mission requirements,
- comply with architecture goals,
- minimize project risk, and
- demonstrate a positive return on the investment.
- provide specific performance measures for the proposed project and address the IT security procedures and funds allocated to security.

NOTE: The level of detail presented should be commensurate with the magnitude of the investment.

NOTE: ITRB expectations, capital asset plan and business case format, and review criteria can be found on the Office of the Secretary, Office of the Chief Information Officer website. For more information click here[6].

Risk Assessment Definition

A risk assessment is a methodical identification and measurement of:

- threats to a system or information processed or stored by the system,
- vulnerability of the system to the threats, and
- the probability, or risk, that a given threat could exploit the vulnerabilities.

Procurement Initiators

Procurement Initiators must perform risk assessments of all DOC IT general support systems as well as major applications.

General Support System

A general support system is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 2: Acquisition Planning, Continued

A major application

A major application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

To prevent or mitigate risk

The procurement initiator, in consultation with the IT security office and other interested parties, use the results of this evaluation to determine controls to prevent or mitigate risk to an acceptable level.

Risk Assessment Methodology

The IT Security Officer can assist by providing the Procurement Initiators with a risk assessment methodology, and by providing assistance in identifying potential threats and interpreting the risk assessment results and suggesting possible cost-effective security countermeasure alternatives.

Perform Risk Assessment

To perform a risk assessment, perform the following actions.

For DOC/NIST recommended information about performing risk assessments click here.[7]

Definition of Assurance

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.

Step	Action
1	Update the preliminary Sensitivity Assessment developed in the Mission and Business by including pertinent information resulting from the requirements analysis and the risk assessment.

Continued on next page

Definition of Assurance (continued)

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>2</td><td>Determine and obtain assurance. There are several techniques for obtaining assurance.</td></tr>
<tr><td>3.</td><td>
<table>
<tr><th colspan="2">Techniques for obtaining assurance include:</th></tr>
<tr><td>1</td><td>Evaluations by Independent Organizations</td></tr>
<tr><td>2</td><td>Evaluations by Another Vendor</td></tr>
<tr><td>3</td><td>Evaluations by Another Government Agency</td></tr>
<tr><td>4</td><td>Accreditations of a System to Operate in s Similar Situation</td></tr>
<tr><td>5</td><td>Self-Certification Following a Formal Procedure</td></tr>
<tr><td>6</td><td>Conformance Testing and Validation Suites</td></tr>
</table>
Update the preliminary Sensitivity Assessment developed in the Mission and Business Planning Phase.</td></tr>
<tr><td></td><td>Use the following procedures to update the preliminary Sensitivity Assessment.
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Determine assurance by ascertaining the degree to which the purchaser of a system knows that the security</td></tr>
</table>
</td></tr>
</table>

Continued on next page

Definition of Assurance (continued)

Step	Action
	2 Obtain Assurance by analyzing the following documents: • Evaluations by Independent Organizations • Evaluations by Another Vendor • Evaluations by Another Government Agency • Accreditation of a System to Operate in a Similar Situation • Self-Certification Following a Formal Procedure • Conformance Testing and Validation Suites
4	Develop Systems Security Plan to provide all the information necessary to secure an IT system throughout the system's life cycle including: • an overview of the security requirements of the system and the information processed; • a delineation of the responsibilities and expected behavior of all individuals who access the system; • information and agreement regarding interconnections with other systems; and • other information necessary for the operation and maintenance of the system **Note:** Refer to National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*,[8] for additional information on the DOC standards for system security plans.

Definition of System Security Plan

An IT system security plan provides an overview of the sensitivity levels and types of data processed or stored in a system and the related security requirements to protect the data.

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 3: Acquisition

Introduction

This phase covers the development and issuance of the solicitation and the receipt and evaluation of offers or quotations. 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 (Statement of Work (SOW);
- how it will be acquired (Source Selection Plan);
- how it will be evaluated, tested, and accepted (offer or quotation evaluation plan); and
- how the contract will be administered (contract administration).

Security Considerations

Security requirements/specifications for the request for offers or quotes should be established for inclusion in the SOW. The requirements or specifications include two types of sources:

- General specifications
- Federally mandated specifications

NOTE: It is incumbent on the procurement initiator to know what federally mandated and general specifications apply to the system(s) being procured. These are technical issues and are, therefore, the responsibility of the procurement initiator who may obtain assistance from the IT Security Officer and Program Managers.

General specifications

General IT security specifications found in policy documents[1] should be reviewed for applicability to the system being procured.

Federally mandated specifications

These are required by law and must be in accordance with applicable Federal Information Processing Standards (FIPS) publications. FIPS publications may be found at the NIST Computer Security Resource Center.[9]

Continued on next page

[1] Applicable OMB Circulars, Memoranda, and policy documents may be found at http://www.whitehouse.gov/ombandand http://www.whitehouse.gov/omb/inforeg/infopoltech.html and section 3.3.2.4 of the Department of Commerce's IT Security Program Policy and Minimum Implementation Standards, http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm#development_stage.

Section 4: Effective Integration: Procurement and System Life Cycles

Phase 3: Acquisition, Continued

Contractor compliance	The SOW and request for offers or quotes are fully developed during this phase and should ensure that the contractor will comply with applicable DOC IT Security Program Policies as discussed in Section 3.3.2.4[10] of the US DOC IT Security Program Policy and Minimum Implementation Standards.
Assignment of Contract Security Risk or Sensitivity Level	The Procurement Initiator or Program Manager, in conjunction with operating IT security officer and servicing security officer (if the contract requires access to classified information), will review the work to be performed under contract and assign the highest risk or classified sensitivity designation to the entire contract in accordance with the criteria stated in Chapter 10, paragraph 1003, of the Department of Commerce Security Manual (http://www.osec.doc.gov/osy/default2.htm). Accordingly, each contract employee will undergo investigative processing based on the contract's risk or sensitivity level designation.
Establish Personnel Security requirements	The Commerce Acquisition Manual (CAM) section 1337.70*, Security Processing Requirements for On-Site Service Contracts*, and related CAM Notice 00-02, provide facility access criteria and contract language for IT service contracts. **NOTE:** It is the responsibility of both the procurement initiator and the contracting officer to develop the offer or quotation evaluation/acceptance criteria and to determine personnel security requirements applicable to the acquisition.
Request for Background Investigation	All contract personnel who will perform work on the contract must undergo investigative processing, or hold a current, valid security clearance, corresponding to the risk or sensitivity level of the contract. Within each contract, the contracting officer must include information that defines the investigative processing requirements associated with the contract's risk level. Requests for background investigations for non-classified contracts are processed through the DOC Office of Security (see the Security Manual, Chapter 11, paragraph 1104 http://www.osec.doc.gov/osy/default2.htm). Requests for background investigations for work on classified contracts must be initiated by the Contractor and processed with and granted by the Defense Industrial Security Clearance Office (DISCO) through the NISPOM (National Industrial Security Program Operating Manual) process (http://www.dss.mil).

Section 4: Effective Integration: Procurement and System Life Cycles

Phase 3: Acquisition, Continued

IT security	IT security should be addressed in the evaluation criteria portion of the solicitation to call attention to the importance of security to the government.
Quotation Evaluation or Acceptance Criteria	Sample Offer or Quotation Evaluation/Acceptance Criteria are: • Testing - Depending on the nature of the system, testing can be part of the offer or quotation evaluation, in the form of live test demonstrations or benchmarks, or it can be part of post-award acceptance testing. • On-site Inspection – Inspections of the offeror's site by the Government can help to ensure that the offeror's security policies and procedures have been correctly implemented. • Offeror's Strategy for Security - This strategy should be commensurate with the size and complexity of the system. All systems acquisitions should request some form of offeror security strategy. In this strategy, the offeror should state how the product or service would meet the security needs of the government. • Offeror's Internal Security Policy and Plan - Procurements that include contract services can evaluate the offeror's internal security policy. Depending on the scope of the acquisition, this may include copies of the offeror's applicable information security, personnel security, and physical security policies.
Final acceptance criteria	The final acceptance criteria will be placed in the solicitation by the Contracting Officer for dissemination to all prospective offerors. Upon receipt of proposals the technical evaluation team will review offerors proposals against the acceptance criteria in the solicitation.
Technical evaluation of offers or quotations	The technical evaluation team conducts a review of offers or quotations to determine the adequacy and capability of the offeror to meet the security requirements listed in the solicitation. The procurement initiator leads the technical evaluation team and prepares a technical evaluation report.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles

Phase 3: Acquisition, Continued Continued

Security review of solicitation

The Procurement Initiator, and/or Program Manager and the IT Security Officer certify that the offer or quotation complies with the security requirements specified in the solicitation and the requirements of the DOC IT Security Program.

If required in the offer or quotation evaluation plan And specified in the solicitation	Then the Procurement Initiator and the IT security Officer	And
	Conduct an on-site inspection of the offeror's facilities to ensure that facility safeguards are commensurate with the sensitivity of data and the value of the assets to be protected during performance of the contract.	The Procurement Initiator provides written confirmation of findings from the inspection to the Contracting Officer.
	The Procurement Initiator and/or the IT Security Officer conduct testing of the offeror's computer security assurances to ensure that the required level of assurance is commensurate with the sensitivity of data and the value of the assets to be protected during performance of the contract.	The Procurement Initiator provides written confirmation to the Contracting Officer that required security safeguards meet the testing criteria.

Note: When the Contracting Officer has received written confirmation that the required security safeguards are in place and that any required testing was satisfactory, the Contracting Officer may award the contract and appoint a Contracting Officer Technical Representative (COTR) by means of a written designation memorandum.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles

Phase 3: Acquisition, Continued Continued

Classified National Security Guidance	For classified contracts, the COTR must develop the Department of Defense Contract Security Classification Specification form (DD-254) to provide guidance to the Contractor concerning access to classified information on the contract. Upon completion of the contract, the final DD-254 will become part of the contract file. For further guidance, see Chapter 43 of the DOC Security Manual (http://www.osec.doc.gov/osy/default2.htm).
Award of the Contract	Once the contract has been awarded, the COTR must ensure that all personnel working on the contract complete nondisclosure agreements for both sensitive and classified information and receive their initial IT Security training and classified briefings (if required).

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 4: Contract Performance Period

Introduction	This phase involves contractor monitoring. The COTR may require IT security expertise to assist in reviewing contract performance measurement documentation, inspect IT security deliverables, or evaluate contract modifications.
Security Considerations	The COTR should ensure that a technically qualified federal employee certifies and a senior program official accredits that the security controls on the system, application, or networks meet the requirements as required by all mandated security policies and guidance routinely throughout the contract performance period. Updates should be provided to the Contracting Officer. **NOTE**: Only a federal employee can be a System Certifier (cannot be the system owner) and the Accreditor (also not the system owner).

Note: The bullet does refer to a formal process of certifying and accrediting. NIST SP 800-37, Guidelines for the Security Certification and Accreditation of Federal Information Systems[11] provide guidelines for certification and accreditation.

Review of Contractor's performance	The COTR should regularly review the contractor's performance to ensure security has not degraded since formal system certification and that changes in the environment and system that result in new threats and vulnerabilities are recognized and appropriate safeguards are put in place. The Risk Assessment and the System Security Plan should be updated accordingly.

Continued on next page

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Responsibilities during the Contract's performance

During the contract performance period the COTR monitors the daily operation of the system in order to:

- maintain continued operational assurance;
- update the system security plan;
- ensure the systematic completion of authorized changes to the configuration, or structure, of the system;
- authorize, control, test, and implement hardware and software changes to the system; and
- ensure incidents of system compromise are reported to the appropriate bureau Computer Incident Response Capability or Team. For more information on incident response procedures, see section 3.14 of the DOC IT Security Program Policy[12].

Classified Contract

For classified contracts, the COTR must verify and/or update the final DD-254, DOD Contract Security Classification Specification form, and submit it to the Contracting Officer for inclusion in the contract record file.

Concurrence and Non-concurrence of contract deliverables

The COTR must provide concurrence/non-concurrence of contract deliverables, i.e. products and/or services delivered to the government under the contract in order to determine if the deliverables meet the specifications set forth in the contract. If so, the government accepts and pays for the deliverables as stipulated in the contract.

Section 4: Effective Integration: Procurement and System Life Cycles, Continued

Phase 5: Contract Closeout Period

Introduction

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 for the contracting officer and the COTR to ensure that government resources and assets are protected.

Security Considerations

DOC should use the following security considerations:

- 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. For more information on refer to SP 800-64 Security Considerations in the Information System Development Life Cycle[13].

Section 4: Effective Integration: Procurement and System Life Cycles,

Phase 5: Contract Closeout Period, Continued

Security Considerations, continued	Dispose 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. Some systems may contain sensitive information after the storage media is removed. If there is doubt whether sensitive information remains on a system, the COTR should consult with the IT Security Program Manager prior to disposing of the system. For classified contracts, the disposal of classified hardware and software must comply with the NISPOM guidance (http://www.archives.gov/isoo/rules_and_regulations/rules_and_regulations.html).

Note: It is incumbent upon the COTR to ensure that the security considerations have been addressed during the contract closeout period and, if necessary, to obtain IT security expertise.

Section 5: IT Security Controls in Systems

Introduction

This section addresses several security controls that can be considered during the preparation of the Statement Of Work (SOW) during the acquisition planning and acquisition phases of a procurement. The controls presented in this section are not exhaustive as there are many different controls that can be applied; but, for many systems, a combination of features will be used. The suggested language or the applicable IT security or policy document may be used in the SOW, as appropriate.

Controls and Suggested SOW language

The definition of the controls and the suggested SOW language follows:

Control Definition	Suggested SOW language
Identification and Authentication Used to enforce accountability and access control, all users or authorized groups must have a unique identifier and use individual passwords compliant with the DOC *Policy on Password Management* to 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).* **Note:** See U.S. Department of Commerce IT Security Program Policy Section: 3.15[14]

Continued on next page

Controls and Suggested SOW language (continued)

Control Definition	Suggested SOW language
Access Control Access control is used to ensure that access to IT resources is authorized at the level of least privilege where necessary. Access control protects confidentiality and integrity and supports the principles of legitimate use, least privilege, and separation of duty.	*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.* **Note:** See U.S. Department of Commerce IT Security Program Policy Section: 3.16[15]
Auditing Auditing is used to provide protection by enabling organizations to record meaningful actions within the system and to hold the user accountable for each action.	Suggested SOW language… *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 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 other security relevant events. The system shall also be able*

	to audit any override of human-readable output markings. *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.* **Note:** See U.S. Department of Commerce IT Security Program Policy Section: 3.17[16]
Cryptography A type of control for protecting sensitive unclassified information. The NIST Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal* Government provides a comprehensive reference for government use of cryptography.	*The cryptographic module and algorithm shall be validated by a Cryptographic Module Testing laboratory.* **Note:** See U.S. Department of Commerce IT Security Program Policy Section: 3.16.7[17]
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.	*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.*

Section 6: Key Security Specifications and Clauses

Introduction

Suggested language for integrating key IT security specifications into offer or quotation documentation can be found in Section 3 of NIST 800-4.[18] Some of the areas covered in the NIST publication are:

- Control of Hardware and Software
- Contract Administration
- Contract/Task Closeout
- Government-furnished equipment (GFE)

Federal Acquisition Regulation (FAR) Clauses

The FAR contains the following clauses that IT security needs to be concerned about:

Clause	Use
FAR 39.107	FAR 39.107, prescribes *FAR 52.239-1, Privacy or Security Safeguards* or a clause substantially the same as the clause at 52.239-1, Privacy or Security Safeguards, in solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services. For a full text version of the clause click here[19].

Continued on next page

Federal Acquisition Regulation (FAR) Clauses (continued)

Clause	Use
Clauses that define the respective responsibilities and allocate risks among the parties to a government contract	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. Contracting Officers should review FAR clauses addressing guarantees, warranties, or liquidated damages for applicability.

Continued on next page

Section 6: Key Security Specifications and Clauses, Continued

Introduction The following table contains key security specifications and clauses.

Clause	Use
Commerce Acquisition Regulation (CAR) 1352.239-73	As prescribed in (CAR 1339.70), the Contracting Officer shall insert **CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES** or a clause substantially the same as it in all DOC solicitations and contracts for services. For a full text version of the clause see Appendix A.
Commerce Acquisition Regulation (CAR) 1352.239-74	As prescribed in (CAR 1339.70), the Contracting Officer shall insert **CAR 1352.239-74 SECURITY PROCESSING REQUIREMENTS FOR CONTRACTORS/SUBCONTRACTOR PERSONNEL FOR ACCESSING DOC INFORMATION TECHNOLOGY SYSTEMS** or a clause substantially the same as it in all DOC solicitations and contracts for services. For a full text version of the clause see Appendix B.

Appendix A

The Contracting Officer shall insert a clause the same as the following in all DOC solicitations and contracts for services. The following language may only be modified by adding more restrictive agency or bureau specific guidance

CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

(a) This clause is applicable to all contracts that include information technology resources or services in which the Contractor must have physical or electronic access to DOC's sensitive or classified information, which is contained in systems that directly support the mission of the Agency. For purposes of this clause the term "Sensitive" is defined by the guidance set forth in:

(1) The *DOC IT Security Program Policy and Minimum Implementation Standards* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html);

(2) The Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, (http://csrc.nist.gov/secplcy/a130app3.txt) which states that there is a "presumption that all [general support systems] contain some sensitive information."; and

(3) The Computer Security Act of 1987 (P.L. 100-235) (http://www.epic.org/crypto/csa/csa.html), including the following definition of the term sensitive information "… any information, the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552 a of title 5, Unites States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

For purposes of this clause, the term "Classified" is defined by the guidance set forth in:

(1) The *DOC IT Security Program Policy and Minimum Implementation Standards, Section 3.3.1.4* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html).

(2) The *DOC Security Manual, Chapter 18* (http://www.osec.doc.gov/osy/).

(3) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include,

but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of DOC IT resources for all of the contractor's systems that are interconnected with a DOC network or DOC systems that are operated by the Contractor.

(b) All Contractor personnel performing under this contract and Contractor equipment used to process or store DOC data, or to connect to DOC networks, must comply with the requirements contained in the DOC *Information Technology Management Handbook* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html), or equivalent/more specific agency or bureau guidance as specified immediately hereafter [insert agency or bureau specific guidance, if applicable].

(c) For all Contractor-owned systems for which performance of the contract requires interconnection with a DOC network or that DOC data be stored or processed on them, the Contractor Shall:

(1) Provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq*.) and the Federal Information Security Management Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946-2961 (2002); Pub. L. No. 107-296, 116 Stat. 2135, 2259-2273 (2002). 38 WEEKLY COMP. PRES. DOC. 51, 2174 (Dec. 23, 2002) (providing statement by President George W. Bush regarding Federal Information Security Management Act of 2002). The plan shall meet IT security requirements in accordance with Federal and DOC policies and procedures that include, but are not limited to:

(a) OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources* (http://csrc.nist.gov/secplcy/a130app3.txt);
(b) National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF) ; and
(c) DOC Procedures and Guidelines in the *Information Technology Management Handbook* (http://www.osec.doc.gov/cio/itmhweb/itmhweb1.html). .
(d) National Industrial Security Program Operating Manual (NISPOM) for classified systems (http://www.dss.mil/isec/nispom.htm); and
(e) [Insert agency or bureau specific guidance].

(2) Within 14 days after contract award, the contractor shall submit for DOC approval a System Certification and Accreditation package, including the IT Security Plan and a system certification test plan, as outlined in *DOC IT Security Program Policy*, Sections 3.4 and 3.5 (http://home.osec.doc.gov/DOC-IT-Security-Program-Policy.htm). The

Certification and Accreditation Package must be consistent with and provide further detail for the security approach contained in the offeror's proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The Certification and Accreditation Package, as approved by the Contracting Officer, in consultation with the DOC IT Security Manager, or Agency/Bureau IT Security Manager/Officer, shall be incorporated as part of the contract. DOC will use the incorporated IT Security Plan as the basis for certification and accreditation of the contractor system that will process DOC data or connect to DOC networks. Failure to submit and receive approval of the Certification and Accreditation Package, as outlined in *DOC IT Security Program Policy*, Sections 3.4 and 3.5 (http://home.osec.doc.gov/DOC-IT-Security-Program-Policy.htm) may result in termination of the contract.

(d) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

Appendix B

The Contracting Officer shall insert a clause the same as the following in all DOC solicitations and contracts for services. The following language may only be modified by adding more restrictive agency or bureau specific guidance. Contracting Officers must include CAR 1352.209-72, *Restrictions Against Disclosures,* in all solicitations and contracts which include CAR 1352.239-74.

CAR 1352.239-74 SECURITY PROCESSING REQUIREMENTS FOR CONTRACTORS/SUBCONTRACTOR PERSONNEL FOR ACCESSING DOC INFORMATION TECHNOLOGY SYSTEMS

(a) Contractor personnel requiring any access to systems operated by the Contractor for DOC or interconnected to a DOC network to perform contract services shall be screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, *Security Processing Requirements for Service Contracts*. DOC shall provide screening using standard personnel screening forms, which the Contractor shall submit to the DOC Contracting Officer's Technical Representative (COTR) based on the following guidance:

1) Contract personnel performing work designated Contract High Risk and personnel performing work designated Contract Moderate Risk in the information technology (IT) occupations and those with "global access" to an automated information system require a favorable pre-employment check before the start of work on the contract, regardless of the expected duration of the contract. After a favorable pre-employment check has been obtained, the Background Investigation (BI) for Contract High Risk and the Minimum Background Investigation (MBI) for Contract IT Moderate Risk positions must be initiated within three working days of the start of work.

2) Contract personnel performing work designated Contract Moderate Risk who are not performing IT-related contract work do not require a favorable pre-employment check prior to their employment; however, the Minimum Background Investigation (MBI) must be initiated within three working days of the subject's start of work on the contract, regardless of the expected duration of the contract.

3) Contract personnel performing work designated Contract Low Risk will require a National Agency Check and Inquiries (NACI) upon the subject's start of work on the contract if the expected duration of the contract exceeds 365 calendar days. The NACI must be initiated within three working days of the subject's start of work on the contract.

4) Contract personnel performing work designated Contract Low Risk will require a Special Agreement Check (SAC) upon the subject's start of work on the contract if the expected duration of the contract (including options) exceeds 180 calendar days but is less than 365 calendar days. The SAC must be initiated within three working days of the subject's start of work on the contract.

5) Contract personnel performing work on contracts requiring access to classified information must undergo investigative processing according to the Department of Defense National Industrial Security Program Operating Manual (NISPOM), (http://www.dss.mil/isec/nispom.htm) and be granted eligibility for access to classified information prior to beginning work on the contract.

The security forms may be obtained from the cognizant DOC security office servicing your bureau, operating unit, or Departmental office. At the option of the government, interim access to DOC IT systems may be granted pending favorable completion of a pre-employment check. Final access may be granted only on completion of an appropriate investigation based upon the risk level assigned to the contract by the Contracting Officer.

(b) Within 5 days after contract award, the Contractor shall certify in writing to the COTR that its employees, in performance of the contract, have completed annual IT security awareness training in DOC IT Security policies, procedures, computer ethics, and best practices, in accordance with *DOC IT Security Program Policy,* section 3.13 (http://home.osec.doc.gov/DOC-IT-Security-Program-Policy.htm). The COTR will inform the Contractor of any other available DOC training resources.

(c) Within 5 days of contract award, the Contractor shall provide the COTR with signed Nondisclosure Agreements as specified in Commerce Acquisition Regulation (CAR), 1352.209-72, *Restrictions Against Disclosures*.

(d) The Contractor shall afford DOC, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOC data or to the function of computer systems operated on behalf of DOC, and to preserve evidence of computer crime.

(e) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

ENDNOTES

[1] http://www.osec.doc.gov/cio/oipr/itsec/DOC-IT-Security-Program-Policy.htm
[2] http://www.osec.doc.gov/cio/oipr/itsec/DOC-IT-Security-Program-Policy.htm
[3] http://csrc.nist.gov/publications/nistpubs/
[4] http://www.arnet.gov/far/loadmainre.html
[5] http://www.whitehouse.gov/omb/circulars/a11/2002/part7.pdf
[6] http://www.osec.doc.gov/cio/oipr/ITPLANPAGE.HTM
[7] GAO AIMD-12.19.6 Financial Information Systems Controls Audit Manual: Volume 1
http://www.gao.gov/special.pubs/ai12.19.6.pdf

GAO/AIMD-98-68 Executive Guide: Information Security Management
http://www.gao.gov/special.pubs/infosec.guide/

GAO/AIMD-00-33 Information Security Risk Assessment: Practices of Leading Organizations
http://www.gao.gov/special.pubs/ai00033.pdf

National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

National Institute of Standards and Technology Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems"
http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

National Institute of Standards and Technology Special Publication 800-27, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)"
http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf

[8] http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF
[9] http://csrc.nist.gov/publications/
[10] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[11] http://csrc.nist.gov/publications/nistpubs/
[12] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[13] http://csrc.nist.gov/publications/nistpubs/index.html
[14] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[15] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[16] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[17] http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm
[18] http://csrc.nist.gov/publications/drafts/800-4_PC_100802.pdf
[19] http://www.arnet.gov/far/loadmainre.html