Table of Contents

FOREWORD
ACKNOWLEDGMENTS

1 GENERAL INFORMATION
    1.1 INTRODUCTION
    1.2 PURPOSE
        1.2.1 FACILITATING THE CONTRACTING PROCESS
        1.2.2 FACILITATING FAIRNESS IN COMPETITIVE ACQUISITION
        1.2.3 MINIMIZING PROCUREMENT COST AND RISK
        1.2.4 ENSURING THE SOLICITATION IS COMPLETE BEFORE ISSUANCE
    1.3 SCOPE
    1.4 BACKGROUND

2 PROCUREMENT PROCESS

3 REQUEST FOR PROPOSAL
    3.1 SECTION C - DESCRIPTIONS/ SPECIFICATIONS
    3.2 SECTION C - STATEMENTS OF WORK (SOW)
    3.3 SECTION F - DELIVERIES AND PERFORMANCE
    3.4 SECTION H - SPECIAL CONTRACT REQUIREMENTS
    3.5 SECTION J - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENT
    3.6 SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS
    3.7 SECTION M - EVALUATION FACTORS FOR AWARD

4 OTHER CONSIDERATIONS
    4.1 NONMANDATORY REQUIREMENTS AND OPTIONS
    4.2 EVIDENCE AVAILABILITY
    4.3 DOCUMENTATION COST
    4.4 INTERPRETING THE TCSEC

5 STANDARD SOLICITATION LANGUAGE

RFP SECTION C -- DESCRIPTIONS/ SPECIFICATIONS/STATEMENTS OF WORK
C.1 SCOPE OF CONTRACT (AUTOMATED INFORMATION SYTEM -- EQUIPMENT,
SOFTWARE AND MAINTENANCE)
C.2 DETAILED SPECIFICATIONS
C.2.1 DISCRETIONARY ACCESS CONTROL SPECIFICATIONS
C.2.2 OBJECT REUSE SPECIFICATIONS
C.2.3 LABELS SPECIFICATIONS
C.2.4 LABEL INTEGRITY SPECIFICATIONS
C.2.5 EXPORTATION OF LABELED INFORMATION SPECIFICATIONS
C.2.6 EXPORTATION TO MULTILEVEL DEVICES SPECIFICATIONS
C.2.7 EXPORTATION TO SINGLE--LEVEL DEVICES SPECIFICATIONS
C.2.8 LABELING HUMAN--READABLE OUTPUT SPECIFICATIONS
C.2.9 SUBJECT SENSITIVITY LABELS SPECIFICATIONS
C.2.10 DEVICE LABELS SPECIFICATIONS
C.2.11 MANDATORY ACCESS CONTROL SPECIFICATIONS
C.2.12 IDENTIFICATION AND AUTHENTICATION SPECIFICATIONS
C.2.13 TRUSTED PATH SPECIFICATIONS
C.2.14 AUDIT SPECIFICATIONS
C.2.15 SYSTEM ARCHITECTURE SPECIFICATIONS

C.2.16 SYSTEM INTEGRITY SPECIFICATIONS
C.2.17 COVERT CHANNEL SPECIFICATIONS
C.2.18 TRUSTED FACILITY MANAGEMENT SPECIFICATIONS
C.2.19 TRUSTED RECOVERY SPECIFICATIONS
C.2.20 OPERATIONAL SECURITY SPECIFICATIONS
C.3 STATEMENTS OF WORK
C.3.1 COVERT CHANNEL ANALYSIS STATEMENT OF WORK
C.3.2 TRUSTED RECOVERY STATEMENT OF WORK
C.3.3 SECURITY TESTING STATEMENT OF WORK
C.3.4 DESIGN SPECIFICATION AND VERIFICATION STATEMENT OF WORK
C.3.5 CONFIGURATION MANAGEMENT STATEMENT OF WORK
C.3.6 TRUSTED DISTRIBUTION STATEMENT OF WORK
C.3.7 SECURITY FEATURES USER'S GUIDE STATEMENT OF WORK
C.3.8 TRUSTED FACILITY MANUAL STATEMENT OF WORK
C.3.10 DESIGN DOCUMENTATION STATEMENT OF WORK
RFP SECTION F -- DELIVERIES AND PERFORMANCE
RFP SECTION J -- LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS
RFP SECTION L -- INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS
RFP ATTACHMENT A - CONTRACT DATA REQUIREMENTS LIST (CDRL) FORM DD1423
RFP ATTACHMENT B - GLOSSARY
RFP ATTACHMENT C - ACRONYMS
RFP ATTACHMENT D - REFERENCES

APPENDIX A BIBLIOGRAPHY

FOREWORD

This guideline, Volume 2 of 4 in the Procurement Guideline Series, 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. Volume 2 addresses the way by which trusted computer system evaluation criteria are translated into language for use in the Request for Proposal Specifications and Statements of Work.

Information contained within the Procurement Guideline Series will facilitate subsequent development of procurement guidance for the "Federal Criteria." This series also includes information being developed for certification and accreditation guidance.

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

National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6000
ATTN: Standards, Criteria, and Guidelines Division

30 June 1993

Patrick R. Gallagher, Jr.
Director
National Computer Security Center

ACKNOWLEDGMENTS

This document has been produced under the guidance of U.S. Army Major Melvin L. DeVilbiss, assisted by Captain Michael Gold, Captain Scott M. Carlson and Mary Whittaker, from the National Security Agency (NSA). This version of this document was developed by Howard L. Johnson, Information Intelligence Sciences, Inc. Reviewing organizations supporting this effort, besides many NSA organizations, included: Contel Federal Systems; CTA, Inc; DCA; DLA; DOE; Grumman Data Systems; GSA; MITRE; USA, CECOM; USA, OSA; USAF, USCINCPAC/ C3; USAF, AFCC; USAF, AFCSC; USMC; USN, ITAC; USN, NCTC; and USN, NISMC. Individuals in these organizations gave generously of their time and expertise in the useful review and critique of this document.

LIST OF FIGURES

Figure 2-1 Security Related Areas 5

LIST OF TABLES

Table 1 Procurement Guideline Series 1

Table 2 RFP Organization 7

Table 3 Data Deliverables 37

1 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 and more complete titles in the Bibliography). This document is the second volume. These guidelines are intended for Federal agency use in acquiring trusted systems.

Table 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 (this guideline).

Computer Security Contract Data Requirements List and Data Item Descriptions Tutorial (to be published in 1993).

How to Evaluate a Bidder's Proposal Document---An Aid to Procurement Initiators and Contractors (to be published in 1993).

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 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; and the Specification and Statement of Work (SOW). 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, provide uniformity in competitive acquisitions, minimize procurement cost and risk, avoid delays in the solicitation process, and help ensure the solicitation is complete before its issuance.

1.2.1 FACILITATING THE CONTRACTING PROCESS

This guideline provides Specification and Statement of Work contract language to procure a trusted system, hopefully satisfied by a product from the NSA Evaluated Product List (EPL). (Note: The EPL is found in the

Information Systems Security Products and Services Catalogue.) This guideline 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 an RFP. The language duplicates the words and intent of the TCSEC.

1.2.2 FACILITATING FAIRNESS IN COMPETITIVE ACQUISITION

The guidelines in this document support the procurement of EPL products and can only be implemented if the requirements for fair competition are satisfied. 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 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 a 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 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.

If there are fewer than five items on the EPL meeting the stated requirements (not just security requirements), the RFP will not dictate that an item come from the EPL. Also, 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 cannot 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 factor for source selection.

1.2.4 ENSURING THE SOLICITATION IS COMPLETE BEFORE ISSUANCE

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

1.3 SCOPE

This guideline reformates and reorders the requirements into a form suitable for use in contractual documents and does not revise the words in DoD 5200.28-STD. This document might be thought of as an adaptation of the TCSEC for procurement. Procurement considerations are documented within the guideline to advise the procurement initiator of factors that may influence procurement decisions, including cost control. All of the factors are addressed as possible augmentations to the specification language provided.

This set of four acquisition documents is not to be misunderstood as DoD policy when it comes to addressing the situation of acquiring complex systems composed of many heterogeneous components. The reason is that the DoD policy has not been finalized that addresses systems with combinations of EPL products and "built and certified" system entities, which may or may

not use Division/Class criteria as requirements from DoD 5200.28- STD.

What will be required for more complicated systems will be a policy for integrating entities, to include determining interface requirements and global policies to be supported across entities. As soon as these composition policies are issued by the DoD, this guideline series will be updated to reflect policy changes. In the meantime, for Program Managers faced with the more complicated situations not currently dealt with in this series, it is hoped that the principles of these guidelines can be extrapolated, using guidance from the NCSC-TG-005, Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria (TCSEC); NCSC-TG-021, Trusted Database Management System Interpretation (TDI) of The Trusted Computer System Evaluation Criteria; and NCSC-TG-009, Computer Security Subsystem Interpretation (CSSI) of the Trusted Computer System Evaluation Criteria.

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 that 1) 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.

2 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.

The procurement process begins with various Government personnel determining operational requirements. Personnel include, but are not limited to, mission

users, Program Managers, and acquisition representatives. The primary goals during this phase include determining the Division/Class and mode of operation, as well as identifying the required security features and assurances.

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.

Physical Security

Communications Security

Procedural Security

Emission Security

Personnel Security

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 using this guideline. 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.

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 REQUEST FOR PROPOSAL

The 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 2). 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 2: RFP Organization

Letter	Section Title
A	Solicitation/Contract Form,Standard Form 33
B	Supplies or Services with Prices and Costs
C	Descriptions/Specifications/Statement 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 Specification or Requirements section that lays out the features and capabilities to included in the system to satisfy mission security requirements. The 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 of the 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 ATTACHMENT

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). It references specific Data Item Description (DID) requirements, which are provided in Volume 3 of the Procurement Guideline Series and also are referenced in RFP Attachment A contained in Chapter 5. 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 DID that specifies the document's content and format. Where requirements differ, there are unique DIDs for each Division/Class.

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

d. References. References have been identified for incorporation into the RFP. Terms support and are compatible with the specification language, and as such, become an integral part. The references are for technical supporting information and should not be interpreted as requirements. References are

included as RFP Attachment D 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 this guideline series.

4 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 nonmandatory 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.

Nonmandatory 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 nonmandatory 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 that are not necessarily 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

Though a vendor supplies NSA with evidence to support a product evaluation, the Government does not necessarily have 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 and then place the responsibility for 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 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 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 the RFP.

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).

Topics in Section C are divided into paragraphs as follows:

a. Text of the Specification or Statement of Work. These are words or references to words suggested for inclusion in the RFP.

b. 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 be redundantly 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.

c. 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 automatically intend their inclusion in the RFP. Only if the procurement initiator decides to make them requirements will they be included in the RFP.

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.

RFP SECTION C -- DESCRIPTIONS/SPECIFICATIONS/STATEMENTS OF WORK

C.1 SCOPE OF CONTRACT (AUTOMATED INFORMATION SYTEM -- 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 DETAILED SPECIFICATIONS

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.

C.2.1 DISCRETIONARY ACCESS CONTROL SPECIFICATIONS 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.

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.

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 a 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.2.2 OBJECT REUSE SPECIFICATIONS

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 2.2.1.2.

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.

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.

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 deallocatation.

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.2.3 LABELS SPECIFICATIONS

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.

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.

Important References

(None)

Labels Procurement Considerations

The tranquillity 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 signalling channels when untrusted subjects are able to detect changes in these variables by observing system behavior.

C.2.4 LABEL INTEGRITY SPECIFICATIONS

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.

Important References

None

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.2.5 EXPORTATION OF LABELED INFORMATION SPECIFICATIONS

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.

Important References

None

Exportation of Labeled Information Procurement Considerations

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

C.2.6 EXPORTATION TO MULTILEVEL DEVICES SPECIFICATIONS

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.

Important References

None

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.2.7 EXPORTATION TO SINGLE--LEVEL DEVICES SPECIFICATIONS

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 2.2.1.3.2.2.

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.

Important References

None

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 tranquillity must be observed during configuration change with a positive action to ensure the level of the device is known to users and observed by the reference validation mechanism.

C.2.8 LABELING HUMAN--READABLE OUTPUT SPECIFICATIONS

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.

Important References

None

Labeling Human--Readable Output Procurement Considerations

The System Administrator is the "user" designated to specify 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.2.9 SUBJECT SENSITIVITY LABELS SPECIFICATIONS 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.

Important References

None

Subject Sensitivity Labels Procurement Considerations

None

C.2.10 DEVICE LABELS SPECIFICATIONS

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.

Important References

None

Device Labels Procurement Considerations

None

C.2.11 MANDATORY ACCESS CONTROL SPECIFICATIONS

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 3.2.1.4.

For Class B3, repeat TCSEC Section 3.3.1.4.

For Class A1, repeat TCSEC Section 4.1.1.4.

TCSEC Section 9.0, "A Guideline on Configuring Mandatory Access Control Features."

Important References

None

Mandatory Access Control Procurement Considerations

None

C.2.12 IDENTIFICATION AND AUTHENTICATION SPECIFICATIONS

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.

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.

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.

(Classes 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.2.13 TRUSTED PATH SPECIFICATIONS

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.

Important References

None

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.2.14 AUDIT SPECIFICATIONS

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.

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.

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.

(Classes 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.

(Classes 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.2.15 SYSTEM ARCHITECTURE SPECIFICATIONS

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.

Important References

None

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 Base 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.2.16 SYSTEM INTEGRITY SPECIFICATIONS

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.

Important References

None

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.2.17 COVERT CHANNEL SPECIFICATIONS

Text of the Specification

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

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."

Covert Channel Procurement 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.2.18 TRUSTED FACILITY MANAGEMENT SPECIFICATIONS 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 2.2.3.1.4.

For Class B1, repeat TCSEC Section 3.1.3.1.4.

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.

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.

Trusted Facility Management Procurement Considerations

The TCSEC addresses System Administrator functions and operator functions and specifically identifies the Automated Data Processing (ADP) 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 title 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.2.19 TRUSTED RECOVERY SPECIFICATIONS

Text of the Specification

(For B3 through A1) Based on the recommendations of a trusted recovery decision, mechanisms shall be provided to assure that, along with procedures, recovery without a protection compromise is obtained after a computer system failure or other discontinuity.

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.

Trusted Recovery Procurement 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.

C.2.20 OPERATIONAL SECURITY SPECIFICATIONS

Text of the Specification

The bidder shall consider and/or recommend security support other than COMPUSEC, especially physical security, emission security, and communications security, 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.

Important References

None

Operational Security Procurement Considerations

The procurement initiator, working with the DAA, shall specify the operational security specifications in this section of the RFP. The following candidate list should be considered along with any others identified:

Division/Class to be satisfied.

Security levels supported.

Security clearances supported.

Security mode(s) to be supported.

Categories, compartments, and caveats supported with rules of support.

Statement of all interfaces and any interface policy required to be supported.

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.

C.3 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 SOW describe the work the contractor is expected to do. The specification of the deliverable is accomplished within a CDRL and its associated DID. Here we have provided sample CDRL numbers to correspond with Section F.

C.3.1 COVERT CHANNEL ANALYSIS STATEMENT OF WORK 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.

(Classes B2--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.

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."

Covert Channel Analysis Procurement Considerations

None

C.3.2 TRUSTED RECOVERY STATEMENT OF WORK

Text of the Statement of Work

(Classes B3--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.

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.

Trusted Recovery Procurement Considerations

None

C.3.3 SECURITY TESTING STATEMENT OF WORK

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 C.3.9, "Test Documentation Statement of Work."

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.

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.3.4 DESIGN SPECIFICATION AND VERIFICATION STATEMENT OF WORK

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.

(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 C.3.10, "Design Documentation Statement of Work." Subsequent deliveries shall be delivered under this task.

(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 C.3.10, "Design Documentation Statement of Work." Subsequent deliveries shall be delivered under this task.

(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 C.3.10, "Design Documentation Statement of Work." Subsequent deliveries shall be delivered under this task.

(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 C.3.10, "Design Documentation Statement of Work." Subsequent deliveries shall be delivered under this task.

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.

Design Specification and Verification Procurement 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.

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

C.3.5 CONFIGURATION MANAGEMENT STATEMENT OF WORK

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.

(Classes B2--A1) Prepare and deliver the TCB Configuration Management Plan in accordance with CDRL 011. One section of this document is originated under Section C.3.6, "Trusted Distribution Statement of Work."

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.

Configuration Management Procurement Considerations

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

(Classes 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.3.6 TRUSTED DISTRIBUTION STATEMENT OF WORK

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 Section C.3.5, "Configuration Management Statement of Work."

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.

Trusted Distribution Procurement Considerations

None

C.3.7 SECURITY FEATURES USER'S GUIDE STATEMENT OF WORK

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.

(Classes C2--A1) The contractor shall produce and deliver the Security Features Users Guide in accordance with CDRL 001.

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.

Security Features User's Guide Procurement 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.3.8 TRUSTED FACILITY MANUAL STATEMENT OF WORK 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.

(Classes C2--A1) The contractor shall deliver the Trusted Facility Manual in accordance with CDRL 002.

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.

Trusted Facility Manual Procurement Considerations

The contractor should conduct an analysis to identify the functions performed by the role of the System Administrator. This analysis should identify all nonsecurity 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.3.9 TEST DOCUMENTATION STATEMENT OF WORK

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.

(Classes C2--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 Section C.3.3, "Security Testing

Statement of Work."

Important References

None

Security Testing Procurement Considerations

The contractor should analyze the sensitivity of information processed on the delivered system, the desired mode of operation, and the 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 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 the development. These 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.3.10 DESIGN DOCUMENTATION STATEMENT OF WORK

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.

(Class C2)

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

(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 C.3.4, "Design

Specification and Verification Statement of Work."

Initial delivery of CDRL 008 is addressed under this task. Subsequent deliveries shall be delivered under Section C.3.4, "Design Specification and Verification Statement of Work."

(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 C.3.4, "Design Specification and Verification Statement of Work."

(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 C.3.4, "Design Specification and Verification Statement of Work."

(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 C.3.4, "Design Specification and Verification Statement of Work."

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.

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 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.

RFP SECTION F -- DELIVERIES AND PERFORMANCE

Text of Section F

(Class 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.3.6, "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.

Table 3: DATA DELIVERABLES

CLASS RANGE	CDRL*	DOCUMENT	SOWs
C2-A1	CDRL 001	Security Feature User's Guide DI-MCCR-81349	C.3.7
C2-A1	CDRL 002	Trusted Facility Manual DI-TMSS-81352	C.3.2, C.3.8
C2-A1	CDRL 003	Philosophy of Protection DI-MISC-81348	C.3.10
B1	CDRL 004	Informal Security Policy Model DI-MISC-81341	C.3.4, C.3.10
B2-A1	CDRL 005	Formal Security Policy Model DI-MISC-81346	C.3.2, C.3.4, C.3.10
B2-A1	CDRL 006	Descriptive Top Level Specification DI-MISC-81342	C.3.2, C.3.4, C.3.10
A1	CDRL 007	Formal Top Level Specification DI-MISC-81347	C.3.4, C.3.10
C2-A1	CDRL 008	Design Specification DI-MCCR-81344	C.3.2, C.3.4, C.3.10
B3-A1	CDRL 009	Trusted Computing Base Verification Report DI-MISC-81350	C.3.4
B2-A1	CDRL 010	Covert Channel Analysis Report DI-MISC-81345	C.3.1

B2-A1	CDRL 011	Trusted Computing Base Configuration Management Plan DI-CMAN-81343	C.3.5, C.3.6
C2-A1	CDRL 012	Security Test Plan DI-NDTI-81351	C.3.2, C.3.9
C2-A1	CDRL 013	Test Procedure DI-NDTI-80603	C.3.9
C2-A1	CDRL 014	Test/Inspection Reports DI-NDTI-80809A	C.3.3, C.3.9

---

* 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.

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.

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.)

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 of an audit trail of accesses and objects the TCB protects.

(Classes B1--A1) The bidder shall describe the operator and system administrator functions related to security, to include changing the security characteristics of a user.

(Classes 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.

(Classes B1--A1) The bidder shall identify specific TCB protection mechanisms with an explanation given to show that they satisfy the model.

(Classes B2--A1) The bidder shall describe the approach to covert channel analysis.

(Classes B2--A1) The bidder shall provide a descriptive top level specification.

(Class A1) A formal top level specification shall be provided.

(Classes 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.

(Classes B3--A1) The bidder shall identify the functions performed by the System Administrator.

(Class 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

RFP ATTACHMENT B - GLOSSARY

Text of the Glossary

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

The ADP system definition used in the TCSEC also should be treated as the definition of 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.

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

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

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.

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-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-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.

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 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.

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).

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," (Draft).

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."