NCSC TECHNICAL REPORT–004
Library No. S–241,359

NATIONAL COMPUTER SECURITY CENTER

A GUIDE TO PROCUREMENT OF SINGLE AND CONNECTED SYSTEMS

LANGUAGE FOR RFP SPECIFICATIONS AND STATEMENTS OF WORK – AN AID TO PROCUREMENT INITIATORS

INCLUDES COMPLEX, EVOLVING, MULTIPOLICY SYSTEMS

July 1994

Approved for Public Release:
Distribution Unlimited

Accession Number: 5413

Publication Date: Jul 01, 1994

Title: Guide to Procurement of Single and Connected Systems Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators

Corporate Author Or Publisher: National Security Agency, 9800 Savage Road, Ft. Geo. G. Meade, MD 2075 Report Number: NCSC Technical Report - 004 Report Number Assigned by Contract Monitor: Library No.S-241,359

Comments on Document: Final Report

Descriptors, Keywords: Security Requirement Policy Complex System Certification Accreditation Automated Information Domain Constant

Pages: 00101

Cataloged Date: Sep 22, 1994

Document Type: HC

Number of Copies In Library: 000001

Record ID: 29396

NCSC TECHNICAL REPORT-004
Library No. S-241,359
July 1994

FOREWORD

This technical report is a strawman update to Volume 2 of 4 of the procurement guideline series. The previous version was updated to deal with complex, evolving, multipolicy systems. It is written to help facilitate the acquisition of trusted computer systems in accordance with DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." It is designed for new or experienced automated information system developers, purchasers, or program managers who must identify and satisfy requirements associated with security-relevant acquisitions. Information contained within this series will facilitate subsequent development of procurement guidance for future national criteria. This series also includes information being developed for certification and accreditation guidance. Finally this Volume 2 procurement strawman addresses the way by which Trusted Computer System Evaluation Criteria, the Trusted Network Interpretation, and the Trusted Database Management System Interpretation using a new approach called Domains of Constant Policy are translated into language for use in the Request for Proposal (RFP) Specifications and Statements of Work.

The business of computers, security, and acquisitions is complex and dynamic. I invite your recommendations for revision to this technical guideline. Our staff will work to keep it current. However, experience of users in the field is the most important source of timely information. Please send comments and suggestions to:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000

ATTN: Standards, Criteria, and Guidelines Division

Reviewed by: _____
GLENN GOMES
Chief, INFOSEC Standards, Criteria & Guidelines Division

Released by: _____
ROBERT J. SCALZI
Chief, INFOSEC Systems Engineering Office

ACKNOWLEDGMENTS

This document has been produced under the guidance of MAJOR (USA) Melvin L. De Vilbiss, the National Security Agency (NSA). It was developed by Howard L. Johnson, Information Intelligence Sciences, Inc.

This STRAWMAN was delivered to the Government in March 1993, as Howard Johnson's last deliverable under contract before his passing on 14 May 1993. We dedicate this document in his memory.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 GENERAL INFORMATION

1.1 INTRODUCTION

The National Security Agency (NSA) wants to clarify the computer security aspects of the Department of Defense (DoD) automated information system (AIS) acquisition process. Therefore, it is producing a four volume guideline series (referenced in Table 1-1 with more complete titles in the Bibliography). This document is a proposed second volume that has been written to deal with complex systems, that is, systems composed of systems. These guidelines are intended for Federal agency use in acquiring trusted systems.

Table 1-1 Procurement Guideline Series

An Introduction to Procurement Initiators on Computer Security Requirements, December 1992.

Language for RFP Specifications and Statements of Work—An Aid to Procurement Initiators, 30 June 1993.

Computer Security Contract Data Requirements List and Data Item Descriptions Tutorial, 28 February 1994.

How to Evaluate a Bidder's Proposal Document—An Aid to Procurement Initiators and Contractors (to be published in 1994).

DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," provides security requirements concerning all protection aspects of automated information systems. It specifies DoD 5200. 28-STD, "DoD Trusted Computer System Evaluation Criteria" (TCSEC), as the requirement source for trusted computer systems. The second page of the DoD 5200. 28-STD states: "This document is used to provide a basis for specifying security requirements in acquisition specifications.

1.2 PURPOSE

The intended user of the document is the "procurement initiator," to include program managers, users, and security managers. These individuals must write the Request for Proposal (RFP), specifically Section C, the Specification and Statement of Work. Volume 1 of this guideline series discusses the responsibilities of different roles in procurement initiation.

The purpose of this document is to facilitate the contracting process, to provide uniformity in competitive acquisitions, to minimize procurement cost and risk, avoid delays in the solicitation process, and to help ensure the solicitation is complete before its issuance.

1.2.1 FACILITATING THE CONTRACTING PROCESS

This guideline provides Specification and Statement of Work (SOW) contract language to procure a trusted system, hopefully satisfied by products from the NSA Evaluated Product List (EPL). This document does not address Government certification and accreditation tasks. The guideline is written to ensure the selected

system will provide adequate security, while avoiding a costly solution. This document has no intent beyond the security aspects of the system.

DoD agencies should use this document whenever considering the acquisition of trusted computer systems. System security requirements are provided in contract language for direct incorporation into a Request For Proposal (RFP). The language duplicates the words and intent of the DoD Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200. 28-STD. It incorporates the approach to be used and provides interpretations to the TCSEC when complex systems are developed. **It includes the situation in which part of the trusted systems are developed under the Trusted Network Interpretation (TNI) or the Trusted Database Interpretation (TDI).**

1.2.2 FACILITATING FAIRNESS IN COMPETITIVE ACQUISITIONS

This guideline promotes the use of EPL products while at the same time satisfying requirements for fair competition. If these requirements have not been satisfied, the procurement can result in a protest and the selection may possibly be nullified. These requirements include:

a. Public Law 98-369 "Competition in Contracting Act of 1984"

b. Title 41, United States Code, Section 418, "Advocates for Competition"

c. Title 10, United States Code, Section 2318, "Advocates for Competition"

d. DoD Instruction 5000.2, "Defense Acquisition Management Policy," February 23, 1991, pp. 5-A-2 through 4

e. DoD 5000. 2-M, "Defense Acquisition Management Documentation and Reports," February, 1991, p. 4-D-1-3 d.(1)

1.2.3 MINIMIZING PROCUREMENT COST AND RISK

Version 1 of this procurement guideline series is written solely to acquire products on the Evaluated Products List (EPL), that is, to enable the procurement initiator to obtain those EPL products available for integration into an application, as opposed to developing a system through specification.

For solutions that use EPL products, not only have the specifications of the evaluated Division/Class been satisfied, but the assurance tasks have been completed and the required documentation produced. Certification evidence, analyses, and operational documents previously produced for an NSA evaluation may be available to ensure trustworthiness and used directly for certification and satisfaction of required proposal and contract data. The results are less development risk and a lower overall cost to the bidder and, consequently, to the Government.

For some well defined entity of a system to be regarded as secure in the TCSEC sense means that, at a minimum, all of the requirements of some specified TCSEC Division/Class must be met. This is discussed further in Volume 1, Chapter 3. To call that entity, for example, a Class B2 entity would require NSA evaluation as a product satisfying the Class B2 criteria. (This convention has evolved over the past several years so that products would not be misrepresented in their evaluation status.)

A successful certification evaluation of an entity (which has not been placed on the NSA evaluated Products List (EPL)) can only state that evaluation and approval have been completed as part of a certification process against the Class B2 set of requirements.

The rationale for this approach is as follows:

a. Although a Division/Class of the TCSEC is used as the basis for the secure part of a system, the procurement and build process can introduce new, conflicting requirements and relax, reinterpret, or change the intent of some of the existing TCSEC requirements. Only an exact evaluation can determine this.

b. The certification evaluation process addresses the needs of a single implementation. It has generally not experienced the finely honed expertise of the NSA evaluation process and personnel; and does not have the same assurance for additional applications as does an EPL product.

The Request for Proposal (RFP) can not dictate that an item come from the EPL because of the limited number of items on the EPL and because the process for placement on the EPL is itself a restricted, Government controlled process. To state such a requirement in the RFP would constitute a discrimination against other vendors desiring to bid. It also can not be stated that, for example, "a B2 system is required" because that implies the solution must be taken from the EPL. Therefore, the specific TCSEC requirements necessary to meet a certain Division/Class rating must be spelled out, without stating that the B2 product is desired. However, the desire for decreased risk and cost (common to EPL products) is normally a strong evaluation weighting factor for source selection.

1.2.4 ENSURING THE SOLICITATION IS COMPLETE BEFORE ISSUANCE

If we try to use existing TCSEC criteria as RFP requirements, it is found that those criteria are not presented in the form and order required by the RFP. The TCSEC intermixes system specifications, work statements and products to be delivered. This guideline organizes the TCSEC requirements into an RFP format.

1.3 SCOPE

This guideline does not revise the words in DoD 5200. 28-STD; it is a reformatting and reordering into a form suitable for use in contractual documents. This document might be thought of as an adaptation of the TCSEC for procurement. Procurement considerations or interpretations are documented or referenced within the guideline to advise the procurement initiator of factors that may influence procurement decisions. All of the factors are addressed as possible augmentations to the specification language provided.

1.4 BACKGROUND

A Federal Government awareness of the lack of guidance in the security arena led to the formation of the DoD Computer Security Evaluation Center (later the National Computer Security Center). The Trusted Product Evaluation Program (TPEP) was started to provide an "independent laboratory" assessment of commercial products.

The TCSEC was published in 1983 and revised to become a DoD standard in December 1985 to provide criteria for evaluating security features and assurance

requirements available in "trusted, commercially available, automatic data processing systems."

The process for acquiring trusted systems is slightly different than other acquisitions. The major differences are: 1) that the security requirements may become a major constraining factor in determining the solution needed to meet the remaining requirements and 2) there exists a void of acquisition guidance for AIS security.

The challenge for the procurement initiator is to specify the requirements with sufficient clarity and flexibility to achieve the desired security functions without limiting the ingenuity and ability of the offerors to supply a compliant overall solution.

1.5 COMPLEX SYSTEMS

The TCSEC and the TNI specify simple systems in the sense that they are supported by a single division/class, a single TCB, and the security requirements that go along with them. The TDI was the first guidance to address multiple TCBs by introducing the concept of TCB subset and the property of more and less primitive and TCB subset dependency. The conceptual portion of the TDI was written primarily to reduce the cost of assurance of a system when multiple TCBs are present, especially addressing the case when one system has been evaluated successfully under the EPL program (e.g., an operating system) and the second system (e.g., a database management system) is being added to it at minimum assurance cost.

The general case of interfacing TCBs into a system, existing or not; evaluated or not evaluated is not addressed by the TDI. These cases where the principles of composability as addressed by the TDI are not or cannot be satisfied, remain to be addressed.

In the approach used here, the system is divided into unique pieces, called domains of constant policy (DOCPs). Each DOCP has or is intended to have one TCB which will be assigned a Division/Class according to the TCSEC. The only overlapping allowed is shared mechanisms. (It may be found later that this is too restrictive, but in the current development, this restriction has helped to make the problem manageable in evolving C3I systems.) There is no intent to assign the system a division/class rating, but rather to require that it conform to specific interface and global policies that will be applicable at any Division/Class.

The goal is that each DOCP satisfies a Division/Class and that the system be adequately secure at the interfaces and through the communication systems to support the individual DOCPs. There is also a set of global policies to be satisfied that have been identified in the TDI and are carried forward and used more generally here.

In summary, use of this approach enjoys the following advantages:

It offers a solid, intuition supported approach for procurement administrators and DAAs.

It requires the statement of operational policy (e.g., DOCPs and n-tuples) from the using organization and architecturally reflects that in the design.

It enforces precise system covering boundary definition.

It allows, and in fact encourages, cost/risk tradeoffs and iteration of operational policy assignment.

It can be applied to pre regulatory (TCSEC, TNI and/or TDI) systems where the interpretation of TCB must be made.

It does not preclude, and in fact supports use of the TNI and TDI.

It forces consideration of cascading risk, requires interface policy, requires global policy.

It accommodates/promotes use of EPL products since the basic building block entity of a system (a DOCP) has a single policy represented by a division/class requirement of the Orange Book.

It addresses security interface requirements to be satisfied if an EPL product component is going to be integrated into the overall security of the AIS system which may contain other EPL products, existing secure systems, or "to be custom built" specifications.

THIS PAGE INTENTIONALLY LEFT BLANK

2.0 PROCUREMENT PROCESS

The procurement process is governed by policy. Here, three types of policy are distinguished. The first kind of policy is referred to simply as security policy or regulatory policy. This is security policy that applies to all DoD systems, personnel, and operations. Next, computer security policy or COMPUSEC policy is represented by the Division/Class criteria in the TCSEC. Finally, operational security policy is that security policy associated with a given application including range of classifications, range of clearances, categories, mode, and other specific operational security decisions that are made. Operational security policy determines which Division/Class should be used and the detailed requirements and characteristics demanded of each particular procurement.

The procurement process begins with the determination of operational requirements by various Government personnel. They include, but are not limited to, mission users, program managers, and acquisition representatives. The primary goals during this phase include determining Division/Class and mode of operation, as well as identifying those security features and assurances required.

Selection of these security specifications requires a clear understanding of the system users' operational and mission needs, the relevant DOD security policies, available technologies, and the system's operational environment. Procurement initiators and offerors must also consider the security-related areas listed in Figure 2-1 below. More detailed information concerning these security areas can be found in DoD 5200.1-R, DoD Directive 5200.28, and DoD 5200. 28-M.

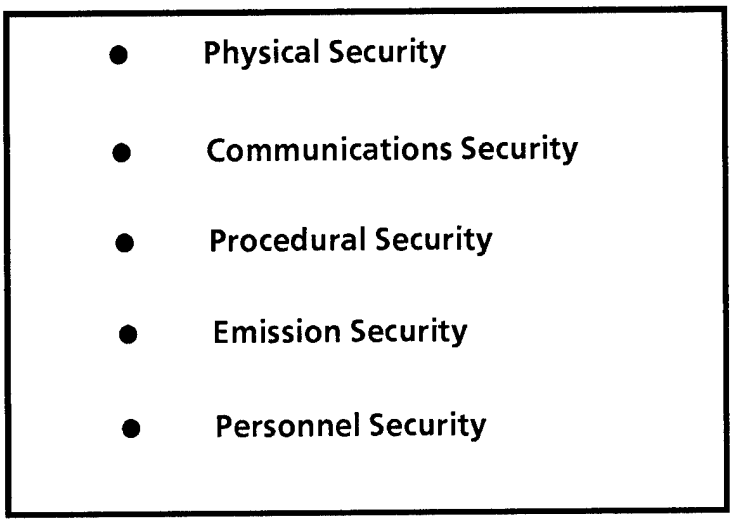

Figure 2-1 Security Related Areas

The Designated Approving Authority (DAA) is responsible under Enclosure 4 of DoD Directive 5200.28 to determine the minimum AIS computer-based security requirements for the mission profile of the system being acquired. Any adjustments to computer security evaluation Division/Class (per step 6 of enclosure 4) will have been completed prior to writing the RFP. The Division/Class that results from this assessment may be changed based on other factors considered by the DAA. The final Division/Class assigned to the system will be used to isolate the appropriate section of the evaluation criteria in the TCSEC, (which is organized by Division/Class).

Later in Chapter 5 of this document we will address specific protection topics in the TCSEC. The paragraph will be used that corresponds to the Division/Class being supported in this procurement. Chapter 5 will identify both Division/Class and the corresponding TCSEC paragraph number to assist the procurement initiator in construction of the RFP.

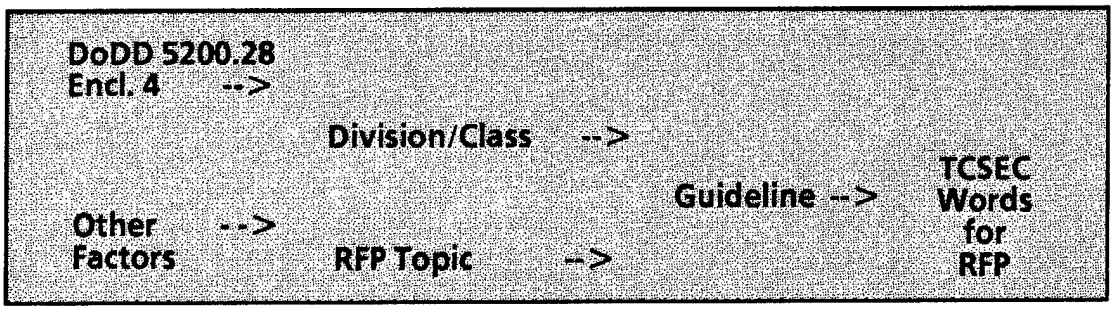

Figure 2-2 Procurement Initiator Guidance

Working with acquisition personnel, the procurement initiators should consult this guideline using the Division/Class selected for the system. The specification language contained in or referenced by this guideline can be applied directly to selected features and assurances. The statements can be amplified to meet specific operational requirements. **Procurement initiators and acquisition personnel must ensure that the security specifications and work statements in Section C of the RFP allow EPL solutions, do not preclude other solutions, and are compliant with the DAA's accreditation requirements.** NSA is eager to help in this determination. The requirements of the TCSEC will be carried through the development life-cycle of the system: RFP, contract, test, certification, and accreditation.

3.0 REQUEST FOR PROPOSAL

The Request for Proposal (RFP) is the focus of this procurement guideline series. A standard RFP has thirteen sections, each designated by a letter of the alphabet (see Table 3-1). The procurement initiator provides input to and review of all of these sections. The majority of the procedural information is controlled directly by the procurement activity. Security relevant sections important to the procurement initiator and addressed in the remainder of this document are highlighted.

Table 3-1 RFP Organization

Letter	Section Title
A	Solicitation/Contract Form, Standard Form 33
B	Supplies or Services with Prices and Costs
C	**Descriptions/Specifications/Statements of Work**
D	Packaging and Marking
E	Inspection and Acceptance
F	**Deliveries and Performance**
G	Contract Administration Data
H	Special Contract Requirements
I	Contract Clauses
J	**List of Documents, Exhibits and Other Attachments**
K	Representations, Certifications and Other Statements of Offerors or Quoters
L	**Instructions, Conditions, and Notices to Offerors**
M	Evaluation Factors for Award

3.1 SECTION C - DESCRIPTIONS/SPECIFICATIONS

The first part of Section C describes the technical requirements to the offeror, including the security requirements. The section is mission user-oriented, and will normally contain a Specifications or Requirements section that lays out the features and capabilities to be included in the system to satisfy mission security requirements. This guideline has consolidated the security functionality requirements of the TCSEC. This will be addressed in detail in Chapter 5.

3.2 SECTION C - STATEMENTS OF WORK (SOW)

The second part of Section C identifies the specific tasks the contractor will perform during the contract period and include security related tasking. The SOW could

include tasks such as system engineering, design, and build. For security, Statements of Work include contractor tasking necessary to achieve specific levels of assurance, including studies and analyses, configuration management, security test and evaluation support, delivery, and maintenance of the trusted system. These work statements also specify the development of the required documentation to be provided under the Contract Data Requirements Lists (CDRLs). This will be addressed in detail in Chapter 5.

3.3 SECTION F - DELIVERIES AND PERFORMANCE

This section covers delivery and installation requirements. Special delivery requirements as specified in the TCSEC need to be included. Performance requirements for the trusted system will also be discussed. This section will be addressed further in Chapter 5 of this guideline.

3.4 SECTION H - SPECIAL CONTRACT REQUIREMENTS

This section of the solicitation contains clauses that are specially tailored for each acquisition. Typical topics covered include: site access and preparation, data rights, maintenance, liquidated damages, and training responsibilities. Although these are not addressed specifically in this guideline, they are often topics of concern to the procurement initiator of trusted systems.

3.5 SECTION J - LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

This section contains a list of documents, exhibits, attachments, and other forms used to build and execute the RFP. There are usually a series of attachments, each one dedicated to a list of specific items. Attachments addressed by this guideline series include the following:

a. The Contract Data Requirements List (CDRL), referencing specific Data Item Description (DID) requirements are provided in Volume 3 of this guideline series and also referenced in RFP Attachment A contained in the Chapter 5 standard presentation of this document. Each SOW task is linked to one or more CDRLs; each CDRL identifies a document or other data that the offeror is required to deliver, along with specific information about that document (e.g. schedule, number and frequency of revisions, distribution). Associated with each CDRL is a Data Item Description (DID) that specifies the document's content and format. Where requirements differ, there are unique DIDs for each Division/Class.

b. Even though it is presented separately, the glossary is an important part of the Specifications and the Statements of Work because it precisely defines terms and further clarifies the language intent. The glossary is included as RFP Attachment B in Chapter 5 of this guideline.

c. Acronyms used in the RFP must be defined in their first use and must also be identified in the accompanying acronym list. Acronyms are included as RFP Attachment C in the Chapter 5 in this guideline.

d. References have been identified for incorporation into the RFP. Terms are compatible with and support the specification language, and as such, become an integral part of an RFP. The references are for technically supporting information and should not be interpreted as requirements. References are included as RFP Attachment D in Chapter 5 of this guideline.

3.6 SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

This section contains the instructions and conditions of the acquisition. It informs Offerors of their actions and responsibilities, if they are planning to submit a proposal. It covers such things as proposal format, oral presentations, and the proposal preparation instructions. Proposal preparation instructions can be used to an advantage by requiring the Offerors to submit outlines of how they will conduct SOW tasking. This will assist in understanding the Offeror's technical approach and allow assessment of their understanding of the technical requirements. This will be addressed in detail in Chapter 5 of this guideline.

3.7 SECTION M - EVALUATION FACTORS FOR AWARD

This presents to the bidder the basis of award and how proposals will be evaluated. It should be taken from the Government's proposal evaluation criteria, addressed in Volume 4 of the procurement guideline series.

THIS PAGE INTENTIONALLY LEFT BLANK

4.0 OTHER CONSIDERATIONS

There are other important factors to consider before the RFP language is presented.

4.1 NONMANDATORY REQUIREMENTS AND OPTIONS

An alternative for procurement initiators is to specify non-mandatory requirements. These requirements are placed in the RFP. The bidder may respond to these requirements or choose not to respond. The bidder will not be penalized for not responding or for proposing an unacceptable response. The bidder can, however, gain points if the approach is deemed acceptable by the evaluators.

Non-mandatory requirements and solutions can also be proposed by the bidder if this is allowed by the RFP. Again bidders will not be penalized for not proposing non-mandatory requirements, for proposing unacceptable requirements, for proposing unacceptable solutions, or for proposing unacceptable desirable options or features. They can gain points by proposing acceptable solutions to acceptable requirements, whether these requirements become part of the contract or not.

Options are requirements that may be proposed by the Government, but ones that may not be intended to be purchased at the same time as the rest of the features. The Government may still want these options addressed in the proposal and evaluated as if they were mandatory requirements.

4.2 EVIDENCE AVAILABILITY

Just because a vendor supplies NSA with evidence to support a product evaluation, does not necessarily mean the Government has rights to that documentation. In order to obtain certification evidence, even the identical documents provided for product evaluation, the Government must task the development of the documentation in the Statement of Work and delivery in the CDRL. Of course, only that documentation that is required for certification and operation should be specified.

4.3 DOCUMENTATION COST

The cost for operational security documentation (e.g. Security Feature User's Guide and Trusted Facility Manual) can be incurred within the contract or directly by the Government. A contract cost is incurred if the operational security documentation is specifically called out in the RFP and therefore generated to Government standards by the offeror. The cost would be incurred directly by the Government if the acquiring agency Program Manager intends to develop the documentation internally. This makes the system appear less expensive. Unfortunately, users seldom have the experience and expertise necessary to generate this unique type of documentation. This can lead to cost growth manifested in contract Engineering Change Proposals (ECPs).

4.4 INTERPRETING THE TCSEC

The philosophy of this document is to present the words of the TCSEC in a suitable form for the RFP and then place the responsibility for additions and changes in the hands of the procurement initiator, all the while warning of the pitfalls. The best approach is for the initiator to propose changes and have them reviewed by NSA, or some other equivalent security organization, to assess potential impact. Care must

be taken not to restrict potentially valid solutions when writing the specification or statement of work sections of the RFP.

The features and assurances for a given TCSEC Division/Class are inseparable. If requirements or taskings are eliminated from a specific level of trust, then that level cannot be certified. If requirements are added, existing EPL solutions could be eliminated.

The Trusted Computing Base (TCB) is the totality of protection mechanisms, hardware, software and/or firmware, the collection of which is responsible for enforcing security. The TCB is the trusted part, but not necessarily the total, of the offeror's solution.

5.0 STANDARD SOLICITATION LANGUAGE

To assist the reader, the paragraph numbering that follows is as one might expect to find it in the RFP. This chapter identifies the language to be used in selected, identified sections of the RFP. The paragraphing gets more difficult when there are multiple policies (DOCPs).

Certain conventions are used in this chapter. The words in bold are either words intended for use in the RFP or references to words intended for use in the RFP. For example, bold paragraphs normally reference specific paragraphs of DoD 5200. 28-STD that are suggested for use verbatim in the RFP document. Paragraphs applicable to only a Division/Class range will have that range in parentheses prior to the paragraph or group of paragraphs. Paragraphs in which the Division/Class are absent are applicable to all Divisions/Classes (C2 - A1).

Paragraph designation is complicated and will be explained here. The basis for (but not the actual) paragraph numbering is as follows:

C.m.n.p.q

C.	Section C of the RFP
m.	Applicable DOCP number designator
n.	n = 1 Scope of Contract, n = 2 Operational Specifications, n = 3 TCSEC Specifications, n = 4 TCSEC Statements of Work
p.	Number of topic taken from TCSEC
q.	Item of concern for procurement initiator

In the Section C of this document, for use by the procurement initiator, section m will be omitted because it is strictly an operational determination. Items of concern for the procurement initiator in Section C, paragraph q above, are divided into paragraphs as follows:

a. Scope of Contract (n=1), Operational Specification (n = 2), Text of the Specification (n = 3), or Statement of Work (n = 4) - Taken primarily from the TCSEC, these are words or references to words suggested for inclusion in the RFP. (This will be a repeat of the currently published Volume 2 Guideline.) This is always applicable and is in bold.

b. DOCP Interface Policy Interpretation - Interface policy of this DOCP with respect to every other communicating DOCP shall be presented. This shall represent operational policy for this development determined by the DAA and through agreements with other DAAs.

c. DOCP Global Policy Interpretation - Global policy imposed on this and all other DOCPs shall be presented here. It shall be the operational policy for this procurement and represent agreements with other parts of evolving systems. This is applicable when there is a complex system and the requirement cannot be totally satisfied with the TDI.

d. Trusted Network Interpretation - References to interpretations and other applicable information contained in the TNI document. Applicable to simple (single NTCB) systems or systems where the TNI is applicable to one or more of the TCBs of a complex system.

e. Trusted Database Management Interpretation - References to interpretations and other applicable information contained in the TDI document. Applicable to complex systems where it has been determined to follow the approach of the TDI. Also applicable to a complex system in which one or more of the DOCPs have been or are to be built under the guidelines of the TDI.

f. Important References - These references should be included in the RFP. They are generally guidelines intended to explain and interpret the TCSEC for the bidder. These references will redundantly be contained in the list of references accompanying the RFP. **It is important to emphasize that even though these references are bold and will be contained in the RFP, they are not RFP requirements.**

g. Procurement Considerations - Here, issues are discussed that have arisen in previous procurements or are apt to arise in future procurements. These issues should be considered by the procurement initiator in the context of his/her particular procurement to circumvent possible later contractual or certification problems. These considerations are not complete, but offer guidance based on known experiences. They are not in bold and therefore we do not intend their inclusion in the RFP.

In the section C being constructed by the procurement initiator, his/her paragraphing will be C.m.n.p.q where the q are subsections:

a. Text of the Specification/Statement of Work
b. Interpretation (Not to be considered as a requirement)
c. References (Not to be considered as a requirement)

The standard language and form for the trusted elements of a secure system, along with important discussion, are provided in the remainder of this chapter, organized according to a subset of the sections of the RFP.

SECTION C - DESCRIPTION/SPECIFICATION/WORK STATEMENT

C.1 SCOPE OF CONTRACT (AUTOMATED INFORMATION SYSTEM - EQUIPMENT, SOFTWARE AND MAINTENANCE)

The Contractor shall furnish the equipment, software, documentation, and other contractor work required for installation and support of all items supplied under this contract. Such items shall be supplied in conformance with the terms and conditions of the contract.

C.2 OPERATIONAL SECURITY SPECIFICATIONS

a. Text of the Specification

The bidder shall considered and/or recommend security support other than COMPUSEC, especially physical security, TEMPEST and COMSEC that shall also be used to protect the system.

The system shall be shown to be compatible with all operational security requirements identified, ensuring that there is nothing in the design of the proposed solution to preclude their satisfaction.

b. DOCP Interface Policy Interpretation

(Note: First time readers should skip to section g below for a background on what is discussed here.)

Interface Policy - Policy established for control of data flow between each pair of communicating DOCPs.

Operational requirements pertain, not only to portions of the system being procured, but also for interfacing parts of the system, meaning all existing TCB subsets or DOCPs. This requires addressing boundaries, physical interfaces, and policy interfaces.

There shall be an explicit interface policy considered between each DOCP and every other DOCP with which it communicates. The interface policy can be thought of as an augmentation to the exportation policy of the TCSEC, however, in many cases, both exportation and importation concerns are expressed. The need for a trusted path to share and mediate security variables also should be assessed. In sending data, a DOCP must support intercommunication (exporting) policies established by its division/class.

c. DOCP Global Policy Interpretation

Global Policy - System level requirements to be satisfied by each DOCP (e.g., audit, recovery, and identification/authentication.)

Global considerations pertain to systems for which there can be or has been no accreditation against a well defined global policy such as that stated in the TDI. If TCBs share mechanisms (e . g., identification/authentication or audit) each individual TCB must be certified alone, using that mechanism. The DAA must use the evidence from those certifications to ensure consistency with interface policy between the entities and any less primitive policy of which this shared mechanism is a part.

d. Trusted Network Interpretation

The decision may be made to use the TNI as the basis for development of one or more DOCP. This decision is made and documented initially as operational security policy with the appropriate DOCP, n-tuple, interface policy and global policies developed. Actual interpretations for use in the RFP are referenced in subsequent specifications and statements of work sections of this document.

e. Trusted Database Management Interpretation

The decision may be made to use the TDI as the basis for development of one or more DOCP. This decision is made and documented initially as operational security policy with the appropriate DOCP, n-tuple, interface policy and global policies developed. Actual interpretations for use in the RFP are referenced in subsequent specifications and statements of work sections of this document.

f. Important References

"Use of the Trusted Computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems," NCSC-Technical Report-002, and "Turning Multiple Evaluated Products Into Trusted Systems," NCSC-Technical Report-003.

g. Operational Security Considerations

Terms are introduced that must be understood to understand the DOCP concepts:

Regulatory/Security Policy - Regulations, Directives, and Standards imposed on the development of secure systems. Especially DoDD 5200.28, DoD 5200.28-STD, and DoD 5200.28-M (DRAFT) and regulations developed by individual Agencies and Organizations to satisfy the requirements of those DoD documents.

Operational Security Policy - Design and operational choices that satisfy regulatory security policy. It includes established DOCPs, security parameters (n-tuples), and security rules of operation.

Domains of Constant Policy (DOCPs) - Unique pieces of the system, each with a single policy and an associated TCB. DOCPs are, in general, nonoverlapping subsets of the system, that, in combination, completely cover the system. A DOCP consists of a well-defined boundary (where an isolation mechanism exists or can be employed) and an n-tuple defining security characteristics. (The isolation is required to ensure that communications is taking place only over known, designated channels.) Each DOCP will have a TCB for support of its own security requirements, however, some of the mechanisms (e.g., audit) may be shared with another DOCP. (This is the only exception to the nonoverlapping principal.)

Operational Security Parameter - Values and relations having a security relationship determined by the procurement initiator and the DAA to be requirements imposed on the system design. They include n-tuples. A partial list (excluding n-tuples) includes:

> statement of operational positions and responsibilities of each associated with security,

statement concerning the intended frequency of mechanism integrity checking during operations,

minimum audit functionality to be supported at all times, plus other increasing levels of audit support and rules for their use,

maximum number of users,

intended hours of operations,

hard copy output,

environment for Software Development.

N-tuples - Operational security policy parameters associated with a DOCP used to eventually determine division/class. "n" might be different for different procurements. At least one value of "n" is different for different DOCPs. The n-tuple that represents operational policy can be simple (clearance and classification levels) or complicated (with categories and other parameters). For the purposes of this document, the n-tuple parameters considered to be basic are values of the parameters:

minimum classification of data,

maximum classification of data,

minimum security clearance,

maximum security clearance,

categories (compartments/caveats),

build status (existing, EPL product, to be built), and

level of assurance achieved (e.g., EPL evaluation at some level, certification evaluation at some level, no evaluation, or other).

Those n-tuple parameters considered to be derived are:

risk index,

exposed risk index,

mode, and

division/class.

Thus in this case n = 11, where 7 are basic and 4 derived.

(1) Background

For a simple system where development is only guided by the TCSEC, there is a single set of operational parameter values used to determine a single division/class. Similarly, in a system designed against the TNI, a single division/class is determined.

When we are dealing with TDI, there are the same single set of operational parameters for each TCB subset considered, though the values may be different for each subset. Because of the subset relation, one least primitive subset represents the system from the outside world. The same is true for DOCPs in which for a given complex system the size and definition of the n-tuple parameters are the same across the system, but the values taken on by the n-tuple parameters will be different for different DOCPs. Therefore, the division/class is probably different as well.

(2) Domains of Constant Policy

The approach is used when any or all of the following system characteristics exist: a) complex - the system is made up of systems, b) evolving - part of the system exists and the rest of the system is being added, and c) multipolicy - different parts of the system can have different policies (i.e., applicable division/class).

Divide the complex system into pieces, addressing each piece, like simple systems are now treated with the Trusted Computer System Evaluation Criteria (TCSEC). Each piece, called a domain of constant policy (DOCP), has a single policy (division/class) supported by a single TCB.

Determine division/class using DoDD 5200.28, Enclosure 4. Using the DOCP's associated n-tuple (n operational security policy parameters such as clearances and classifications), a risk index is identified, subject to modification by the Designated Approving Authority (DAA).

Connected DOCPs are subject to cascading risk, requiring a search that considers each pair of potentially intercommunicating DOCPs. Identified risk increases can result in an increased risk index, called exposed risk index. This is a primary factor to determine DOCP division/class. Risk contributing DOCPs are candidates for operational policy changes or added mechanisms.

Optimal operational policy is determined through requirement and design iteration (e.g., seeking lowest affordable risk) and DOCPs are assigned an updated division/class. An interface policy is developed, constraining communications to conform to all security policies, including local policies (e.g., two man rule) and mutual suspicion. Global policy is developed across DOCPs, consistent and mutually supportive in areas such as identification/authentication, audit, and trusted recovery.

(3) Risk Assessment

Exposed Risk Index - An adjusted risk index for a DOCP determined from DoDD 5200.28 [4], Enclosure 4, that considers exposure (cascading risk) from other DOCPs.

Contributed Risk - The summed amount of increase in exposed risk potentially contributed by a single DOCP to all other DOCPs. Two DOCPs could potentially increase the risk index of a third DOCP from its original level (i.e., providing an exposed risk index), but in the analysis technique, only one of the contributing DOCPs actually does. Nevertheless, each of the contributing DOCPs receives an increase in contributed risk.

Solely Contributed Risk - The risk contributed by a DOCP which could not have also been contributed by another, summed across all other potentially contributing DOCPs.

A DOCP and its n-tuple are working entities in the sense that tradeoff decisions concerning policy, costs, and mechanisms may make it necessary to change the operational policy (i.e., the DOCPs and their characteristics). It is only after these adjustments are completed that the derived policy parameters (exposed risk, mode, and TCSEC division/class) are finalized. (Many of the concepts of propagated risk were referenced in NCSC-Technical Report-002.)

A small part of the risk management process for simple systems is the risk assessment procedure identified in DoDD 5200.28, Enclosure 4, that identifies a risk index using some of the operational security policy, with other considerations, to guide the DAA in making adjustments. The same procedure is used for DOCPs with the exception that the cascading risk from intercommunicating DOCPs is also taken into account. Exposure is represented by changes to the operational security parameters (levels or clearances) before enclosure 4 is applied. The exposed risk is a new risk index value called the exposed risk index.

Contributed risk is the summed amount of increase in exposed risk potentially contributed by a single DOCP to all other DOCPs. (Two or more DOCPs could have potentially changed the risk level of yet another DOCP from its original level, but in the analysis technique, only one actually does. Nevertheless, they all receive an increase in contributed risk). Solely contributed risk is the risk contributed by one DOCP which could not have been also contributed by another DOCP .

The exposed risk can be decreased by changing either the local operational policies or the operational policies of the contributing DOCP(s). The contributed risk factors, are an indicator to the DAA where the changing of policy or the implementation of guards may do the most good in reducing the risk of the overall system. This is all done before mechanisms are considered, thus, as you might guess, this is the first of two iterations. The two contributed risk factors (contributed risk and solely contribute risk) help identify to the DAA the areas where changes in operational policy can have the largest risk reduction advantage. The propagated risk assessment is repeated to assess the shared risk aspects of the adjustments.

(4) Protection Assessment

With the operational policy (DOCPs and n-tuples), interface policy, and global policy established, design can be accomplished based on the division/classes chosen. Upgrades to existing architectures will probably involve providing mechanisms to support the global and interface policies. System and TCB isolation may need to be enhanced. Compensation for previously ignored exposed risk may involve manual or automated guards and strict interface control. Some mechanisms may be replaced to take advantage of technology advances. New and replacement designs will take advantage of EPL products where possible.

Besides protection mechanism assessment, there needs to be an assessment of assurance. This includes determining the evaluation rigor used, or planned to be used, in testing and evaluating the DOCP. In both upgrade and new systems with EPL products, a strategy for certification evaluation must be developed that maximizes the use of prior evidence, while not diminishing the quality of the assurance.

It is at this point a second iterative analysis should be undertaken to take into account the success of the proposed mechanisms in meeting the regulatory and operational security policy. It allows reexamination of the process all the way back to the specification of operational policy. The two contributed risk factors (i.e.,

contributed risk and solely contributed risk) again help identify to the DAA the areas where changes in operational policy can have the largest risk and cost reduction advantage. The protection assessment can be reaccomplished considering actual architectural solutions. What remains is a statement of the residual risk within the system. The DAA must determine the acceptability of the risk, and, if required, the process must be reviewed and corrected.

The results of this second iterative analysis may result in updates to the operational security policy and security architectural design. At this point, new development may begin. The operational security policy is used along with regulatory security policy as a basis for certification and accreditation.

C.3 TECHNICAL SPECIFICATIONS

a. Text of the Specification

Detailed technical specifications are found in this section. The glossary and acronyms referenced in Section J and attached to this RFP are considered to be part of this specification.

(For single policy systems, this section should be traversed once using a single division/class. If the TNI is being used in as an interpretation to the TCSEC, then the appropriate division/class entry for the TNI should be considered. If a multipolicy system is being specified, then either the TDI or DOCP will be used. For the TDI, there must be a specification for each TCB subset and a set of corresponding TCSEC specifications, as well as consideration of the appropriate TDI interpretations for the determined division/class. Similarly, if the DOCP approach is being used, then the Interface and Global Policy Specifications must be identified.)

b. DOCP Interface Policy Interpretation

A DOCP has two interface responsibilities: 1) it must ensure that data it sends continues to be supported by the policies imposed on it and 2) it must appropriately handle data it receives based on any policy information known about that data.

The policy can be discretionary and/or mandatory and includes categories (compartments, caveats, need to know). The responsibility for establishing the policy, linking it to the data, and assuring proper understanding by the receiver is required of the sender. Policy can be preestablished based on data identification through DOCP agreements, it can be communicated via labels, or it can be communicated and implemented manually by security administrators.

Sending DOCPs must be assured that data is being released into a system that can be trusted to interpret and carry out the policy. Factors to consider include the potential for eavesdropping, spoofing, or policy alteration.

Once data is in the possession of a receiving DOCP, it becomes the responsibility of that TCB to impose its knowledge of the policy on that data and treat it accordingly. Suspected or actual violations of interface policy must be treated as a special case and the data protected.

A DOCP may not be affordably and certifiably able to support division/class increases determined by considering exposed risk. Special communications mechanisms or added protection features within the potential receiving DOCP may help to ameliorate this situation (i.e., decrease the exposed risk). This can provide an operational solution that must be agreed to by the potentially sending DOCP. In any case, the DAA from the sending DOCP ultimately has responsibility for the decision.

In a policy of mutual suspicion, a sending DOCP must establish interface policy consistent with the level of trust it has established for potential receiving DOCPs. If the level of trust determined does not coincide with the certification and/or accreditation level given that DOCP, the sending DOCP should further restrict the communication policy, beyond that normally implied by the TCSEC and its interpretations to a level where the sending DOCP is willing to accept the remaining risk. Similarly, if a receiving DOCP cannot trust the content or policy associated with data provided by another DOCP, then a receipt and handling policy must be

established consistent with the risk the receiving DOCP is willing to accept. This policy may be more restrictive than that required by the TCSEC and its interpretations.

c. DOCP Global Policy Interpretation

To be secure, either there shall be no sharing between DOCPs of discretionary controlled data, the entire connected system should satisfy a single previously established discretionary access control policy, it must be accomplished by sharing access control mechanisms, or DOCPs must share access control information between mechanisms, ensuring a secure protection and a system that cannot be defeated because of time lags and communications threats. In older systems that do not allow subjects to access objects in other systems, this requirement is often satisfied because only standard messages are formatted and allowed to be transmitted. In these cases the subjects do not have access to objects beyond the scope of their own TCB.

Even if each TCB has its own data for identification and authentication, the information for individual users that may potentially request access in more than one TCB or may have access to objects in more than one TCB, must be consistent. The individual cannot assume more than one identity or be performing two functions simultaneously (unless the system security has accounted for such support). There must be a way to associate audit records generated by different TCBs for the same Individual subject.

Someone must be assigned the authority and assume the responsibility of security administrator for each of the TCBs. In addition, a security administrator must represent the authority of each hierarchical stage of DAAs.

Implications of failure of one of the component TCBs must be reviewed from the standpoint of impact to all of the other intercommunicating entities. A way to cooperatively shut down and recover in a secure manner must exist.

TCBs following the subsetted TCB principles set forth by the TDI need not be concerned with additional interface and global policies beyond those stated within the TDI.

d. Trusted Network Interpretation

The specific Trusted Network Interpretations to topics of the Trusted Computer System Evaluation Criteria are referenced in their entirety in the specifications and statements of work.

e. Trusted Database Management Interpretation

The specific Trusted Database Management System Interpretations to topics of the Trusted Computer System Evaluation Criteria are referenced in their entirety in the specifications and statements of work.

f. Important References

"Use of the Trusted Computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems," (NCSC-Technical Report-002). Also, "Turning Multiple Evaluated Products Into Trusted Systems," (NCSC-Technical Report-003).

g. Technical Specifications Considerations

(None)

C.3.1 DISCRETIONARY ACCESS CONTROL SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.1.1.

For Class B1, repeat TCSEC Section 3.1.1.1.

For Class B2, repeat TCSEC Section 3.2.1.1.

For Class B3, repeat TCSEC Section 3.3.1.1.

For Class A1, repeat TCSEC Section 4.1.1.1.)

b. DOCP Interface Policy Interpretation

The interface policy for discretionary access control depends greatly on the specific implementation. If the objects involved remain under strict control of the single TCB (i.e., DOCP) and are not passed on to other DOCPs, The policy can be shown to be satisfied. If the object contents are shared, then communicating DOCPs must also support the policy. If the policy remains constant, then this can be handled procedurally. The most difficult situation is that in which the discretionary policy varies, that is the access control matrix is updated and that result must be updated in one, several, or all DOCPs over a trusted path.

c. DOCP Global Policy Interpretation

The alternative to a complicated interface policy is to define a global policy that can be shown to be supported by each of the DOCP TCBs. Further, through the discretionary policy, the positions of access of each of the subjects can be controlled. Again this may be a solution for an existing, evolving system, but is less desirable for a multi user, general purpose system using object oriented sophisticated off-the-shelf software capabilities.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator:

For Class C2, TNI Section 2.2.1.1 applies.

For Class B1, TNI Section 3.1.1.1 applies.

For Class B2, TNI Section 3.2.1.1 applies.

For Class B3, TNI Section 3.3.1.1 applies.

For Class A1, TNI Section 4.1.1.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.1 and IR-2.1.1 applies.

For Class C2, TDI Appendix A Section C2-1.1 applies.

For Class B1, TDI Appendix A Section B1-1.1 applies.

For Class B2, TDI Appendix A Section B2-1.1 applies.

For Class B3, TDI Appendix A Section B3-1.1 applies.

For Class A1, TDI Appendix A Section A1-1.1 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-003, "A Guide to Understanding Discretionary Access Control in Trusted Systems," September 30, 1987.

g. Discretionary Access Control Procurement Considerations

Unauthorized users include both those not authorized to use the system and legitimate users not authorized to access a specific piece of information being protected.

"Users" do not include "operators," "system programmers," "Security Officers," and other system support personnel. The latter are distinct from users and are subject to the Trusted Facility Management and the System Architecture requirements.

Deletion of subjects (e.g., users) and objects (e.g., data) is a potential problem. The mechanism should handle the deletion effectively, making certain that dangling references do not grant unintended access.

The ability to assign access permissions to an object by a user should be controlled with the same precision as the ability to access the objects themselves. Four basic models for control exist: hierarchical, concept of ownership, laissez-faire, and centralized. These are discussed in NCSC-TG-003.

The TCB should enforce need-to-know access restrictions placed on information managed by the information system. The need-to-know access restrictions for the information, when created or changed, should be determined by the office of primary responsibility or the originator of the information. Only users determined to have appropriate clearances in addition to required "need-to-know" for information should be allowed to access the information.

The design must consider that discretionary access control is usually used for both user access control and system access control. For example, the system may contain several types of objects (known as public objects) that are designed to be read by all users, or executed by all users, but allowing only trusted subjects modification privileges.

Discretionary access control will not stop Trojan horses. An attacker can trick a more privileged user to run a program containing his Trojan horse, that in turn copies the user access files to the attackers address space. Trojan horses are addressed in NCSC-TG-003.

The Commercial-Off-The-Shelf (COTS) systems may vary with respect to the granularity of objects to which discretionary access control is applied. Generally, they are organized to provide Discretionary Access Control (DAC) at the file level or at the application level. Database design can often handle the cases when a different level of granularity is desired by the procuring agency so that EPL products can apply. The procuring agency should take particular care, whenever possible, to write RFP specifications for DAC that can be met by at least some existing commercially available products. (This is further addressed in Volume 1, Chapter 3)

C.3.2 OBJECT REUSE SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.1.2.

For Class B1, repeat TCSEC Section 3.1.1.2.

For Class B2, repeat TCSEC Section 3.2.1.2.

For Class B3, repeat TCSEC Section 3.3.1.2.

For Class A1, repeat TCSEC Section 4.1.1.2.)

b. DOCP Interface Policy Interpretation

Since, by definition, there is no part of the system which is not a part of a DOCP, a physical interconnection is either part of the DOCP at one end of the connection or at the other end of the connection or it is a DOCP all by itself. Therefore, storage objects must meet the requirements of the corresponding division/class and therefore its object reuse requirements.

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.1.2 applies.

For Class B1, TNI Section 3.1.1.2 applies.

For Class B2, TNI Section 3.2.1.2 applies.

For Class B3, TNI Section 3.3.1.2 applies.

For Class A1, TNI Section 4.1.1.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.2 and IR-2.1.2 applies.

For Class C2, TDI Appendix A Section C2-1.2 applies.

For Class B1, TDI Appendix A Section B1-1.2 applies.

For Class B2, TDI Appendix A Section B2-1.2 applies.

For Class B3, TDI Appendix A Section B3-1.2 applies.

For Class A1, TDI Appendix A Section A1-1.2 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-025, "A Guide to Understanding Data Remanence in Automated Information Systems," September 1991.

NCSC-TG-018, "A Guide to Understanding Object Reuse in Trusted Systems," July, 1992.

g. Object Reuse Procurement Considerations

The purpose of object reuse mechanisms is to prevent disclosure of sensitive information by ensuring that residual information is no longer available. This objective can be achieved by clearing objects either upon allocation or deallocation.

Object reuse is a concern when an object is not fully allocated, that is, the granularity is larger than the data. The object reuse requirement must be satisfied based on the object size, not the data allocation.

C.3.3 LABELS SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.

For Class B2, repeat TCSEC Section 3.2.1.3.

For Class B3, repeat TCSEC Section 3.3.1.3.

For Class A1, repeat TCSEC Section 4.1.1.3.)

b. DOCP Interface Policy Interpretation

The interface policy must be implemented so as to satisfy the labels policy directly or by demonstrating the equivalence of the implementation. The contents of labels is a subset of the information that must accompany data communicated. The solution to an existing evolving system may involve use of a trusted path for security interface information. Interface data may be required to satisfy the discretionary policy or other special (e.g., two man rule) policies, and therefore be required at C2, as well as higher, division/classes.

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3 applies.

For Class B2, TNI Section 3.2.1.3 applies.

For Class B3, TNI Section 3.3.1.3 applies.

For Class A1, TNI Section 4.1.1.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3 applies.

For Class B2, TDI Appendix A Section B2-1.3 applies.

For Class B3, TDI Appendix A Section B3-1.3 applies.

For Class A1, TDI Appendix A Section A1-1.3 applies.)

f. Important References

(None)

g. Labels Procurement Considerations

The tranquility principle states that the security level of an object cannot change while the object is being processed by a system. The same can be stated about changes to security clearances. This is a critical area, both from the standpoint of changes only being invocable by an authorized individual under the direct control of the TCB, and ensuring the system cannot be spoofed when such changes are being made.

Labeling of data is not used solely to control classified information. The mandatory policy can also be used for unclassified sensitive or privacy applications.

A distinction must be made between objects that are explicitly labeled and those that are implicitly labeled. For example, a labeled file may contain many tuples or records mediated by the reference monitor.

Internal TCB variables that are not visible to untrusted subjects need not be labeled, provided they are not directly or indirectly accessible by subjects external to the TCB. However, it is important to understand that such internal variables can function as covert signaling channels when untrusted subjects are able to detect changes in these variables by observing system behavior.

C.3.4 LABEL INTEGRITY SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.1.

For Class B2, repeat TCSEC Section 3.2.1.3.1.

For Class B3, repeat TCSEC Section 3.3.1.3.1.

For Class A1, repeat TCSEC Section 4.1.1.3.1.)

b. DOCP Interface Policy Interpretation

The integrity requirement applies to any interface information transmitted to define physical and logical interface.

c. DOCP Global Policy Interpretation

Shared label interpretation between DOCPs must be identical through use of identical labels and software or through carefully planned transformations that can be shown to provide identical interpretation results.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3.1 applies.

For Class B2, TNI Section 3.2.1.3.1 applies.

For Class B3, TNI Section 3.3.1.3.1 applies.

For Class A1, TNI Section 4.1.1.3.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3.1 applies.

For Class B2, TDI Appendix A Section B2-1.3.1 applies.

For Class B3, TDI Appendix A Section B3-1.3.1 applies.

For Class A1, TDI Appendix A Section A1-1.3.1 applies.)

f. Important References

(None)

g. Label Integrity Procurement Considerations

Care is needed when specifying the means of binding an object and its label. A cryptographic mechanism is one of many approaches adequate to provide assurance of the binding since the relationship and content are preserved, and there is protection from disclosure.

The form of internal sensitivity labels may differ from their external (exported) form, but the meaning must be retained.

C.3.5 EXPORTATION OF LABELED INFORMATION SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.2.

For Class B2, repeat TCSEC Section 3.2.1.3.2.

For Class B3, repeat TCSEC Section 3.3.1.3.2.

For Class A1, repeat TCSEC Section 4.1.1.3.2.)

b. DOCP Interface Policy Interpretation

The exportation requirement should be satisfied as part of the interface policy requirement. Depending on the discretionary policy and other policy requirements, special designation of a channel or device may go beyond the single-level, multi-level considerations. Shared channels or devices must consider security of one DOCP with respect to the co-using DOCPs.

c. DOCP Global Policy Interpretation

Labels and label interpretation between DOCPs shall be identical or transformed to provide identical interpretation.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3.2 applies.

For Class B2, TNI Section 3.2.1.3.2 applies.

For Class B3, TNI Section 3.3.1.3.2 applies.

For Class A1, TNI Section 4.1.1.3.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3.2 applies.

For Class B2, TDI Appendix A Section B2-1.3.2 applies.

For Class B3, TDI Appendix A Section B3-1.3.2 applies.

For Class A1, TDI Appendix A Section A1-1.3.2 applies.)

f. Important References

(None)

g. Exportation of Labeled Information Procurement Considerations

Changes in designation should be made by a properly authorized individual, normally the System Administrator, considering the tranquility principle. Such changes are auditable.

C.3.6 EXPORTATION TO MULTI LEVEL DEVICES SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.2.1.

For Class B2, repeat TCSEC Section 3.2.1.3.2.1.

For Class B3, repeat TCSEC Section 3.3.1.3.2.1.

For Class A1, repeat TCSEC Section 4.1.1.3.2.1.)

b. DOCP Interface Policy Interpretation

The interface policy shall support the multilevel exportation device specification. A device supported by more than one DOCP shall be shown to satisfy the requirements of each DOCP while simultaneously supporting the requirements of the others. The solution may involve use of isolation mechanisms with different dedicated modes depending on the DOCP.

c. DOCP Global Policy Interpretation

A global policy involving the unique assignment of devices to a single DOCP at one time might be considered as a feasible solution.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3.2.1 applies.

For Class B2, TNI Section 3.2.1.3.2.1 applies.

For Class B3, TNI Section 3.3.1.3.2.1 applies.

For Class A1, TNI Section 4.1.1.3.2.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3.2 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3.2 applies.

For Class B2, TDI Appendix A Section B2-1.3.2 applies.

For Class B3, TDI Appendix A Section B3-1.3.2 applies.

For Class A1, TDI Appendix A Section A1-1.3.2 applies.)

f. Important References

(None)

g. Exportation to Multilevel Devices Procurement Considerations

The sensitivity label of an object imported to a multilevel device must be within the range of the device and considered to be accurate by the TCB. It is considered to be accurate because it has been protected by the security mechanisms of the environment through which it has traversed before it reaches the multilevel device.

C.3.7 EXPORTATION TO SINGLE LEVEL DEVICES SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.2.2.

For Class B2, repeat TCSEC Section 3.2.1.3.2.2.

For Class B3, repeat TCSEC Section 3.3.1.3.2.2.

For Class A1, repeat TCSEC Section 4.1.1.3.2.2.)

b. DOCP Interface Policy Interpretation

The interface policy shall support the single-level exportation device specification. A device supported by more than one DOCP shall be shown to satisfy the requirements of each DOCP while simultaneously supporting the requirements of the others. The solution may involve use of isolation mechanisms with different dedicated modes depending on the DOCP.

c. DOCP Global Policy Interpretation

A global policy involving the unique assignment of devices to a single DOCP at one time might be considered as a feasible solution.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3.2.2 applies.

For Class B2, TNI Section 3.2.1.3.2.2 applies.

For Class B3, TNI Section 3.3.1.3.2.2 applies.

For Class A1, TNI Section 4.1.1.3.2.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3.2 applies.

For Class B2, TDI Appendix A Section B2-1.3.2 applies.

For Class B3, TDI Appendix A Section B3-1.3.2 applies.

For Class A1, TDI Appendix A Section A1-1.3.2 applies.)

f. Important References

(None)

g. Exportation to Single-level Devices Procurement Considerations

Sometimes operational use of a single level device is actually to be at one level for a period of time and then to switch to another level. Here it is wise to employ labels. If labels are not used then tranquility must be observed during configuration changes with a positive action to ensure the level of the device is known to users and observed by the reference validation mechanism.

C.3.8 LABELING HUMAN-READABLE OUTPUT SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.3.2.3.

For Class B2, repeat TCSEC Section 3.2.1.3.2.3.

For Class B3, repeat TCSEC Section 3.3.1.3.2.3.

For Class A1, repeat TCSEC Section 4.1.1.3.2.3.)

b. DOCP Interface Policy Interpretation

Where the data is formatted for a human readable output device, the human-readable output requirement shall be included as part of the interface policy requirement.

c. DOCP Global Policy Interpretation

DOCPs receiving data in human-readable output form shall be expected to be formatted for human-readable output with classification, category and caveat markings.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.1.3.2.3 applies.

For Class B2, TNI Section 3.2.1.3.2.3 applies.

For Class B3, TNI Section 3.3.1.3.2.3 applies.

For Class A1, TNI Section 4.1.1.3.2.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B1, TDI Appendix A Section B1-1.3.2.3 applies.

For Class B2, TDI Appendix A Section B2-1.3.2.3 applies.

For Class B3, TDI Appendix A Section B3-1.3.2.3 applies.

For Class A1, TDI Appendix A Section A1-1.3.2.3 applies.)

f. Important References

(None)

g. Labeling Human-Readable Output Procurement Considerations

The System Administrator specifies the printed or displayed sensitivity label that is to be associated with exported information. The TCB is required to mark the beginning and end of all human-readable, paged, hard-copy output with sensitivity labels that properly represent the sensitivity of the output. This helps users protect data they are using.

C.3.9 SUBJECT SENSITIVITY LABELS SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.1.3.3.

For Class B3, repeat TCSEC Section 3.3.1.3.3.

For Class A1, repeat TCSEC Section 4.1.1.3.3.)

b. DOCP Interface Policy Interpretation

The interface policy shall identify when one DOCP has the capability for change in the security level associated with a user and requires action or notification of that user by another DOCP.

c. DOCP Global Policy Interpretation

At B2 and above, the TCSEC requires the following:

The TCB shall immediately notify a terminal user of each change in the security level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity level.

For complex systems, the user interface could be to a DOCP that does not support a mandatory access control policy. Thus, a change noted by a DOCP that does support such a policy would have to be relayed to the user, possibly through cooperative action of the full sequence of DOCPs. Similarly, a request by a terminal user for the complete sensitivity level could be initially received by a DOCP that does not support a mandatory access control policy and will require cooperation between DOCPs to determine the complete subject sensitivity level and to provide that information to the requesting user.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.1.3.3 applies.

For Class B3, TNI Section 3.3.1.3.3 applies.

For Class A1, TNI Section 4.1.1.3.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B2, TDI Appendix A Section B2-1.3.3 applies.

For Class B3, TDI Appendix A Section B3-1.3.3 applies.

For Class A1, TDI Appendix A Section A1-1.3.3 applies.)

f. Important References

(None)

g. Subject Sensitivity Labels Procurement Considerations

(None)

C.3.10 DEVICE LABELS SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.1.3.4.

For Class B3, repeat TCSEC Section 3.3.1.3.4.

For Class A1, repeat TCSEC Section 4.1.1.3.4.)

b. DOCP Interface Policy Interpretation

There shall be labels associated with each physically connected DOCP and a label associated with each logically connected DOCP. That label shall be used for enforcement of the interface policy of the DOCP with respect to each intercommunicating DOCP.

c. DOCP Global Policy Interpretation

Labels along with building and interpreting software shall be identical between DOCPs or it shall be shown that transformation formats and software produce identical interpretation.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.1.3.4 applies.

For Class B3, TNI Section 3.3.1.3.4 applies.

For Class A1, TNI Section 4.1.1.3.4 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.3 and IR-3 applies.

For Class B2, TDI Appendix A Section B2-1.3.4 applies.

For Class B3, TDI Appendix A Section B3-1.3.4 applies.

For Class A1, TDI Appendix A Section A1-1.3.4 applies.)

f. Important References

(None)

g. Device Labels Procurement Considerations

(None)

C.3.11 MANDATORY ACCESS CONTROL SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.1.4.

For Class B2, repeat TCSEC Section 3.2.1.4.

For Class B3, repeat TCSEC Section 3.3.1.4.

For Class A1, repeat TCSEC Section 4.1.1.4.

Also Section 9.0 of the TCSEC should be repeated in the specification portion of the RFP verbatim.)

b. DOCP Interface Policy Interpretation

The interface policy shall be shown to uphold the mandatory policy of each DOCP and, if different, to be more conservative to account for mutual suspicion.

c. DOCP Global Policy Interpretation

Mandatory policy shall support hierarchical classification according to the rules established by the Bell-La Padula model. Categories that are defined at one DOCP shall be shown to be supported by interpretation software or conservatism in data transmittal so that the mandatory policy is shown to be supported throughout the system.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.1.4 applies.

For Class B3, TNI Section 3.3.1.4 applies.

For Class A1, TNI Section 4.1.1.4 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.1.4 and IR-2.1.4 applies.

For Class B2, TDI Appendix A Section B2-1.4 applies.

For Class B3, TDI Appendix A Section B3-1.4 applies.

For Class A1, TDI Appendix A Section A1-1.4 applies.)

f. Important References

(None)

g. Mandatory Access Control Procurement Considerations

(None)

C.3.12 IDENTIFICATION AND AUTHENTICATION SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.2.1.

For Class B1, repeat TCSEC Section 3.1.2.1.

For Class B2, repeat TCSEC Section 3.2.2.1.

For Class B3, repeat TCSEC Section 3.3.2.1.

For Class A1, repeat TCSEC Section 4.1.2.1.)

b. DOCP Interface Policy Interpretation

Trusted paths shall be used at all division classes to provide TCBs to relay authentication data. Public key cryptography shall be considered as an isolation mechanism to protect authentication data.

c. DOCP Global Policy Interpretation

The identification and authentication requirements in the TCSEC address the need to correctly associate authorizations with subjects. In a system made of several DOCPs,

it is possible that only one of several DOCPs will provide identification and authentication, which will be used by other DOCPs. Alternatively, identification and authentication may be provided directly in more than one DOCP. In either case, the DOCPs have to work cooperatively to use identification and authentication data for uniquely identifying users and for associating users with auditable actions.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.2.1 applies.

For Class B1, TNI Section 3.1.2.1 applies.

For Class B2, TNI Section 3.2.2.1 applies.

For Class B3, TNI Section 3.3.2.1 applies.

For Class A1, TNI Section 4.1.2.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.2.1 and IR-2.2.1 applies.

For Class C2, TDI Appendix A Section C2-2.1 applies.

For Class B1, TDI Appendix A Section B1-2.1 applies.

For Class B2, TDI Appendix A Section B2-2.1 applies.

For Class B3, TDI Appendix A Section B3-2.1 applies.

For Class A1, TDI Appendix A Section A1-2.1 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

CSC-STD-002-85, "Department of Defense (DoD) Password Management Guideline," April 12, 1985.

NCSC-TG-017, "A Guide to Understanding Identification and Authentication in Trusted Systems," September 1, 1991.

g. Identification and Authentication Procurement Considerations

(This subject is discussed in Volume 1 Chapter 3 of the Procurement Guideline Series.)

Technology has provided techniques and products that vary greatly in terms of reducing attack risk while satisfying these requirements. The procurement initiator should ensure that the solution that satisfies the requirements is also state-of-the-art in level of protection and consistent with the requirements of this particular application.

To be effective, authentication mechanisms must uniquely and unforgeably identify an individual. Identification and authentication data is vulnerable to interception by an intruder interposed between a user and the TCB. Compromise may result from mishandling off-line versions of the data (e.g.,backup files, fault induced system dumps, or listings). Even a one-way encrypted file can be compared with an encryption dictionary of probable authentication data, if the encryption algorithm and key are known.

(B1 - A1) Authorizations include functional roles assigned to individuals. Most roles can only be occupied by one person at a time. A role has its own set of authorizations that are normally different than the authorizations given to the individuals who can assume the role. An individual should not be allowed to assume a role and operate as an individual at the same time.

If passwords are to be used, an automatic password generator is strongly recommended. If users are allowed to pick their own specific authenticators, their behavior is stereotypical enough to permit guessing or reproducing. Password generators are available that have been endorsed by NSA and can be obtained as Government off-the-shelf items.

Password aging is an important consideration that can be enforced administratively or by the identification/authentication function.

Smart cards and biometric approaches are effective, especially when they augment a password approach.

Whenever the subject is an operating computer program (i.e., a process), that process shall be directly associated with just one individual user, i.e., the person being served by the process. If the process is a system-owned process (e.g., a background process such as a print spooler), the person associated with the process is generally considered to be the Security Officer, the System Administrator, or the operator who initiated the process. The security level and other subject data that can influence access decisions shall be within the range of personnel security clearances associated with the individual user.

C.3.13 TRUSTED PATH SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.2.1.1.

For Class B3, repeat TCSEC Section 3.3.2.1.1.

For Class A1, repeat TCSEC Section 4.1.2.1.1.)

b. DOCP Interface Policy Interpretation

At B2, the only required uses of trusted path are login and authentication. At B3 and above, occasions "when a positive TCB-to-user connection is required (e.g., login, change subject security level)" are included. In both cases, a system designer may choose to use trusted path for situations where the security-relevant event could be recognized or handled in more than one DOCP subset. On those occasions, the careful coordination of all the involved DOCPs in the correct handling of trusted path situations must be shown. If a single DOCP implements trusted path and all the invocations of trusted path are limited to that DOCP (that is, the flow of control in responding to a trusted path initiation never leaves the DOCP until the response is complete), then nothing further would be required.

c. DOCP Global Policy Interpretation

The description of the limitation of trusted path to a single DOCP will suffice for the global part of the requirement, leaving only the demonstration of local satisfaction of the requirement by the identified DOCP.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.2.1.1 applies.

For Class B3, TNI Section 3.3.2.1.1 applies.

For Class A1, TNI Section 4.1.2.1.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.2 and IR-2.2 applies.

For Class B2, TDI Appendix A Section B2-2.1.1 applies.

For Class B3, TDI Appendix A Section B3-2.1.1 applies.

For Class A1, TDI Appendix A Section A1-2.1.1 applies.)

f. Important References

(None)

g. Trusted Path Procurement Considerations

It is important to note that the intent is to protect identification and authentication data at the B2 level, while at the B3 and A1 levels all intercommunications between the TCB and the user can be protected.

Technology is providing products that greatly reduce the possibility of successful attacks involving the trusted path. The procurement initiator should ensure that the solution that satisfies the requirements is also state-of-the-art in level of protection.

C.3.14 AUDIT SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.2.2.

For Class B1, repeat TCSEC Section 3.1.2.2.

For Class B2, repeat TCSEC Section 3.2.2.2.

For Class B3, repeat TCSEC Section 3.3.2.2.

For Class A1, repeat TCSEC Section 4.1.2.2.)

b. DOCP Interface Policy Interpretation

The interface policy shall accommodate the passage of audit data over a trusted path between DOCPs as may be required by the global policy.

c. DOCP Global Policy Interpretation

If each of several DOCPs meets the audit requirements locally, then there is the issue of whether the set of audit records meets the requirements of being able to note and record individual user actions, and at B3 and above, to be able to initiate required action. If not all the DOCPs meet the audit requirements locally, then the requirements must be satisfied by the cooperative action of the set of DOCPs. In both cases, consideration of the audit characteristics of all the DOCPs has to be part of determining that the entire system meets the strictest TCB audit requirements.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.2.2 applies.

For Class B1, TNI Section 3.1.2.2 applies.

For Class B2, TNI Section 3.2.2.2 applies.

For Class B3, TNI Section 3.3.2.2 applies.

For Class A1, TNI Section 4.1.2.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.2.2 and IR-2.2.2 applies.

For Class C2, TDI Appendix A Section C2-2.2 applies.

For Class B1, TDI Appendix A Section B1-2.2 applies.

For Class B2, TDI Appendix A Section B2-2.2 applies.

For Class B3, TDI Appendix A Section B3-2.2 applies.

For Class A1, TDI Appendix A Section A1-2.2 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-001, "A Guide to Understanding Audit in Trusted Systems," June 1, 1988.

g. Audit Procurement Considerations

The option should exist that either some maximum of security related activities be audited or that the System Administrator select events to be audited based on overhead considerations.

An audit control switch available to the System Administrator can allow selection of audit levels, but never to allow less than some required minimum as determined by the DAA.

A requirement exists that authorized personnel shall be able to read all events recorded on the audit trail. A selection option is required that may either be a preselection or a post selection-option. The preselection option limits the audit data recorded. The post selection option reduces the data analyzed from that recorded.

Switches and options must not violate the requirements and intent of the TCSEC.

The audit information should be sufficient to reconstruct a complete sequence of security related events. Audit analysis tools can greatly enhance the efficiency of the audit control function for the System Administrator. (See NCSC-TG-001 for further discussion.)

The capability should be provided to prevent System Administrator and Security Officer functions from turning off auditing or modifying those results.

Only the System Administrator or Security Officer should be able to select what is to be audited from other events.

(B3 - A1) The requirement to "monitor the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy" is subject to interpretation. It is the topic of an entire subfield of security known as

intrusion detection. The DAA must determine what is reasonable in the context of the particular application.

(B3 - A1) "If the occurrence or accumulation of these security relevant events continues, the system shall take the least disruptive action to terminate the event." The approach taken is very application peculiar and the DAA must further specify the action to be taken.

C.3.15 SYSTEM ARCHITECTURE SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.3.1.1.

For Class B1, repeat TCSEC Section 3.1.3.1.1.

For Class B2, repeat TCSEC Section 3.2.3.1.1.

For Class B3, repeat TCSEC Section 3.3.3.1.1.

For Class A1, repeat TCSEC Section 4.1.3.1.1.)

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

For many of the system architecture requirements, demonstrating that a requirement is satisfied by all of the constituent DOCPs is sufficient to demonstrate that it is satisfied for the composite system. The requirements for the "TCB [to] maintain a domain for its execution" and for the TCB to "maintain process isolation through the provision of distinct address spaces" could be satisfied by the composite DOCP TCBs without each constituent DOCP TCB meeting the requirement.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.3.1.1 applies.

For Class B1, TNI Section 3.1.3.1.1 applies.

For Class B2, TNI Section 3.2.3.1.1 applies.

For Class B3, TNI Section 3.3.3.1.1 applies.

For Class A1, TNI Section 4.1.3.1.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-5 applies.

For Class C2, TDI Appendix A Section C2-3.1.1 applies.

For Class B1, TDI Appendix A Section B1-3.1.1 applies.

For Class B2, TDI Appendix A Section B2-3.1.1 applies.

For Class B3, TDI Appendix A Section B3-3.1.1 applies.

For Class A1, TDI Appendix A Section A1-3.1.1 applies.)

f. Important References

(None)

g. System Architecture Procurement Considerations

"Domain" as used in the TCSEC refers to the set of objects a subject has the ability to access. It is, for example, the protection environment in which a process is executing. Domain is sometimes also called "context" or "address space."

Protection granularity can be an issue. Finer granularity (e.g., a few bytes) is ideal for providing precise control (down to the byte or word level), but requires a significant amount of computer overhead to maintain. The trade-off usually made is to have coarser granularity (e.g., 1024 byte blocks) to reduce hardware complexity and retain acceptable performance. (See Volume 1, Chapter 3 of this Guideline Series.)

An important consideration is sensitivity label mapping to protection domain mechanisms. Hardware features (usually called "keys") allow the TCB to associate specific hardware "registers" with the main memory areas (domains) they are protecting. There should be sufficient types and numbers of "registers" to ensure the number of sensitivity labels for information in the system can be adequately mapped. Common ways to achieve these capabilities are through "Descriptor Based Registers," "Bounds Registers," and "Virtual Memory Mapping Registers," although other approaches may also be used.

Asynchronous events are not predictable (e.g., arrival of a message, the printer running out of paper, or communications link errors). Asynchronous event mechanisms are hardware features that handle the unpredictable, usually by "interrupting" the processor. Once interrupted, the processor then deals with the event. Interpretation of DoD 5200.28-STD will probably require hardware features that will cause the processor to recognize and respond to specific asynchronous events, such as "security policy violations" (in DoD 5200.28-STD phrasing, violations of the Simple Security Property or Star Property). Unless hardware features support these properties, software must interpret the results of every operation, causing a severe performance penalty. The penalty may come into conflict with mission performance requirements.

C.3.16 SYSTEM INTEGRITY SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.3.1.2.

For Class B1, repeat TCSEC Section 3.1.3.1.2.

For Class B2, repeat TCSEC Section 3.2.3.1.2.

For Class B3, repeat TCSEC Section 3.3.3.1.2.

For Class A1, repeat TCSEC Section 4.1.3.1.2.)

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.3.1.2 applies.

For Class B1, TNI Section 3.1.3.1.2 applies.

For Class B2, TNI Section 3.2.3.1.2 applies.

For Class B3, TNI Section 3.3.3.1.2 applies.

For Class A1, TNI Section 4.1.3.1.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.2 applies.

For Class C2, TDI Appendix A Section C2-3.1.2 applies.

For Class B1, TDI Appendix A Section B1-3.1.2 applies.

For Class B2, TDI Appendix A Section B2-3.1.2 applies.

For Class B3, TDI Appendix A Section B3-3.1.2 applies.

For Class A1, TDI Appendix A Section A1-3.1.2 applies.)

f. Important References

(None)

g. System Integrity Procurement Considerations

System integrity requirements must be satisfied in the operational system, not just demonstrated as part of test. The DAA shall establish the frequency with which system integrity validation must be accomplished and it should be incorporated into procedural security.

C.3.17 COVERT CHANNEL SPECIFICATIONS

a. Text of the Specification

(For B2 through A1) Wherever possible, covert channels identified by the covert channel analysis with bandwidths that exceed a rate of one bit in ten seconds, shall be eliminated or the TCB shall provide the capability to audit their use.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.3.1.3 applies.

For Class B3, TNI Section 3.3.3.1.3 applies.

For Class A1, TNI Section 4.1.3.1.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.3 applies.

For Class B2, TDI Appendix A Section B2-3.1.3 applies.

For Class B3, TDI Appendix A Section B3-3.1.3 applies.

For Class A1, TDI Appendix A Section A1-3.1.3 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

For Class B2, TCSEC Section 3.2.3.1.3.

For Class B3, TCSEC Section 3.3.3.1.3.

For Class A1, TCSEC Section 4.1.3.1.3.

TCSEC Section 8.0, A Guideline on Covert Channels.

g. Covert Channel Considerations

The TCSEC only requires the analysis of covert channels, tradeoffs involved in restricting the channels, and identification of the auditable events that may be used in the exploitation of known channels. Here it requires that some action be taken for correcting them. The procurement initiator should clearly specify in the RFP what will be expected of a contractor. Proposal evaluation should further determine what is intended by the bidder. This issue must be clearly understood by the Government and the bidder and documented in the specification before an award is made.

Covert Channel auditing and control mechanisms can vary widely from one system to another. In general, the ability to meet both performance and security requirements increases as the security protection mechanisms become more flexible.

C.3.18 TRUSTED FACILITY MANAGEMENT SPECIFICATIONS

a. Text of the Specification

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the specification portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.3.1.4.

For Class B3, repeat TCSEC Section 3.3.3.1.4.

For Class A1, repeat TCSEC Section 4.1.3.1.4.)

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

The ability to run a trusted system facility properly applies to the combination of DOCP TCBs. This requirement can be met across several DOCPs and be shown to apply to all of the composing DOCPs provided the individual DOCPs meet the requirement and the interactions between the DOCPs at the facility management level are clear.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.3.1.4 applies.

For Class B3, TNI Section 3.3.3.1.4 applies.

For Class A1, TNI Section 4.1.3.1.4 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.4 applies.

For Class B2, TDI Appendix A Section B2-3.1.4 applies.

For Class B3, TDI Appendix A Section B3-3.1.4 applies.

For Class A1, TDI Appendix A Section A1-3.1.4 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-015, "A Guide to Understanding Trusted Facility Management," October 18, 1989.

g. Trusted Facility Management Considerations

The TCSEC addresses System Administrator functions and operator functions and specifically identifies the ADP (Automated Data Processing) System Administrator. The roles and individuals must be specifically identified for this particular application and the RFP should show the mapping of particular roles and those called out in the TCSEC. For example, if the Security Officer and the ADP System Administrator are one and the same, it should be stated or only one name should be used consistently throughout the RFP. If there is more than one operator role, this should be identified.

The acquisition authority must carefully consider the division of functions between the operator and the System Administrator because the cost of changing them is often high.

C.3.19 TRUSTED RECOVERY SPECIFICATIONS

a. Text of the Specification

(For B3 through A1) Based on the recommendations of a trusted recovery analysis, mechanisms shall be provided to assure that, along with procedures, after a

computer system failure or other discontinuity, recovery without a protection compromise is obtained.

b. DOCP Interface Policy Interpretation

Interface policy shall accommodate and satisfy the required intercommunications between DOCPs to effect global recovery.

c. DOCP Global Policy Interpretation

In the case of "an ADP system failure or other discontinuity," each DOCP in a B3 or above system needs to be able to recover "without a protection compromise." Further, the recovery actions of distinct DOCPs needs to be coordinated and combined so that the resulting system is not only recovered as far as each DOCP TCB is concerned, but is also recovered as a system.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class B3, TNI Section 3.3.3.1.5 applies.

For Class A1, TNI Section 4.1.3.1.5 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.5 applies

For Class B3, TDI Appendix A Section B3-3.1.5 applies.

For Class A1, TDI Appendix A Section A1-3.1.5 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

For Class B3, TCSEC Section 3.3.3.1.5.

For Class A1, TCSEC Section 4.1.3.1.5.

NCSC-TG-022, "A Guide to Understanding Trusted Recovery in Trusted Systems," December 30, 1991.

g. Trusted Recovery Considerations

Satisfactory recovery can have significantly different meaning to different applications because of differences in the time criticality of operational results. The

procurement initiator must be certain that the true operational requirements for this particular application are reflected in the RFP.

Note that satisfaction of this requirement does not guarantee data recovery. It keeps the system from blindly compromising data and allows the System Administrator to reach a known good point in the process where other mission mechanisms (e.g., backup) can safely proceed. Trusted recovery does not obviate the need for responsible backup procedures and practices.

THIS PAGE INTENTIONALLY LEFT BLANK

C.4 STATEMENTS OF WORK

Detailed Statements of Work can be found in this section. The glossary and acronyms referenced in Section J and attached to this RFP are considered to be part of this Statement of Work.

For each task, the requirements of the Statement of Work (SOW) describe the work the Contractor is expected to do. The specification of the deliverable is accomplished within a Contract Data Requirements List (CDRL) and its associated Data Item Description (DID). Here we have provided sample CDRL numbers to correspond with Section F.

(The appropriate information and considerations for determining Statements of Work for the RFP is done just the same as was done in the Specification guided by the decision for single policy SOWs using TCSEC, single policy SOWS using the TCSEC along with the TNI interpretation, multipolicy SOWS using the TDI and finally multipolicy SOWs with DOCPs.)

C.4.1 COVERT CHANNEL ANALYSIS STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.3.1.3.

For Class B3, repeat TCSEC Section 3.3.3.1.3.

For Class A1, repeat TCSEC Section 4.1.3.1.3.)

(For B2 through A1)
The Contractor shall conduct an analysis of all auditable events that may occur in the exploitation of the identified covert channels.

The Contractor shall conduct an analysis of identified covert channels and bandwidths that are non detectable by the auditing mechanisms. The contractor shall determine the auditability of channels that have a bandwidth in excess of one bit in ten seconds.

A report of the results of these analyses shall be provided in the form of a Covert Channel Analysis Report, written in accordance with CDRL 010.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.3.1.3 applies.

For Class B3, TNI Section 3.3.3.1.3 applies.

For Class A1, TNI Section 4.1.3.1.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.3 applies.

For Class B2, TDI Appendix A Section B2-3.1.3 applies.

For Class B3, TDI Appendix A Section B3-3.1.3 applies.

For Class A1, TDI Appendix A Section A1-3.1.3 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

TCSEC Section 8.0 "A Guideline on Covert Channels."

g. Covert Channel Analysis Considerations

(None)

C.4.2 TRUSTED RECOVERY STATEMENT OF WORK

a. Text of the Statement of Work

(For B3 through A1)
The Contractor shall conduct an analysis of the computer system design to determine procedures and/or mechanisms that need to be activated in case of a system failure or other discontinuity.

Where procedures are recommended they should be thoroughly documented in CDRL 002 Trusted Facility Manual.

Where design is recommended it is delivered in the form of system design in accordance with CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; CDRL 008, Design Specification; and CDRL 012 Security Test Plan.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

In the case of "an ADP system failure or other discontinuity," each DOCP in a B3 or above system needs to be able to recover "without a protection compromise." Further, the recovery actions of distinct DOCPs needs to be coordinated and combined so that the resulting system is not only recovered as far as each DOCP TCB is concerned, but is also recovered as a system.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class B3, TNI Section 3.3.3.1.5 applies.

For Class A1, TNI Section 4.1.3.1.5 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.1 and IR-2.3.1.5 applies.

For Class B3, TDI Appendix A Section B3-3.1.5 applies.

For Class A1, TDI Appendix A Section A1-3.1.5 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

For Class B3, TCSEC Section 3.3.3.1.5.

For Class A1, TCSEC Section 4.1.3.1.5.

NCSC-TG-022, "A Guide to Understanding Trusted Recovery in Trusted Systems," December 30, 1991.

TCSEC Section 5.3.3, Assurance Control Objective, p. 63.

g. Trusted Recovery Procurement Considerations

(None)

C.4.3 SECURITY TESTING STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.3.2.1. and TCSEC Section 10.1.

For Class B1, repeat TCSEC Section 3.1.3.2.1. and TCSEC Section 10.2.

For Class B2, repeat TCSEC Section 3.2.3.2.1. and TCSEC Section 10.2.

For Class B3, repeat TCSEC Section 3.3.3.2.1. and TCSEC Section 10.2.

For Class A1, repeat TCSEC Section 4.1.3.2.1. and TCSEC Section 10.3.)

The contractor shall deliver test results in the form of Test Reports in accordance with CDRL 014. A final summary Test Report is called out under Section 4.9 Test Documentation Statement of Work.

b. DOCP Interface Policy Interpretation

Security testing shall include testing against the individual DOCP interface policies and requirements.

c. DOCP Global Policy Interpretation

This requirement applies as stated in the TCSEC to the entire TCB. If a TCB consists of TCB subsets meeting the conditions for evaluation by parts, the satisfaction of the requirements by each TCB subset suffices to satisfy the requirement for the entire TCB. Otherwise, security testing must include testing of the entire TCB (even if the results of testing the individual TCB subsets are available).

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TNI should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.3.2.1 applies.

For Class B1, TNI Section 3.1.3.2.1 applies.

For Class B2, TNI Section 3.2.3.2.1 applies.

For Class B3, TNI Section 3.3.3.2.1 applies.

For Class A1, TNI Section 4.1.3.2.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.2 and IR-2.3.2.1 applies.

For Class C2, TDI Appendix A Section C2-3.2.1 applies.

For Class B1, TDI Appendix A Section B1-3.2.1 applies.

For Class B2, TDI Appendix A Section B2-3.2.1 applies.

For Class B3, TDI Appendix A Section B3-3.2.1 applies.

For Class A1, TDI Appendix A Section A1-3.2.1 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-002, "Trusted Product Evaluations: A Guide for Vendors," June 22, 1990.

NCSC-TG-019, "Trusted Product Evaluation Questionnaire," May 2, 1992.

NCSC-TG-028, "Assessing Controlled Access Protection," May 25, 1992.

g. Security Testing Procurement Considerations

Many of the statements in the security testing requirements are subject to interpretation, (e.g., "relatively resistant to penetration," consistency with top level specifications, "no more than a few correctable flaws," and "reasonable confidence that few remain"). The Procurement Initiator in the RFP must attempt to convey in any manner possible what will be expected by the Government, not only in satisfying the security testing requirement but in terms of meeting the certification evaluation. Similarly in evaluation of the bidder's response to testing requirements of the RFP, the Government must be very careful to understand that the contractor understands what is required. As an example, there is a great advantage in identifying who will conduct the penetration analysis (B2 and above) and how the results of that penetration will be dealt with. A clear understanding must exist and be documented before an award is made.

C.4.4 DESIGN SPECIFICATION AND VERIFICATION STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class B1, repeat TCSEC Section 3.1.3.2.2.

For Class B2, repeat TCSEC Section 3.2.3.2.2.

For Class B3, repeat TCSEC Section 3.3.3.2.2.

For Class A1, repeat TCSEC Section 4.1.3.2.2.)

(For Class B1)
Documentation developed under CDRL 004, Informal Security Policy Model, and CDRL 008, Design Specification, shall be maintained as a result of this effort with updates delivered according to the CDRL.

Initial delivery of CDRL 004, Informal Security Policy Model, and CDRL 008, Design Specification, is addressed in Section 4.10, Design Document Statement of Work. Subsequent deliveries shall be delivered under this task.

(For Class B2)
Documentation developed under CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; and CDRL 008, Design Specification; shall be maintained as a result of this effort with updates delivered according to the CDRL.

Initial delivery of CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; and CDRL 008, Design Specification; is addressed in Section 4.10, Design Document Statement of Work. Subsequent deliveries shall be delivered under this task.

(For Class B3)
Documentation developed under CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; and CDRL 008, Design Specification; shall be maintained as a result of this effort with updates delivered according to the CDRL.

Documentation resulting from this effort shall be provided in accordance with CDRL 009 Trusted Computing Base Verification Report.

Initial delivery of CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; and CDRL 008, Design Specification; is addressed in Section 4.10, Design Document Statement of Work. Subsequent deliveries shall be delivered under this task.

(For Class A1)
Documentation developed under CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; CDRL 007, Formal Top Level Specification; and CDRL 008, Design Specification; shall be maintained as a result of this effort with updates delivered according to the CDRL.

Documentation resulting from this effort shall be provided in accordance with CDRL 009, Trusted Computing Base Verification Report.

Initial delivery of CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; CDRL 007, Formal Top Level Specification; and CDRL 008, Design Specification; is addressed in Section 4.10, Design Document Statement of Work. Subsequent deliveries shall be delivered under this task.

b. DOCP Interface Policy Interpretation

Design specification and verification requirements apply to interface policy and the resultant interface requirements between DOCPs.

c. DOCP Global Policy Interpretation

For many of the design specification and verification requirements, demonstrating that a requirement is satisfied by all of the constituent DOCPs is sufficient to demonstrate that it is satisfied for the composite system. The requirements for a "formal model of the security policy supported by the TCB" and that the DTLS at B3

and the FTLS at A1 "be an accurate description of the TCB interface" applies in a limited way to the entire TCB.

After complying security models are provided for the individual DOCPs, a convincing argument is required to explain how the set of models represents, abstractly, the policy of the entire system.

After complying top-level specifications (DTLS at B3 and FTLS at A1) are provided for the individual DOCPs, an explicit and convincing description how the set of top-level specifications describe the TCB interface with respect to exceptions, errors and effects must also be provided.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class B1, TNI Section 3.1.3.2.2 applies.

For Class B2, TNI Section 3.2.3.2.2 applies.

For Class B3, TNI Section 3.3.3.2.2 applies.

For Class A1, TNI Section 4.1.3.2.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.2 and IR-2.3.2.2 applies.

For Class B1, TDI Appendix A Section B1-3.2.2 applies.

For Class B2, TDI Appendix A Section B2-3.2.2 applies.

For Class B3, TDI Appendix A Section B3-3.2.2 applies.

For Class A1, TDI Appendix A Section A1-3.2.2 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-014, "Guidelines for Formal Verification Systems," April 1, 1989.

g. Design Specification and Verification Considerations

If there is a multifaceted policy (e.g., both mandatory access control and discretionary access control policies), then all facets must be represented in the Top Level Specification and Security Model.

(B2 - A1) To broaden the audience, there is often an advantage to requiring an informal policy model as well as a formal one.

C.4.5 CONFIGURATION MANAGEMENT STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class B2, repeat TCSEC Section 3.2.3.2.3.

For Class B3, repeat TCSEC Section 3.3.3.2.3.

For Class A1, repeat TCSEC Section 4.1.3.2.3.)

(B2 through A1) Prepare and deliver TCB Configuration Management Plan in accordance with CDRL 011. One section of this document is originated under C.4.6.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class B2, TNI Section 3.2.3.2.3 applies.

For Class B3, TNI Section 3.3.3.2.3 applies.

For Class A1, TNI Section 4.1.3.2.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.2 and IR-2.3.2.3 applies.

For Class B2, TDI Appendix A Section B2-3.2.3 applies.

For Class B3, TDI Appendix A Section B3-3.2.3 applies.

For Class A1, TDI Appendix A Section A1-3.2.3 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-006, "A Guide to Understanding Configuration Management in Trusted Systems," March 28, 1988.

g. Configuration Management Considerations

Master copies should be protected at the level of the operational data for which it will be used.

(B2 - A1) The maintenance of a consistent mapping between code and documentation may require further definition (e . g., including the response time for bringing documentation up to date with changes and the exact amount of effort to go into this requirement).

C.4.6 TRUSTED DISTRIBUTION STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class A1, repeat TCSEC Section 4.1.3.2.4.)

These procedures shall be delivered as a Section on Trusted Distribution as a part of the Trusted Computing Base Configuration Management Plan in accordance with CDRL 011. The rest of the document is developed under 4.5, Configuration Management Statement of Work.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class A1, TNI Section 4.1.3.2.4 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.3.2 and IR-2.3.2.4 applies.

For Class A1, TDI Appendix A Section A1-3.2.4 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-008, "A Guide to Understanding Trusted Distribution in Trusted Systems," December 15, 1988.

g. Trusted Distribution Procurement Considerations

(None)

C.4.7 SECURITY FEATURES USER'S GUIDE STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.4.1.

For Class B1, repeat TCSEC Section 3.1.4.1.

For Class B2, repeat TCSEC Section 3.2.4.1.

For Class B3, repeat TCSEC Section 3.3.4.1.

For Class A1, repeat TCSEC Section 4.1.4.1.)

(C2 through A1) The Contractor shall produce and deliver the Security Features User's Guide in accordance with CDRL 001.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.4.1 applies.

For Class B1, TNI Section 3.1.4.1 applies.

For Class B2, TNI Section 3.2.4.1 applies.

For Class B3, TNI Section 3.3.4.1 applies.

For Class A1, TNI Section 4.1.4.1 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.4.1 and IR-2.4.1 applies.

For Class C2, TDI Appendix A Section C2-4.1 applies.

For Class B1, TDI Appendix A Section B1-4.1 applies.

For Class B2, TDI Appendix A Section B2-4.1 applies.

For Class B3, TDI Appendix A Section B3-4.1 applies.

For Class A1, TDI Appendix A Section A1-4.1 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-026, "A Guide to Writing the Security Features User's Guide for Trusted Systems," September 1991.

g. Security Features User's Guide Considerations

The Contractor should conduct a security engineering analysis to determine user functionality related to security. This analysis should also develop the user guidelines for consistent and effective use of the protection features of the proposed solution. This analysis should address a description of expected system reaction to security-related events.

C.4.8 TRUSTED FACILITY MANUAL STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.4.2.

For Class B1, repeat TCSEC Section 3.1.4.2.

For Class B2, repeat TCSEC Section 3.2.4.2.

For Class B3, repeat TCSEC Section 3.3.4.2.

For Class A1, repeat TCSEC Section 4.1.4.2.)

(C2 through A1) The Contractor shall deliver the Trusted Facility Manual in accordance with CDRL 002.

b. DOCP Interface Policy Interpretation

(None)

c. DOCP Global Policy Interpretation

(None)

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.4.2 applies.

For Class B1, TNI Section 3.1.4.2 applies.

For Class B2, TNI Section 3.2.4.2 applies.

For Class B3, TNI Section 3.3.4.2 applies.

For Class A1, TNI Section 4.1.4.2 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.4.2 and IR-2.4.2 applies.

For Class C2, TDI Appendix A Section C2-4.2 applies.

For Class B1, TDI Appendix A Section B1-4.2 applies.

For Class B2, TDI Appendix A Section B2-4.2 applies.

For Class B3, TDI Appendix A Section B3-4.2 applies.

For Class A1, TDI Appendix A Section A1-4.2 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-027, "Information System Security Officer Guideline," June 1991.

g. Trusted Facility Manual Considerations

The Contractor should conduct an analysis to identify the functions performed by the role of the System Administrator. This analysis should identify all non-security functions that can be performed in the System Administrator role. The Contractor should conduct an analysis to determine, for the operator and System Administrator, the specific cautions about functions and privileges that should be controlled while

running a secure facility and the specific interactions of the protection features. The Contractor should also conduct an engineering analysis of the system to identify all information and events to be audited, including rationale (i.e., cost, conformance to requirements, security, and performance impacts) for the selection of each item. The Contractor should also identify the types of events that occur within the system that are not audited, along with reasons for not auditing them.

C.4.9 TEST DOCUMENTATION STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.4.3.

For Class B1, repeat TCSEC Section 3.1.4.3.

For Class B2, repeat TCSEC Section 3.2.4.3.

For Class B3, repeat TCSEC Section 3.3.4.3.

For Class A1, repeat TCSEC Section 4.1.4.3.)

(C2 through A1)
The Contractor shall deliver the Security Test Plan in accordance with CDRL 012.

The Contractor shall deliver the Test Procedure in accordance with CDRL 013.

The Contractor shall deliver the Test Report in accordance with CDRL 014 using as input Test Reports generated in 4.3 Security Testing Statement of Work.

b. DOCP Interface Policy Interpretation

Test Documentation shall include testing of interface requirements.

c. DOCP Global Policy Interpretation

Test Documentation shall include testing of global requirements.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.4.3 applies.

For Class B1, TNI Section 3.1.4.3 applies.

For Class B2, TNI Section 3.2.4.3 applies.

For Class B3, TNI Section 3.3.4.3 applies.

For Class A1, TNI Section 4.1.4.3 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.4.3 and IR-2.4.3 applies.

For Class C2, TDI Appendix A Section C2-4.3 applies.

For Class B1, TDI Appendix A Section B1-4.3 applies.

For Class B2, TDI Appendix A Section B2-4.3 applies.

For Class B3, TDI Appendix A Section B3-4.3 applies.

For Class A1, TDI Appendix A Section A1-4.3 applies.)

f. Important References

(None)

g. Security Testing Procurement Considerations

The Contractor should analyze the sensitivity of information processed on the delivered system, the desired mode of operation, and the Designated Approving Authority's (DAA's) certification requirements to assist in developing the test approach.

If an entity other than a contractor is to do the Security Testing, and Test Report, this should be clarified in the Statement of Work. The Test Plan (which is a management tool detailing who does what and when) and Test Procedures (which is a step-by-step testing script) should be prepared by the Contractor to ensure that specific knowledge of the TCB implementation can be included in their development. The Test Plan and Test Procedure may later be augmented or modified by the entity doing the testing under separate contract or agreement.

For B2 and above, penetration testing must consider the specific operational environment and threat model of this particular application.

C.4.10 DESIGN DOCUMENTATION STATEMENT OF WORK

a. Text of the Statement of Work

(Where the given Division/Class is applicable, the corresponding section of the TCSEC should be repeated in the statement of work portion of the RFP verbatim:

For Class C2, repeat TCSEC Section 2.2.4.4.

For Class B1, repeat TCSEC Section 3.1.4.4.

For Class B2, repeat TCSEC Section 3.2.4.4.

For Class B3, repeat TCSEC Section 3.3.4.4.

For Class A1, repeat TCSEC Section 4.1.4.4.)

(For Class C2)
Documentation resulting from this effort shall be provided in accordance with CDRL 003, Philosophy of Protection Report, and CDRL 008, Design Specification.

(For Class B1)
Documentation resulting from this effort shall be provided in accordance with CDRL 003, Philosophy of Protection Report; CDRL 004, Informal Security Policy Model; and CDRL 008, Design Specification.

Initial delivery of CDRL 004 and CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section 4.4, Design Specification and Verification Statement of Work.

Initial delivery of CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section 4.4, Design Specification and Verification Statement of Work.

(For Class B2)
Documentation resulting from this effort shall be provided in accordance with CDRL 003, Philosophy of Protection Report; CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; and CDRL 008, Design Specification.

Initial delivery of CDRL 005, CDRL 006, and CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section 4.4, Design Specification and Verification Statement of Work.

(For Class B3)
Documentation resulting from this effort shall be provided in accordance with CDRL 003, Philosophy of Protection Report; CDRL 005, Formal Security Policy Model; CDRL 006 Descriptive Top Level Specification; and CDRL 008, Design Specification.

Initial delivery of CDRL 005, CDRL 006, and CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section 4.4, Design Specification and Verification Statement of Work.

(For Class A1)
Documentation resulting from this effort shall be provided in accordance with CDRL 003, Philosophy of Protection Report; CDRL 005, Formal Security Policy Model; CDRL 006, Descriptive Top Level Specification; CDRL 007, Formal Top Level Specification; and CDRL 008, Design Specification.

Initial delivery of CDRL 005, CDRL 006, CDRL 007, and CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section 4.4, Design Specification and Verification Statement of Work.

b. DOCP Interface Policy Interpretation

Design Documentation shall include design resulting from interface requirements.

c. DOCP Global Policy Interpretation

Design Documentation shall include design resulting from global requirements.

d. Trusted Network Interpretation

(Where the given Division/Class is applicable and the TNI is selected, the corresponding section of the TCSEC should be considered by the procurement initiator in the specification portion of the RFP:

For Class C2, TNI Section 2.2.4.4 applies.

For Class B1, TNI Section 3.1.4.4 applies.

For Class B2, TNI Section 3.2.4.4 applies.

For Class B3, TNI Section 3.3.4.4 applies.

For Class A1, TNI Section 4.1.4.4 applies.)

e. Trusted Database Management Interpretation

(Where the given Division/Class is applicable and the TDI is selected, the corresponding section of the TDI should be considered by the procurement initiator:

For all classes, TDI Sections TC-5.2.4.4 and IR-2.4.4 applies.

For Class C2, TDI Appendix A Section C2-4.4 applies.

For Class B1, TDI Appendix A Section B1-4.4 applies.

For Class B2, TDI Appendix A Section B2-4.4 applies.

For Class B3, TDI Appendix A Section B3-4.4 applies.

For Class A1, TDI Appendix A Section A1-4.4 applies.)

f. Important References

(Note: References are for information only and, unless specified elsewhere, are not to be taken as requirements.)

NCSC-TG-007, "A Guide to Understanding Design Documentation in Trusted Systems," October 2, 1988.

g. Design Documentation Procurement Considerations

The Contractor should conduct an analysis of the sensitivity of information to be processed on the delivered system, the desired mode of operation, and the Designated Approving Authority's (DAA's) certification requirements to determine a philosophy of protection for the system. This should also analyze how that philosophy of protection is translated into the specific system TCB.

The Contractor should analyze the TCB enforcement of the security policy specified in the philosophy of protection document.

THIS PAGE INTENTIONALLY LEFT BLANK

RFP SECTION F – DELIVERIES AND PERFORMANCE

Text of Section F

(A1) Procedures generated under Trusted Distribution Statement of Work shall be followed for TCB software, firmware and hardware as well as updates. (See Section C.4.6, "Trusted Distribution Statement of Work.")

Data Deliverables: The following data deliverables in the form of Contract Data Requirements Lists are found referenced in Section J of this RFP and contained in Attachment A. (For multipolicy systems, these documents are called for more than once, e.g., once for every DOCP. The CDRL can call for a separate document for each requirement, but more often it makes sense to have a single document with a single general system section to address otherwise repetitive system factors, a section for each DOCP or TCB subset to deal with uniqueness, and finally a section associated with each division/class contained in the system.)

CLASS RANGE	CDRL*	DOCUMENT	SOWs
C2–A1	CDRL 001	Security Feature User's Guide DI-MCCR-81349	C.4.7
C2–A1	CDRL 002	Trusted Facility Manual DI-TMSS-81352	C.4.2, C.4.8
C2–A1	CDRL 003	Philosophy of Protection DI-MISC-81348	C.4.10
B1	CDRL 004	Informal Security Policy Model DI-MISC-81341	C.4.4, C.4.10
B2–A1	CDRL 005	Formal Security Policy Model DI-MISC-81346	C.4.2, C.4.4, C.4.10
B2–A1	CDRL 006	Descriptive Top Level Specification DI-MISC-81342	C.4.2, C.4.4, C.4.10
A1	CDRL 007	Formal Top Level Specification DI-MISC-81347	C.4.4, C.4.10
C2–A1	CDRL 008	Design Specification DI-MCCR-81344	C.4.2, C.4.4, C.4.10
B3–A1	CDRL 009	Trusted Computing Base Verification Report DI-MISC-81350	C.4.4
B2–A1	CDRL 010	Covert Channel Analysis Report DI-MISC-81345	C.4.1
B2–A1	CDRL 011	Trusted Computing Base Configuration Management Plan DI-CMAN-81343	C.4.5, C.4.6
C2–A1	CDRL 012	Security Test Plan DI-NDTI-81351	C.4.2, C.4.9
C2–A1	CDRL 013	Test Procedure DI-NDTI-80603	C.4.9
C2–A1	CDRL 014	Test/Inspection Reports DI-NDTI-80809A	C.4.3, C.4.9

Table F-1 Data Deliverables (*) See note at top of next page.

*** These are sample CDRL's used to facilitate the presentations of this guideline. Procurement initiators will have their own CDRL's, and will therefore need to cross-reference the cited SOW paragraph numbers listed above and insert their own CDRL numbers in those paragraphs.**

Important References

NCSC-TG-006, "A Guide to Understanding Configuration Management in Trusted Systems," March 28, 1988.

NCSC-TG-008, "A Guide to Understanding Trusted Distribution in Trusted Systems," December 15, 1988.

Section F Procurement Considerations

Deliveries:

The referenced document, NCSC-TG-008, discusses protective packaging, couriers, registered mail, message authentication codes, encryption, and site validation.

Performance:

Application specific performance requirements must be developed by the procurement initiator and placed in Section F of the RFP as requirements. The following is a sample list of such requirements that need to be quantified for the application:

- Performance requirements must be satisfied under both typical and peak conditions.
- Performance requirements should be such that both mission and audit requirements can be met without performance conflict.
- The bidder shall identify the time to initialize, recover, and shutdown the system in a secure state, consistent with RFP requirements.

The bidder shall identify the maximum, minimum and average time to perform reference verification once a subject request has been made, consistent with RFP requirements.

- The bidder shall identify the maximum, minimum, and average time to create an audit record associated with an auditable event.
- The bidder shall identify the amount of time required of a user for security during a best case, typical case, and worst case user session, consistent with RFP requirements.
- The bidder shall identify the maximum, average, and minimum amount of time required to seek out a specific audit record, the audit records associated with a single subject over a day, and the audit records associated with a single object over the day, consistent with RFP requirements.

- The bidder shall identify the maximum, average, and minimum percentage overhead due to security in the intended operational environment over the course of a day, consistent with RFP requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

RFP SECTION J – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

Text of Section J

The following is a listing of all attachments to the contract:

ATTACHMENT NO.	TITLE
A	CONTRACT DATA REQUIREMENTS LIST
B	GLOSSARY
C	ACRONYMS
D	REFERENCES

Important References

(None)

Section J Procurement Considerations

RFP Sections A through K, when combined with the attachments referenced above, constitute the contract. Sections L (discussed next) and M (discussed in Volume 4 of this guideline series) serve only to support the RFP and are discarded once the contract has been awarded.

THIS PAGE INTENTIONALLY LEFT BLANK

RFP SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

Text of Section L

(These statements shall be included under GENERAL INSTRUCTIONS FOR THE PREPARATION OF PROPOSALS – SPECIFIC INSTRUCTIONS. In multipolicy proposal, theoretically there could be a proposal for each unique DOCP or TCB subset. However, from a practical viewpoint, and to withstand the redundancy, it is best to have a general presentation of the requirements, dealing with exceptions as appropriate, whether because of Division/Class or some other reason.)

Offerors shall identify in the technical proposal the commercially available products proposed to meet the acquisition's operational and security requirements and/or reasons that none were chosen as part of the offeror's solution. Responses must be supported by appropriate published technical specifications and technical documents.

Offerors shall identify tests, analyses, and documents previously produced for the development and evaluation of any proposed EPL product to be used in satisfying the requirements of this contract. Offerors shall also provide reasons why such information is not available or is not being proposed as part of the solution, if this is the case.

TECHNICAL

- **The bidder shall precisely identify all security related hardware, firmware, and software.**
- **The bidder shall present a description of the philosophy of protection and an explanation of how this philosophy will be translated into the TCB.**
- **If the TCB is composed of distinct modules, the interfaces between these modules shall be described by the bidder.**
- **The bidder shall provide procedures for examining and maintaining audit files.**
- **The bidder shall describe the test plan.**
- **The bidder shall describe the approach to configuration management.**
- **The bidder shall describe trusted initialization and shutdown.**
- **The bidder shall describe the process of creating, maintaining, and protecting from modification, or unauthorized access or destruction, an audit trail of accesses, and objects the TCB protects.**
- **(B1–A1) The bidder shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user.**

- (B1–A1) The bidder shall state a security model either informally or formally and provide an explanation to show that it is sufficient to enforce the security policy.
- (B1–A1) The bidder shall identify specific TCB protection mechanisms with an explanation given to show that they satisfy the model.
- (B2–A1) The bidder shall describe the approach to covert channel analysis.
- (B2–A1) The bidder shall provide a descriptive top level specification.
- (A1) A formal top level specification shall be provided.
- (B3–A1) The bidder shall define system recovery procedures or mechanisms with an explanation as to how the system will recover without a protection compromise.
- (B3–A1) The bidder shall identify the functions performed by the System Administrator.
- (A1) The bidder shall describe techniques to show that the Formal Top Level Specification (FTLS) is consistent with the model.
- The bidder shall show an understanding of the mission requirements and reflect the security relevant aspects in the proposed solution.
- The bidder shall show an understanding of the environment of the system as stated in the RFP and the system proposed shall address and meet all of the environmental requirements.

MANAGEMENT

- Secure systems developed, tested, and placed into operational usage have notoriously high cost risk, schedule risk, and technical risk because of the ease in misunderstanding the full implications of the Government requirements as contained in the *TCSEC*. The bidder shall provide, not only anticipated program plan items, but also where deviations could occur, the worst those deviations could become, and the approach to be taken to recover from such anomalies.
- The bidder shall summarize security experience applicable to this project, major successes, problems and their solutions, and explain how such experience will be brought to bear.
- The bidder shall explain the relationship between the senior security specialist and the Program Manager and how it will be assured that technical issues will be resolved to reduce security risk and cost to the Government.
- The bidder shall identify key individuals on this project; summarize their applicable education, training, and work experience; specifically state their experience with trusted system design, development, and test including Division/Class and whether NSA evaluation or certification evaluation were successfully achieved.

- The bidder shall identify who specifically is responsible for any security modeling, security testing, configuration management, TCB design, and TCB build, as applicable.

- The bidder shall show how the security organization operates as a cohesive entity within the overall project organization so that security receives the appropriate attention and continuity through development phases, as applicable.

- The bidder shall show how the management plan is organized such that time and effort is not wasted on problems that can arise in design and development of a trusted system.

- The bidder shall show how potential problems are identified early and how they are treated at a high level with the appropriate level of expertise before they result in a high cost or increased risk situation.

- The bidder shall show specific personnel continuity during the critical stages of design, development, test, certification and accreditation, as applicable.

- The bidder shall identify who will be the primary interface during certification.

- The schedule shall be easily and precisely associated with the work plan with the deliverables identified in the management proposal and in the technical proposal.

- Items that are schedule critical to the project and items where there is high schedule risk shall be delineated to the appropriate detail level on the schedule.

- The bidder shall identify from his/her experience where the areas of greatest schedule risk exist in his/her proposed approach to satisfy the requirements of the RFP for this secure system.

- For the areas of high schedule risk, the bidder shall show how he/she intends to identify the situation of a schedule slippage and then what will be done to minimize the impact of the deviation.

COST

- Commercial off–the–shelf items shall be broken down to the degree that they will be described on the purchase order. Other uniquely identified deliverables (e.g., manuals, computer programs, services) shall be identifiable to level–of–effort, schedule, and overall cost.

- Costs of all items associated in any way with security and the acquisition/development of the secure system shall be identifiable in the cost breakdown.

- The bidder shall identify from his/her experience where the areas of greatest cost risk exist in his/her proposed approach to satisfy the requirements of the RFP for this secure system.

- **For the areas of high cost risk, the bidder shall show how he/she intends to identify the situation of a cost overrun and then what will be done to minimize the impact of the deviation.**

GENERAL

- **A single work breakdown structure shall be used in all three proposals, allowing a precise cross referencing between cost, effort, schedule, individuals, and elements of the technical work plan.**

- **Tradeoffs may be purely technical or they may be decided because of cost, schedule or risk issues. The bidder shall identify significant tradeoffs along with the results and rationale for the decision.**

- **The bidder shall identify what significant tradeoffs are yet to be made along with the factors involved in the decision.**

Important References

(None)

Section L Procurement Considerations

In procuring EPL products, a goal is to use as much of the existing documentation and certification evidence as possible in satisfaction of the requirements of the contract. Usually this data does not belong to the Government. Thus bidders are encouraged to seek out and attempt to buy or otherwise obtain existing documentation from the developing vendor in an attempt to reduce the cost and risk of the bid and ensuing contract. This approach can also provide a significant competitive advantage for EPL solutions.

RFP ATTACHMENT A - CONTRACT DATA REQUIREMENTS LIST (CDRL) FORM DD1423

Contract Data Requirements List Discussion

CDRLs will be provided for the following documents as part of Volume 3 of this guideline series. The CDRLs should be attached to this section and adapted to the procurement. For each document and for each Division/Class there will also be a DID Number and DID source reference.

- Security Feature User's Guide
- Trusted Facility Manual
- Philosophy of Protection Report
- Informal Security Policy Model
- Formal Security Policy Model
- Descriptive Top Level Specification
- Formal Top Level Specification
- Design Specification
- Trusted Computing Base Verification Report
- Covert Channel Analysis Report
- TCB Configuration Management Plan
- Security Test Plan
- Test Procedure
- Test Reports

THIS PAGE INTENTIONALLY LEFT BLANK

RFP ATTACHMENT B - GLOSSARY

Text of the Glossary

(The Glossary Section of the TCSEC should be repeated here verbatim.)

The ADP (automated data processing) system definition used in the TCSEC should be treated as synonymous with AIS.

Important References

NCSC-TG-004, Glossary of Computer Security Terms, October 21,1988.

Glossary Procurement Considerations

Any conflicts between security terms and system terms must be found and resolved. Precise accuracy of interpretation requirements in the Specifications and Statements of Work depends greatly on these definitions. Changes must not be made that might invalidate the Security Specifications and Statements of Work.

THIS PAGE INTENTIONALLY LEFT BLANK

RFP ATTACHMENT C - ACRONYMS

ADP	Automated Data Processing
AIS	Automated Information System
CDRL	Contract Data Requirements List
COTS	Commercial-Off-The-Shelf
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DID	Data Item Description
DOCP	Domain of Constant Policy
DoD	Department of Defense
DTLS	Descriptive Top–Level Specification
ECP	Engineering Change Proposal
EPL	Evaluated Products List
FTLS	Formal Top–Level Specification
NCSC	National Computer Security Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
RFP	Request for Proposal
SOW	Statement of Work
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria

THIS PAGE INTENTIONALLY LEFT BLANK

RFP ATTACHMENT D - REFERENCES

Text of the References

DoD 5200.1-R, Information Security Program Regulation, August 1982, June 1986, change June 27, 1988.

DoD 5200.2-R, DoD Personnel Security Program, January 1987.

DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), March 21, 1988.

DoD 5200.28-M, (Draft) "Automated Information System Security Manual," April 29, 1991.

DoD 5200.28-STD, DoD Trusted System Evaluation Criteria, December 26, 1985.

CSC-STD-002-85, Department of Defense (DoD) Password Management Guideline, April 12, 1985.

Johnson, H.L., "Use of the Trusted computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems," A technical report written for the NSA, February 1, 1993.

NCSC-TG-001, A Guide to Understanding Audit in Trusted Systems, June 1, 1988.

NCSC-TG-002, Version 2, Trusted Product Evaluation, A Guide for Vendors, April 29, 1990.

NCSC-TG-003, A Guide to Understanding Discretionary Access Control (DAC) in Trusted Systems, September 30, 1987.

NCSC-TG-004, Glossary of Computer Security Terms, October 21,1988.

NCSC-TG-005, Trusted Network Interpretation, July 31, 1987.

NCSC-TG-006, A Guide to Understanding Configuration Management in Trusted Systems, March 28, 1988.

NCSC-TG-007, A Guide to Understanding Design Documentation in Trusted Systems, October 2, 1988.

(A1 Only) NCSC-TG-008, A Guide to Understanding Trusted Distribution in Trusted Systems, December 15, 1988.

NCSC-TG-010, Version 1, A Guide to Understanding Security Modeling in Trusted Systems, October, 1992.

(A1 Only) NCSC-TG-014, Guidelines for Formal Verification Systems, April 1, 1989.

NCSC-TG-015, A Guide to Understanding Trusted Facility Management, October 18, 1989.

NCSC-TG-016, Version 1, Guidelines for Writing Trusted Facility Manuals, October, 1992.

NCSC-TG-017, A Guide to Understanding Identification and Authentication in Trusted Systems, September 1, 1991.

NCSC-TG-018, A Guide to Understanding Object Reuse in Trusted Systems, July, 1992.

NCSC-TG-019, Trusted Product Evaluation Questionnaire, October 16, 1989.

NCSC-TG-021, Trusted Database Management System Interpretation of the TCSEC, April, 1991.

NCSC-TG-022, A Guide to Understanding Trusted Recovery in Trusted Systems, December 30, 1991.

NCSC-TG-024, Version 1, Volume 4/4, (Draft) "A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document—An Aid to Procurement Initiators and Contractors."

NCSC-TG-025, A Guide to Understanding Data Remanence in Automated Information Systems, September 1991.

NCSC-TG-026, A Guide to Writing the Security Features User's Guide for Trusted Systems, September 1991.
NCSC-TG-027, Information System Security Officer Guideline, June 1991.

NCSC-TG-028, Assessing Controlled Access Protection, May 25, 1992.

NCSC-TG-030, A Guide to Understanding Covert Channel Analysis of Trusted Systems, November 1993.

A single complimentary copy of NSA guidelines (CSC-STD- and NCSC-TG-) may be obtained from Department of Defense, INFOSEC Awareness Operations Center, Fort George G. Meade, MD 20755-6000. By phone, call (410) 766-8729.

DoD documents and more than single copies of NSA guidelines may be obtained from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402. Mastercard or VISA may be used. By phone, call (202) 783-3238.

Important References

None

References Procurement Considerations

DoD and NSA continue to publish guides and other supportive documents. The initiator should continue to check the document list to ensure a complete set of references are being supplied and the most up to date versions are being referenced.

(This is the end of the standard RFP. The following Appendix pertains only to this Volume 2 Strawman Guideline.)

APPENDIX A BIBLIOGRAPHY

This is the bibliography for this guideline and is not intended to be part of the standard RFP provided in previous sections.

AFSSM 5031, *Complex System Guide*, Air Force Special Security Instruction, Air Force Cryptologic Support Center, Air Force Intelligence Command, 1991.

A Guide to Standard Solicitation Documents for Federal Information Processing Resources, General Services Administration, June 30, 1991.

"Competition in Contracting Act of 1984" (CICA).

CSC-STD-002-85, *Department of Defense (DoD) Password Management Guideline*, April 12, 1985.

CSC-STD-003-85, *Computer Security Requirements—Guidance for Applying the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) to Specific Environments*, June 25, 1985 (Updated as enclosure 4 of DoD Directive 5200.28).

CSC-STD-004-85, *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements—Guidance for Applying the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC) to Specific Environments*, June 25, 1985.

DoD Instruction 5000.2, *Defense Acquisition Management Policy*, February 23, 1991.

DoD 5000.2-M, *Defense Acquisition Management Documentation and Reports*, February, 1991.

DoD 5010.12-L, *Acquisition Management Systems and Data Requirements Control List*, October 1, 1990.

DoD 5200.1-R, *Information Security Program Regulation*, June 1986, Change June 27, 1988.

DoD 5200.2-R, *DoD Personnel Security Program*, January 1987.

DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988.

DoD 5200.28-M, (Draft) "Automated Information System Security Manual," April 29, 1991.

DoD 5200.28-STD, *DoD Trusted Computer System Evaluation Criteria*, December 26, 1985.

DoD Directive 5215.1, *Computer Security Evaluation Center*, October 25, 1982.

DoD Directive 5220.22, *Industrial Security Program*, December 8, 1980.

DoD 5220.22-M, *Industrial Security Manual for Safeguarding Classified Information*, January 1991.

DoD 5220.22-R, *Industrial Security Regulation*, December, 1985.

Executive Order 12356, "National Security Information," April 6, 1982.

"Federal Acquisition Regulation" (FAR) Title 48, 1990 edition issued by General Services Administration, DoD, and National Institute of Standards and Technology (these organizations also issue the "DoD FAR Supplement").

Federal Information Resources Management Regulation (FIRMR), General Services Administration (41 CFR Ch 201).

FIPS PUB 31, *Guidelines for ADP Physical Security and Risk Management*, U.S. Department of Commerce, National Bureau of Standards, June 1974.

FIPS PUB 39, *Glossary for Computer System Security*, U.S. Department of Commerce, National Bureau of Standards, February 15, 1976.

FIPS PUB 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, U.S. Department of Commerce, National Bureau of Standards.

FIPS PUB 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification*, U.S. Department of Commerce, National Bureau of Standards, April 1, 1977.

FIPS PUB 65, *Guideline for Automatic Data Processing Risk Analysis*, U.S. Department of Commerce, National Bureau of Standards, August 1, 1979.

FIPS PUB 73, *Guidelines for Security of Computer Applications*, U.S. Department of Commerce, National Bureau of Standards, June 30, 1980.

FIPS PUB 83, *Guideline for User Authentication Techniques for Computer Network Access*, U.S. Department of Commerce, National Bureau of Standards.

FIPS PUB 102, *Guidelines for Computer Security Certification and Accreditation*, U.S. Department of Commerce, National Bureau of Standards, Sept., 27, 1983.

FIPS PUB 112, *Password Usage Standard*, U.S. Department of Commerce, National Bureau of Standards, May 30, 1985.

Gasser, M., *Building a Secure Computer System*, Van Nostrand Reinhold, NY, 1988.

Information Systems Security Products and Services Catalogue, National Security Agency, (Published Quarterly).

Johnson, H.L., *An Approach to Security Test*, AFCEA 4th Annual Symposium on C3I Technology, Information and Security, Philadelphia, PA, 16-18 August 1988.

Johnson, H.L., and J. D. Layne, *Modeling Security Risk in Networks*, Proceedings 11th National Computer Security Conference, NIST and NCSC, October 17-20, 1988, pp. 59-64.

Johnson, H.L., *Use of the Trusted Computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems*, A technical report written for the NSA, February 1, 1993.

MIL-HDBK-245B, *Preparation of Statements of Work.*

MIL-STD-481, *Configuration Control, Engineering Changes, Deviations and Waivers.*

MIL-STD-483A, *Configuration Management Practices for Systems, Equipment, Munitions, and Computer Software.*

MIL-STD-490A, *Specification Practices.*

MIL-STD-499, *Engineering Management.*

MIL-STD-499B, *System Engineering.*

MIL-STD-1521A, *Technical Review and Audits for Systems, Equipments and Computer Programs*, 1 June 1976, with Notice 1, 29 September 1978 and Notice 2, December 21, 1981.

NCSC-TG-001, *A Guide to Understanding Audit in Trusted Systems*, June 1, 1988.

NCSC-TG-002, Version 2, *Trusted Product Evaluation, A Guide for Vendors*, April 29, 1990.

NCSC-TG-003, *A Guide to Understanding Discretionary Access Control (DAC) in Trusted Systems*, September 30, 1987.

NCSC-TG-004, *Glossary of Computer Security Terms*, October 21, 1988.

NCSC-TG-005, *Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC)*, July 31, 1987.

NCSC-TG-006, *A Guide to Understanding Configuration Management in Trusted Systems*, March 28, 1988.

NCSC-TG-007, *A Guide to Understanding Design Documentation in Trusted Systems*, October 2, 1988.

NCSC-TG-008, *A Guide to Understanding Trusted Distribution in Trusted Systems*, December 15, 1988.

NCSC-TG-009, *Computer Security Subsystem Interpretation (CSSI) of the Trusted Computer System Evaluation Criteria (TCSEC)*, September 16, 1988.

NCSC-TG-010, Version 1, *A Guide to Understanding Security Modeling in Trusted Systems*, October, 1992.

NCSC-TG-011, *Trusted Network Interpretation Environments Guideline*, 1 August, 1990.

NCSC-TG-013, *Rating Maintenance Phase, Program Document*, June 23, 1989.

NCSC-TG-014, *Guidelines for Formal Verification Systems*, April 1, 1989.

NCSC-TG-015, *A Guide to Understanding Trusted Facility Management*, October 18, 1989.

NCSC-TG-016, Version 1, *Guidelines for Writing Trusted Facility Manuals*, October, 1992.

NCSC-TG-017, *A Guide to Understanding Identification and Authentication in Trusted Systems*, September 1, 1991.

NCSC-TG-018, *A Guide to Understanding Object Reuse in Trusted Systems*, July, 1992.

NCSC-TG-019, *Trusted Product Evaluation Questionnaire*, October 16, 1989.

NCSC-TG-021, *Trusted Database Management System Interpretation of The Trusted Computer System Evaluation Criteria (TCSEC)*, April 1991.

NCSC-TG-022, *A Guide to Understanding Trusted Recovery in Trusted Systems*, December 30, 1991.

NCSC-TG-024, Version 1:

- Volume 1/4, *A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements*, Dec,1992.
- Volume 2/4, *A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work—An Aid to Procurement Initiators*, 30 June 1993.
- Volume 3/4, "A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Descriptions Tutorial," 28 February 1994.
- Volume 4/4, "A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document—An Aid to Procurement Initiators **and** Contractors," (Draft).

NCSC-TG-025, *A Guide to Understanding Data Remanence in Information Systems*, September 1991.

NCSC-TG-026, *A Guide to Writing the Security Features User's Guide for Trusted Systems*, September 1991.

NCSC-TG-027, *Information System Security Officer Guideline*, June 1991.

NCSC-TG-028, *Assessing Controlled Access Protection*, May 25, 1992.

OMB Circular Number A-130, *Management of Federal Information Resources*, Appendix III "Security of Federal Automated Information Systems," December 12, 1985.

Public Law 98-369, "Competition in Contracting Act of 1984."

Public Law 100-235, "Computer Security Act of 1987," January 8, 1988.

Standard Solicitation Document for Federal Information Processing (FIP) Systems (Hardware, Software and Maintenance), General Services Administration, June 30, 1991.

Title 10, United States Code, Section 2318, "Advocates for Competition."

Title 41, United States Code, Section 418, "Advocates for Competition."

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 1994	Final

4. TITLE AND SUBTITLE *Volume 2/4 (Strawman) A Guide to Procurement of Single and Connected Systems Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators Includes Complex, Evolving, Multipolicy Systems*

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Intelligence Sciences, Inc., Howard Johnson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Security Agency
Attention: INFOSEC Standards, Criteria, and Guidelines Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
NCSC TECHNICAL REPORT - 004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
Library No. S-241,359

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release: Distribution Unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This technical report is a strawman update to Volume 2 of 4 of the procurement guideline series. The previous version was updated to deal with complex, evolving, multipolicy systems. It is written to help facilitate the acquisition of trusted computer systems in accordance with DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria." It is designed for new or experienced automated information system developers, purchasers, or program managers who must identify and satisfy requirements associated with security-relevant acquisitions. Information contained within this series will facilitate subsequent development of procurement guidance for future national criteria. This series also includes information being developed for certification and accreditation guidance. Finally this Volume 2 document addresses the way by which Trusted Computer System Evaluation Criteria, the Trusted Network Interpretation, and the Trusted Database Management System Interpretation using a new approach called Domains of Constant Policy are translated into language for use in the Request for Proposal (RFP) Specifications and Statements of Work.

14. SUBJECT TERMS
Security Requirements, Security Policy, Complex System Security, Certification and Accreditation Security, Automated Information Systems, Domains of Constant Policy

15. NUMBER OF PAGES
101

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	