Computer Security
Contract Data Requirements List
and Data Item Description
Tutorial

Table of Contents

FOREWORD

This guideline, Volume 3 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 3 explains Contract Data Requirements Lists (CDRLs) and Data Item Description (DIDs) and their use in the acquisition process.

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

28 February 1994

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

ACKNOWLEDGEMENTS

Special recognition is extended to MAJ (USA) Mel DeVilbiss and CPT (USA) Scott M. Carlson, National Security Agency (NSA), who integrated theory, policy, and practice into, and directed the production of this document.

Acknowledgement is also given to the primary author, Joan Fowler, Grumman Data Systems (GDS); and the contributions of Dan Gambel, GDS; Nicholas Pantiuk, GDS; Virgil Gibson, GDS; Yvonne Smith, GDS; Judy Hemenway, GDS and Howard Johnson, Information Intelligence Sciences, Inc.

Organizations that were particularly helpful in providing constructive reviews and advice besides many NSA organizations, included: Contel Federal Systems; CTA, Inc.; DCA; DLA; DOE; GSA; MITRE; NISMC; USA, CECOM; USA, OSA; USAF, AFCC; USAF, AFCSC; USAF, USCINCPAC/C3; USMC; USN, ITAC; USN, NCTC; and USN, NISMC.

Special thanks to Carol Oakes, Senior Technical Editor, MITRE, for her assistance with the final editing of this guideline.

LIST OF TABLES

LIST OF FIGURES

PREFACE

This guideline is intended to be used by Federal Agencies to facilitate the definition of computer security deliverables required in the acquisition of trusted products.

This guideline is Volume 3 of a 4-volume series of Automated Information System (AIS) procurement guidelines produced by the National Computer Security Center (NCSC). The complete set of documents is intended to help clarify the complex issues associated with the acquisition process relevant to computers, security, and contracting by explaining to procurement initiators specification and Statement of Work (SOW) procedures to follow for including computer security requirements in procurements. Volume 1, An Introduction to Procurement Initiators on Computer Security Requirements, provides guidance to promote the understanding of requirements and guide the acquisition of secure products within the DoD. Volume 2, Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators, provides SOW contract language for the specification of Evaluated Products List (EPL) commercial products or their equivalents. Volume 4, How to Evaluate a Bidder`s Proposal Document - An Aid to Procurement Initiators and Contractors, provides specific guidance for a procurement initiator in writing a Request for Proposal for computer security systems.

The material contained herein as Volume 3 specifies the data deliverables to meet security assurance needs by providing guidance on Contract Data Requirements Lists (CDRLs) and their associated Data Item Descriptions (DIDs).

1 GENERAL INFORMATION

1.1 Purpose and Scope

This guideline explains Contract Data Requirements Lists (CDRLs) and Data Item Descriptions (DIDs) and their use in the acquisition process, specifically the acquisition of data that supports trusted products. The guideline provides instructions that may be used in tailoring DIDs to comply with the various levels of trust specified by Department of Defense, (DoD) 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC). Sample CDRLs are provided in Appendix A, and the actual security DIDs are included in Appendix B.

This guideline is intended for use by DoD procurement initiators when considering the acquisition of trusted computer products. The emphasis of the guideline is on the data requirements for products.

Many trusted data requirements dictate the documentation required for integration, testing, assurance, certification, and accreditation. Additionally, there are numerous documentation requirements for general software (e.g., Defense System Software Development, Military Standard (MIL-STD)-2167A). This guideline addresses only the data requirements that are specifically required by the TCSEC.

Finally, this guideline is geared toward the data requirements involved in the acquisition of Evaluated Products List (EPL) Commercial Off-the-Shelf (COTS) packages. However, the data requirements are the same whether the product is on the EPL or not. Therefore, this guideline is applicable to the data requirements for any acquisition in which security is a factor.

The following limitations should be noted when using this guideline:

*The procurement initiator is responsible under Enclosure 4 of Department of Defense Directive (DoDD) 5200.28 for assessing the minimum Automated Information System (AIS) computer-based security requirements for the mission profile being acquired. The result of this assessment is a TCSEC Class that is to be used to index into the appropriate sections of this guideline. It is not sufficient only to quote a TCSEC Class in Requests for Proposal (RFPs) -- all of the individual requirements must be included in the RFP.

*This is not a complete acquisition guideline; it is a guideline to procure only security-related documentation. Only the requirements of the CDRL and DID sections of an RFP are addressed in this guideline.

*This document is not a revision or interpretation of the TCSEC; it is a reformatting and reordering into a form suitable for DIDs and the use of these DIDs. There is no intent to change the TCSEC or any vendor-specific interpretations of the TCSEC in this document.

This guideline will facilitate the acquisition and proliferation of products on the EPL. The guideline is intended to enable the procurement initiator to obtain security documentation for those EPL products that are available and have documentation.

If a product is evaluated as meeting a TCSEC class, then its evaluation and evaluation documentation remains valid (i.e., nothing in this guideline is to be interpreted as invalidating an EPL evaluation). However, since products not yet on the EPL may also be used to satisfy an acquisition, the cost advantage of having completed the EPL evaluation documentation provides an incentive for industry to submit products for evaluation. Once evaluated and on the EPL, the products can be proposed at a lower risk and cost in meeting government requirements at certain levels and, depending on the product, without modification. This approach provides a competitive advantage to those companies that expend the effort to obtain product evaluation on the EPL with the associated evaluation documentation, and provides a cost savings to the government.

1.2 Background

The CDRLs and DIDs play an important part in the acquisition of a product and its documentation. They are the vehicle by which the government is able to procure the necessary documentation to verify the design and implementation, and to use the product operationally.

The acquisition process (as defined in DoDD 5000.1) is a directed, funded effort that is designed to provide a new or improved capability in response to a validated need. The directive establishes a disciplined approach for translating operational needs into a stable, affordable program.

For the purposes of this guideline, the most important process in acquiring documentation for trusted products is the definition of the documentation required. This is done in the RFP, which is the most widely used document for acquisitions. The key components of the RFP package are description/specification; special contract requirements; list of documents, exhibits, and other attachments; and instructions, conditions, and notices to offerors.

The description/specification section of an RFP describes the mandatory technical and performance requirements to the contractor. It contains a Statement of Work (SOW) that identifies the specific tasks the contractor will perform during the contract period as well as the specification containing the definition/requirements of the acquisition. (This definition of the entity being acquired becomes the target for the security documentation.) The SOW also provides the opportunity to require delivery of information or specific data. This is done by referencing the appropriate CDRL number in the SOW paragraph. The information or specific data are a by-product of the actual SOW task. Thus, each SOW task normally refers to one or more CDRL items. The data referenced by the CDRL could be a list, plan, manual, computer-produced file or program, or a report.

The CDRL identifies the data that the contractor is required to prepare and deliver as part of the contract. The CDRL is also the vehicle by which data delivery dates are established, as well as providing delivery instructions and any other special requirements (e.g., number of copies). Each CDRL refers, in turn, to one DID. The DID should be referred to by the latest revision number and the name.

The DID specifies the actual content and format of the deliverable data, and therefore it drives the effort required to prepare the data item. In most acquisitions, the government reviews the documentation delivered with the product or service and uses it to assess whether all contractual requirements have been satisfied. Currently, about 2,000 standard approved DIDs exist. These DIDs were created by various DoD offices, forwarded through channels to the DoD Data Administrator, and subsequently approved for general use in contracts.

The DoD guide to the available DIDs is published semiannually as the Acquisition Management Systems and Data Requirements Control List (AMSDL). The AMSDL lists all standard DIDs in three different sequences: numerical, keyword (indexed), and functional area program category. It also provides a list of superseded and deleted DIDs. The DID numbers on the AMSDL are frequently changing when new DIDs supersede other DIDs. Less frequently, DID names change. It is a good habit to use both the DID number and name whenever referring to a DID.

The DIDs needed for security-relevant documentation are very specific in nature. Only recently has the AMSDL listed all the DIDs required to satisfy TCSEC requirements for documentation. We have included these DIDs in Appendix B of this guideline for the reader's convenience.

The special contract requirements section of the RFP contains clauses that are unique and specially tailored for each acquisition. The attachments section contains a list of all 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. For example, the CDRLs would be one attachment. The actual exhibits and attachments, including the CDRLs and DIDs, are physically appended to the end of the RFP.

Finally, the instructions section of the solicitation contains the instructions, conditions, and notices to offerors of the acquisition, covering such areas as proposal format, oral presentations, and the proposal preparation instructions.

1.3 Structure of the Guideline

The remainder of this guideline has four sections and five appendixes. Section 2, "Security Documentation," introduces the TCSEC requirements for documentation, the documentation that will typically be available with COTS products, and the role and placement of security documentation in the life cycle of a program. Section 3, "Contract Data Requirements List Issues," introduces a CDRL, with an explanation of each block on the CDRL. Section 4, "Data Item Description Modification," presents an introduction to DIDs and general guidelines on the tailoring of DIDs. Section 5, "Data Item Description Tailoring Instructions," describes the format of DIDs and provides both general and specific guidelines on the tailoring of the security DIDs.

Appendix A contains sample CDRLs for each relevant TCSEC class of each security document. These CDRLs can be used by the procurement initiator as sample CDRLs to include in an RFP. The italicized data should be replaced with project information. The blocks on the sample CDRLs that have been left blank should be filled in with the appropriate information for a specific RFP. Section 3 provides the guidance for completing these blocks, as well as a description of all of the blocks on the CDRL. Block 16 of the sample CDRLs is especially noteworthy because it contains all pertinent data item information not specified elsewhere on the form and any required amplifications of other block inputs. This block can be used as shown in the sample.

Appendix B contains 14 AMSDL approved Security DIDs that describe all of the documentation required by the TCSEC. Each DID can be included in an RFP with a corresponding CDRL to tailor the DID for the specific RFP.

Appendixes C, D, and E contain the References, Glossary, and Acronyms, respectively. These appendixes provide a common understanding of the terms and references used in this guideline.

2 SECURITY DOCUMENTATION

2.1 TCSEC Documentation Requirements

The Trusted Computer System Evaluation Criteria (TCSEC) requirements for documentation allow the government to ensure that the design of the Trusted Computing Base (TCB) is such that the defined security policy will be enforced. The security policy is defined by applicable laws, regulations, and directives. Additionally, this documentation provides the guidance for the user and the administrator to securely operate the product.

The security documentation requirements in the TCSEC are defined for each class. As with the functional requirements for trusted products, the documentation requirements for the most part are cumulative. This means that generally the documentation requirements at the lower class levels are usually also required at the upper class levels, with additional requirements added at the upper class levels. This is not always true for a specific document.

The level of classification of all of these security documents is determined by the classification of the processing and information being described. Naturally, if the source code or design that is described in the security documentation is classified, then the documents describing this source code or design in detail will also be classified. At times, no single portion of the source code is classified, but the combination of all the source code is classified. If this is the case, then the combination of all of the detailed documentation would be classified.

Documentation required by the TCSEC falls into three high-level categories: Operational Manuals, Design Documentation, and Assurance Documentation. The descriptions below for each of these three categories discuss the general contents of the documents included in the category.

2.1.1 Operational Manuals

The Operational Manuals include the Security Features User's Guide (SFUG) and the Trusted Facility Manual (TFM). The SFUG identifies techniques for making effective use of the security features. It provides the necessary information to understand and use the Discretionary and Mandatory Access Control mechanisms that protect information processed or stored.

The TFM explains the roles of the Security Administrator, System Administrator, and System Operator in establishing, operating, and maintaining a secure environment. It describes the procedures for selecting security options to ensure that the operational requirements will be met in a secure manner. The level of detail of the TFM spans the gap between the user-oriented SFUG and the security engineer-oriented design documentation.

2.1.2 Design Documentation

The design documentation includes the Philosophy of Protection Report, the Informal and Formal Security Policy Models, the Descriptive Top-Level Specification (DTLS), the Formal Top-Level Specification (FTLS), the Design Specification, and the TCB Verification Report.

The Philosophy of Protection Report provides a description of the security policy for the product. It also contains the overall high-level design of a TCB, delineating each of the protection mechanisms employed to enforce the policy.

An informal security policy model is an abstract representation of a TCB and the security policy enforced by the TCB. The Informal Security Policy Model document contains the informal security policy model, its associated convincing assurance arguments, and supporting explanations and documentation for both the model and assurance arguments. The model consists of two segments: (1) an informal description of the policy that is to be enforced by the TCB, and (2) an informal description of the abstract protection mechanism(s) within the TCB, which enforce the described policy. The model includes the representation of the initial state of the TCB; the representation of subjects, objects, modes of access, and security labels; the set of security properties enforced by the TCB; and the representations of the operations performed.

A formal security policy model is a mathematically precise abstract representation of a security policy and the abstract protection mechanisms that enforce the policy. To be acceptable as a basis for a TCB, the model must be supported by formal proof. The Formal Security Policy Model document contains the formal security policy model, its associated proofs, and the supporting explanations and documentation for both the model and proofs. The model contained in the Formal Security Policy Model document consists of two segments: (1) the mathematical representation of the policy, and (2) the mathematical representation of the abstract protection mechanism(s) within the TCB.

The DTLS is a top-level specification using English language descriptions. It completely and accurately describes the TCB in terms of exceptions, error messages, and effects. The DTLS is an accurate description of the TCB interface. It describes the security capabilities in functional terms and concepts, and therefore takes the broad form of a "security features functional description." The DTLS is traceable to the formal security policy model.

The FTLS is a mathematically precise abstract representation of the TCB. The TCSEC requires that the FTLS provide an accurate description of the TCB interface; describe the TCB in terms of exceptions, error messages, and effects; and include hardware or firmware elements if their properties are visible at the TCB interface. The FTLS document contains the Formal Top-Level Specification, its associated proofs and assurance arguments, and supporting explanations and documentation for the specification, proofs, and assurance arguments.

The Design Specification demonstrates that correct implementation and enforcement of the security policy exists in the TCB. It explains the protection mechanisms of the TCB to the extent that the effect of a change on the TCB can be evaluated prior to a change being performed. The Design Specification contains enough information so that it may serve as a guide to understanding the implementation of the TCB.

At the TCB Class B3 level, the TCB Verification Report provides the correspondence between the DTLS and the implementing source code to demonstrate that the TCB has been correctly and accurately implemented. At the TCB Class A1 level, the FTLS is mapped to the source code to demonstrate that the FTLS has been accurately implemented in the selected programming language (and hardware).

2.1.3 Assurance Documentation

The third category of documentation is the assurance documentation. This includes the Covert Channel Analysis (CCA) Report, the TCB Configuration Management (CM) Plan, and security test documents (Plan, Procedures, and Report).

The CCA Report is a description of the analysis of covert channels. Covert channels can be used to circumvent the access control features built into a TCB. There are two different types of malicious covert channels: storage channels and timing channels. These channels present opportunities to maliciously exploit characteristics of the TCB, or operating system-provided functions. By doing so, information can bypass mandatory access controls. The exploitation of covert channels causes unintentional side effects and unavoidably visible system calls/acknowledgments. For TCB classes B2, B3, and A1, covert channels must be identified, removed if possible, and their activity audited.

The TCB CM Plan details the configuration management procedures for a TCB. It addresses hardware, firmware, software, testing, and documentation. The TCB CM Plan indicates how the security requirements baseline will be maintained. It provides assurance that the security protections are safe from the introduction of improper hardware, firmware, and software during the developmental and operational life of the system. Finally, it describes the configuration control process, configuration management procedures, and review and approval procedures for changes to the security design implementation of the TCB.

The security test documentation consists of three documents, the Security Test Plan, Security Test Procedures, and the Security Test Report. The Security Test Plan provides the strategy to test the security mechanisms of the TCB. It also documents in detail the plan for conducting security tests (e.g., what security features will be tested, why they will be tested, and how they will be tested). Essentially, the Security Test Plan explains how the test results will be analyzed to show that the TCB will satisfy the security requirements. The Security Test Procedures identify the step-by-step testing operations to be performed in sufficient detail to permit total duplication of the test program. The document identifies the items to be tested, the test equipment and support required, the test conditions to be imposed, the parameters to be measured, and the pass/fail criteria against which the test results will be measured. Finally, the Security Test Report describes the tests performed, discusses the test analyses, and provides the results of the tests. The report includes all recorded test data or logs.

2.1.4 Documentation Presentation

The documentation requirements discussed in this subsection deal only with the TCSEC requirements for the documentation of a TCB. It does not deal with other documentation that should be written when following sound software engineering practices (e.g., MIL-STD-2167A documentation). Some of the TCSEC documentation, especially the security design and configuration management documentation, may seem redundant to the general software documentation. However, the security design and configuration management documentation has a specific purpose and should not be neglected. Depending on the program, it may make sense to incorporate the security design and configuration management documentation into the general documentation. This is a decision to be made by program personnel prior to release of the RFP. The security designing configuration management DIDs (included as Appendix B) can be tailored as stand-alone documents, brief documents with pointers to the standard design/configuration management documentation, or completely subsumed documents within the standard design/configuration management documentation.

Table 1: Documentation Requirements by TCSEC Class

DOCUMENTATION	TCSEC CLASS				
	C2	B1	B2	B3	A1
Security Features User`s Guide	X	X	X	X	X
Trusted Facility Manual	X	X	X	X	X
Philosophy of Protection	X	X	X	X	X
Informal Security Policy Model		Y			
Formal Security Policy Model		Y	X	X	X
Descriptive Top-Level Specification			X	X	X
Formal Top-Level Specification			X	X	X
Design Specification	X	X	X	X	X
TCB Verification Report				X	X
Covert Channel Analysis Report			X	X	X
TCB Configuration Management Plan			X	X	X
Security Test Plan	X	X	X	X	X
Test Procedure	X	X	X	X	X
Test/Inspection Reports	X	X	X	X	X

X = Required at the TCSEC Class

Y = For TCSEC Class B1, either an informal or a formal security policy model is required

Table 1 cross references the security documentation described above to the

TCSEC classes. An "X" indicates the class at which the TCSEC contains a requirement for the documentation. For those documents which are required at multiple classes, the specific requirements for the document change at each of the higher classes.

As reflected in Table 1, the required class for all of the security documentation (except the informal and formal security policy model) is explicitly defined in the TCSEC. The TCSEC requires either an informal or a formal security policy model at TCSEC Class B1. The determination of which security policy model should be required at TCSEC Class B1 should be made by the program office for each specific program.

2.2 COTS Documentation

When buying COTS software, certain documentation is available with a particular focus and level. The focus of the documentation is the generic product. The level of the security documentation depends on whether the product is on the EPL (or under evaluation) or simply being acquired without prior EPL status as a requirement.

Whether or not the product is on the EPL, generic user manuals are always available for any COTS product. These user manuals provide information on all of the features of the product, usually not just the security features. If the product requires an administrator, administrator manuals will be available. Design and test documentation, either for general features or security features, usually are not provided with COTS packages unless expressly purchased.

If the COTS product is on the EPL, a whole spectrum of TCSEC documents will be available for the class at which the product was evaluated. However, these documents (except the user and administrator manuals) are not normally included in the standard delivery of the product and must be specifically ordered for each procurement. Since these documents may be highly proprietary to the company developing the COTS product, the cost of the detailed documentation may be prohibitive to an acquisition. Careful assessment of the requirement for the detailed product documentation, particularly since the product is on the EPL, must be made to determine the cost-benefit trade-off for this documentation.

If the COTS product is under evaluation by the National Computer Security Center (NCSC), but has not yet passed evaluation, the stage that the product has reached in the evaluation will determine the amount of security documentation readily available for the product. The same caveats discussed above for COTS products on the EPL apply to those undergoing evaluation. However, the products which are under evaluation are by their very nature more advanced, since they are still under development and can make use of the latest technology for trusted products. Including products that are under evaluation benefits a program due to the volatile nature of security technology. On the other hand, there is also a greater risk in using a product that is undergoing evaluation. Such a product, being new, is less likely to have been tested in an operational environment. The product will not have as much, if any, field use from which to draw experience.

If the COTS product is not on the EPL, no security assurance documentation is likely to exist for the product. Therefore, any security documentation required for the product must be generated for the acquisition. Once again, depending on the detail of the documentation required, the cost of the development of this documentation may be prohibitive to the acquisition. This cost may include, for example, the procurement of a source code license for the product in order to have the data available to develop the security documentation. This prohibitive cost for source code licenses is especially true for closed proprietary systems. The cost may not be as prohibitive in an open systems environment, although developing documentation will always be substantially more expensive to the government than buying COTS documentation. Again, a cost-benefit analysis should be performed that includes the real requirements for detailed security documentation.

COTS product documentation can be a detailed description of the product. The DIDs for Commercial Off-the-Shelf (COTS) Manuals, DI-TMSS-80527, and Supplemental Data for Commercial Off-the-Shelf (COTS) Manuals, DI-TMSS-80528, should be addressed when requiring COTS documentation. Whatever method is used to request the COTS documentation, the documentation will be geared toward the generic design and use of the product. If the product must be modified or extended for a program, the COTS documentation for the product will not include these modifications and extensions, unless the modifications are performed by the vendor and the updated documentation is purchased during the acquisition.

2.3 Security Documentation in a Program Life Cycle

The role of security documentation in the procurement process and life cycle of a program is to provide a basis for trusting the hardware, firmware, and software mechanisms. This basis for trust must be clearly documented such that it is possible to independently examine the evidence to evaluate the sufficiency of the security mechanism(s).

The preparation of security documentation demands an engineering discipline be imposed on the development of the software. The use of a strict engineering discipline during development further contributes toward a more consistent implementation of the TCB. A result of this strict engineering discipline permeates the program, not just the TCB implementation.

The TCSEC describes the type of written evidence in the form of operational manuals and design and assurance documentation required for each class. During the procurement process, the required documentation must be explicitly defined. During the implementation process, this documentation must be developed, reviewed, and inspected to prove the ability of the security mechanisms to enforce the security policy. During the operational phase, the operational manuals for users and administrators are used to apply the provided security mechanisms. During any maintenance phase, the documentation is used to determine what effect a change may have on security. This evaluation must be accomplished prior to a change being performed. Finally, during the implementation, operational, and maintenance phases, configuration control verifies that only approved changes are included in the trusted product.

Security documentation is a subset of the software and hardware documentation required for a TCB. There are numerous documentation approaches and standards (e.g., MIL-STD-2167A) used today with their associated documentation requirements. The security documentation defined in this guideline is to be used in addition to the standard software and hardware documentation (e.g., Software Requirements Specifications, Software Design Documents, Interface Design Documents, or Software Test Plans). Security documentation is not a replacement for this standard documentation, nor is standard documentation a replacement for security documentation.

The security documentation defined in this guideline can fit very easily into the timeline defined by MIL-STD-2167A. Figure 1 illustrates the security documentation along with interdependencies and relative delivery schedules. The reviews on the timeline are the MIL-STD-2167A reviews. Each of the documents can be acquired, along with the standard software and hardware documentation, within the standard MIL-STD-2167A review cycle. Several iterations may be required before some security documents may be finalized. Additionally, although all of the lines in Figure 1 point downward, it may be necessary in any acquisition to change documents and models to reflect the actual implementation. As changes are made in a program for a multitude of reasons, the earlier documents may require revision. For simplification, no feedback mechanism is reflected in the figure.

Figure 2 relates the test documentation to other security documentation. The dotted box containing "Risk Assessment" indicates a process that is not performed by the developer/integrator team. The risk assessment process identifies some acquisition-specific security requirements that need to be included in the System Specification. Additionally, the risk assessment process enumerates the specific system vulnerabilities that are used to develop the Security Test Plan.

3 CONTRACT DATA REQUIREMENTS LIST ISSUES

3.1 What is a Contract Data Requirements List?

A CDRL (DD Form 1423-1) delineates the data delivery requirements for data acquisitions resulting from a contractual task. It is used to specify the data to be delivered during a contract, the schedule for that delivery, and the form in which that delivery must be made. The CDRL designates the DID that will be used to define documentation and specifies any tailoring instructions for the DID. Figure 3 displays DD Form 1423-1.

3.2 Contract Data Requirements List Format

The CDRL form itself consists of 26 blocks. These blocks are expanded in accordance with DI-A-23434C, which is the DID for "List, Contract Data Requirements" (DD Form 1423-1). The information needed to request data is included in these blocks. They include:

*Block 1-Sequence Number

*Block 2-Title or Description of Data

*Block 3 -Subtitle

*Block 4-Authority (Data Item (or DID) Number)

*Block 5–Contract Reference

*Block 6–Technical Office

*Block 7 –DD Form 250 Requirement

*Block 8–Approval (APP) Code

*Block 9 –Input to Integrating Associated Contractor (IAC)

*Block 10–Frequency

*Block 11–As of Date

*Block 12 –Date for First Submission

*Block 13–Date of Subsequent Submission/Event Identification

*Block 14–Distribution and Addressees

*Block 15–Total

*Block 16–Remarks

*Block 17–26 – Not Contractual Information

A few of these blocks are critical in amplifying the delivery requirements of data. Block 16 is the most critical in that it is used to tailor the requirements of the DID to best suit the specific acquisition. Blocks 10 through 13 are also critical in defining the delivery schedule for the data. The following subsections describe the general instructions and information needed to complete each block on the CDRL. Appendix A contains sample CDRLs for each TCSEC class, as appropriate. These sample CDRLs can be used for any acquisition by completing the blocks left blank and replacing the italicized information.

3.2.1 Block 1: Sequence Number

Block 1 contains the sequence number for the data item. The practice usually adhered to is to start with "A001, A002,...." If separate groups of data items are required (e.g., over two fiscal periods or option periods), using "A00X" for one group (where "X" is used as a place holder and will have to be replaced with an appropriate number) and "B00X" for the second group is helpful.

3.2.2 Block 2: Title or Description of Data

Block 2 contains the exact title as it appears on the DID. For the security documentation contained in the sample CDRLs in Appendix A, the exact title of the DID is the title of the data item being acquired, except for the Test Procedures and Test Report. These two DIDs are generic; therefore, they are not specifically written for security test documentation.

3.2.3 Block 3: Subtitle

Block 3 contains the title of the data item if it differs from the title of the DID or requires further information. In Appendix A, the CDRLs for the Security Test Procedures and Security Test Report require further amplification as indicated in those CDRLs.

3.2.4 Block 4: Authority (Data Item (or DID) Number)

Block 4 contains the DID identification number including the revision letter and date from DD Form 1664 block 2. These are the instructions in DI-A-23434C. It is not ordinary practice to include the date in this block of the CDRL.

3.2.5 Block 5: Contract Reference

Block 5 contains the specific location of the contractual effort in the procurement instrument that will generate the requirement for the data item.

For the purposes of this guideline, the procurement instrument is the RFP and, specifically, the SOW (Section C of the RFP). The specific SOW paragraph (C.X, where X is a place holder which will have to be replaced with the appropriate number) should be cited in this block. (See Volume 2, pg. 11, of this Procurement Guideline series for more details.)

3.2.6 Block 6: Technical Office

Block 6 contains the office responsible for determining the technical adequacy of the data. This may be the accepting, requiring, using, or inspecting offices depending on the type of data and decisions made relative to quality assurance responsibilities. It is the responsibility of the procurement initiator to identify this office and include it in this block.

3.2.7 Block 7: DD Form 250 Requirement

Block 7 contains the designated location for performance of government inspection and acceptance. The acceptance indicated in this block is not the same as the approval of a document indicated in block 8.

This block has been left blank in the sample CDRLs in Appendix A. However, in actual CDRLs, a blank in this block indicates that the inspection and acceptance location is specified in Block 16. If this is not true for the specific acquisition, the block should indicate the location for the inspection and acceptance.

3.2.8 Block 8: Approval (APP) Code

Block 8 contains the appropriate approval for the document. An "A" indicates that advance written approval is required prior to either initial preparation or final acceptance of the document by the government, or prior to publication and distribution of the final version of the document to addressees in Block 14. Clarification of approval will be defined in Block 16. Also, if a preliminary draft is required, indication will be cited in Block 16 with the identification of which addressees will receive the review copies. When control of distribution by addressees listed in Block 14 to secondary addressees is required, the following code will be used: a "D" will be used to indicate that a distribution statement is required, or, an "N" will indicate that a distribution statement is not required. An "A" code may be combined with a "D" code, for "AD", to indicate that both approval and a distribution statement are required. An "A" code may be combined with an "N" code, for "AN", to indicate that approval is required, but a distribution statement is not required.

This block has been left blank in the sample CDRLs in Appendix A. It is the responsibility of the procurement initiator to identify the appropriate information for this block in the specific acquisition.

3.2.9 Block 9: Input to Integrating Associated Contractor (IAC)

If data are dependent upon the integrated result of specific inputs from other participating contractors or data are input to an IAC, Block 9 contains an "X". In all other cases, the block should remain blank.

This block is used if the government must provide input to a contractor so that the contractor can produce a document. For the data described in this guideline, this block will be left blank in most cases. This block is blank in the sample CDRLs in Appendix A.

3.2.10 Block 10: Frequency

Block 10 contains a frequency code for the data. In Appendix A, all of the CDRLs indicate "OTIME" (One Time) submission since all of these documents should be produced once for each release, phase, or version of a TCB in a single contract. If multiple releases, phases, or versions of the TCB exist in the acquisition plan, then multiple CDRLs using the same DID should be generated: one for each release, phase, or version. Additionally, there may be multiple drafts and a final version of the document, but the schedule and number of drafts and final are indicated in Block 16.

A frequent error in the content of this block is "ASREQ" (As Required) without amplification in Block 16. There is no way that a contractor can determine the cost of an "As Required" document during the proposal writing phase of a procurement. Therefore, in a proposal the contractor must assume "not required" for the frequency of delivery of documents with the "ASREQ" frequency. The result of this assumption is that the contractor will not include the cost of draft and final versions of a document in the price. Additionally, the government would not have the opportunity to conduct the draft and review cycle, which is beneficial to a complete document. The contractor may indicate that the draft and review cycle is to be done either as an option or through a task order, with the resulting additional cost to the contract. Therefore, it is always best to be explicit in stating the exact number of drafts that will be required for any data procured. This explicit definition does not belong in Block 10, but rather in Block 16.

3.2.11 Block 11: As of Date

Block 11 contains the date that the data will be received by the requiring office. If the data are constrained by a specific event or milestone, enter this constraint. If the data are submitted only once, enter the "as of" date (cutoff date).

This block has been left blank in the sample CDRLs in Appendix A. The milestones in Figure 1 should be used to constrain the data. Blocks 13 or 16 should be used for further explanation of the date in Block 11.

3.2.12 Block 12: Date for First Submission

Block 12 contains the date for initial data to be submitted to the government. If the first delivery is predicated on conditions, such as an event, enter "See Block 16" and state the conditions in Block 16. A table of codes shown in DI-A-23434C can be used for this block. However, this table does not include codes for any of the reviews currently used in the life cycle of an acquisition. Further, this table and all of the instructions for delivery dates in DI-A-23434C do not make provisions for the draft delivery, government comment, and final delivery cycle, which is most common and useful for security documentation.

All of the sample CDRLs in Appendix A have "See Block 16" in Block 12 because the first submission of all security documentation is predicated on an event, or a review. The documentation should be delivered prior to the review date. Again, the actual calendar date to which this event correlates should never be before the actual calendar date from Block 11.

The CDRLs in Appendix A use a review strategy of receiving draft documents 30 days before a milestone, government comments 45 days after receipt of draft, and final delivery 60 days after receipt of government comments. The number of days (i.e., 30 and 45) in this strategy has been arbitrarily defined for this guideline. These numbers should be modified to reflect the standard for the program office for a specific acquisition.

The sample CDRLs in Appendix A include formal reviews as the events that trigger the delivery of the security documentation. It is strongly encouraged that at least a variation of the review cycle be used for any acquisition. If, however, formal reviews are not planned for the program, then other events may be used that trigger the necessity for the documentation. An example is that the TFM and SFUG are needed before training can begin. Therefore, it is not an unreasonable solution to

require the delivery of these documents in draft form at a certain number of days prior to training for government review, and then the final version of the document to be delivered during training.

However, to request all of the security documentation at a single milestone in the program (when some of the documentation is dependent on other portions of the total set of security documentation), or to require all documentation to be delivered for the first time when the accreditation will begin, is counterproductive to the success of the program. This does not allow the contractor to develop the security documentation with the dependencies indicated in Figure 1, nor does it allow the government to review the work in progress and, if necessary, redirect the effort.

3.2.13 Block 13: Date of Subsequent Submission/Event Identification

Block 13 contains the date on which subsequent submissions of the data should be made. If the subsequent submissions are keyed to an event, "See Block 16" should be entered.

All of the sample CDRLs in Appendix A have "See Block 16" in Block 13 because subsequent submissions are predicated on an event, or a review, or the contractor receipt of government comments. The date of any subsequent submissions should never be prior to the date of the first submission.

The discussion on the events, which trigger the first submission of data (block 12) contained in the preceding subsection, applies to this block also. Blocks 12 and 13 should be consistent in their approaches. For example, if formal reviews are used in Block 12, formal reviews should also be used in Block 13. If, on the other hand, another type of event (e.g., start of training) is used in Block 12, that type of event should also be used in Block 13. This will help to avoid the problem of delivering subsequent submissions (Block 13) prior to the first submission (Block 12).

3.2.14 Block 14: Distribution and Addressees

Block 14 contains the code of addressees and the number of copies (regular and reproducible) to be sent to each addressee. Regular copies required should be indicated to the left of a slash mark and reproducible copies to the right (i.e., DDC 20/0). The type of the reproducible copies should be explained in Block 16. Regular copies are clean copies, and reproducible copies are copies on some reproducible medium (e.g., vellum, negatives). Since reproducible copies incur an additional cost to create (e.g., cost of the medium plus the cost of making the copy), this form of delivery should be limited to only those parties having a legitimate need for the item. The first addressee shown should be the acceptance activity, if acceptance by DD Form 250 is to be accomplished at the destination. This block may be continued in Block 16.

Documents are usually delivered via removable media, electronic connection, or hardcopy. Any other delivery instructions which are appropriate for the specific acquisition may be included in Block 16 of the CDRL. The Formal Top-Level Specification and the TCB Verification Report, unlike the other documents developed from the DIDs included in this tutorial, may consist of computer listings as opposed to text documentation. The CDRLs for these two documents should permit computer-readable media, the listings for which would be voluminous.

3.2.15 Block 15: Total

Block 15 contains the total number of regular and/or reproducible copies. This number may be obtained by adding all of the insertions in Block 14. Regular copies should be indicated to the left of the slash mark and reproducible copies to the right.

3.2.16 Block 16: Remarks

Block 16 contains all pertinent data item information not specified elsewhere on the form and any required amplification of other block inputs. Always enter the identification, "Block __" of the DD Form 1423-1 being addressed before each informational sentence(s).

Block 16 is also used to tailor the DID specified in the CDRL. Section 5 of this guideline discusses the specific tailoring instructions for each of the security DIDs.

3.2.17 Blocks 17 through 26

Blocks 17 through 26 do not cite contractual information but are used in negotiating and preparing the contract (not within the scope of this guideline).

4 DATA ITEM DESCRIPTION MODIFICATION

4.1 What is a Data Item Description?

A DID (DD Form 1664) delineates the data preparation instructions necessary to formulate a document. It is used to define the data required of a contractor, including the data content, preparation instructions, format, and intended use. DIDs are structured to facilitate the tailoring (deletion) of requirements not applicable to a specific acquisition. Cautions on the use of tailoring are included in subsection 4.3.

The AMSDL identifies all source documents and related DIDs approved for use in defense contracts. These DIDs are reviewed by a board before being included on the list. Once on the list, the DID is maintained by the originating component and the Office of Primary Responsibility (OPR). These DIDs are available for use by any government component. The DIDs included as Appendix B of this guideline are being listed in the AMSDL.

Occasionally, a documentation requirement exists for which a DID is not available on the AMSDL. One-time DIDs may be developed in this case for a specific acquisition. Cautions on the use of one-time DIDs are included in subsection 4.3. One-time DIDs may only be published by appropriate authorized DoD offices.

DIDs are used for various purposes during the life cycle of an acquisition. During the procurement process, a DID is used by the government to specify the deliverables that will be required during the contract. The contractor uses the DID to estimate the cost of the documentation delivery during contract performance.

During contract performance, a DID is used by a contractor to guide documentation development for a contract. A DID must have enough explicit direction for the development of the documentation. If this is not the case, there is no guarantee that the documentation delivery will satisfy the requirements of the government. However, oversimplifying the requirements of the document in a DID may prohibit the use of existing documentation.

Finally, a DID is used by the government to evaluate the completeness of documentation deliveries. It is the "ruler" that indicates what was supposed to be delivered, and, as such, it is used to determine whether the delivery has met the criteria of the DID. Using the DID, the government cannot evaluate the technical aspects of the deliverable, but is able to determine whether the document contains the correct types of information.

4.2 Tailoring Overview

Tailoring is the process of evaluating individual potential requirements in a selected DID to determine their pertinence and cost-effectiveness for a specific system acquisition, and tailoring (deleting) those requirements to ensure that each contributes to an optimal balance between need and cost. DIDs must be structured to facilitate the tailoring (deletion) of requirements not applicable to a specific acquisition (see DoD-STD-963A: Section 4.5.4). Thus, tailoring of DIDs involves deleting those requirements that are not needed. It is intended to eliminate unnecessary and duplicative requirements. For DIDs on the AMSDL, requirements may be deleted or partially deleted, but not modified to add requirements to the DID.

Tailoring should be performed during the acquisition process. As objectives and tasking change during that process, tailoring decisions for each contract will change accordingly. The tailoring for a given contract is an incremental activity. Draft tailoring prepared by the contracting agency will be refined based on inputs from the user and support personnel, potential bidders, and other interested parties.

General tailoring guidance is provided in Military Handbook (MIL-HDBK)-248B, Military Handbook, Acquisition Streamlining. MIL-HDBK-248B is the basis for the tailoring guidance in this guideline.

4.2.1 Reasons for Tailoring

Requirements that are not mandated by law or established DoD policy, and do not contribute to operational effectiveness and suitability or effective management of acquisition, operation, or support, should be excluded from an acquisition. Implementing policies in DoD organizations repeat and amplify this high-level statement. Therefore, the acquisition initiator should select and tailor technical requirements to acquire only those technical data essential to carrying out the acquisition strategy.

Advantages that can be achieved through tailoring to specific requirements of an acquisition are the following:

*Avoid unneeded activities, controls, and practices.

*Eliminate duplicative requirements that may be invoked when multiple DIDs are on contract.

*Expedite performance of a project by avoiding unnecessary requirements. This may reduce the schedule and allow the delivery of products sooner.

It is important to balance the tailoring decisions between near-term savings of cost and time and possible long-term adverse effects. Sample trade-offs made during the tailoring process are as follows:

*Eliminating requirements from user and administration documents can save time and money in the initial development, but may have severe negative effects on the long-term cost of using and supporting the program.

*Eliminating stages of testing can save time and money in the short term, but can result in reduced quality, and expensive and time-consuming rework if the product is delivered before it is ready.

*Reducing requirements from security analysis documentation can save time and money in the short term, but can result in loss of data and possibly a compromise if the product is not built securely.

*Reducing requirements for configuration management can save time and money in the short term, but can result in expensive and time-consuming recovery procedures if the program loses track of hardware, firmware, software, and documentation versions.

4.2.2 Tailoring Responsibilities

It is important for the government program manager to involve all key system acquisition participants in the tailoring process. These participants include:

*Technical staff in, and available to, the program office, such as software engineering, configuration management, security engineering, quality assurance, and test personnel.

*Contract Administration Service and contracting office personnel.

*User and support personnel.

*Development contractors. It is highly desirable to solicit potential contractor input early in the tailoring process. This may be done before the RFP, for a draft RFP, or for the final RFP.

In a best value environment, contractors may also be permitted to propose tailoring in their proposal, their Best and Final Offer (BAFO), and during contract negotiations in order to refine cost and schedule impacts.

This team approach has significant benefits. With each participant contributing specialized expertise, the government program manager can arrive at a sound, informed tailoring approach. However, it is essential that the security support personnel review the tailoring decisions to ensure that specified requirements are met. The final decisions, subject to appropriate review, remain the responsibility of the government program manager.

4.3 Cautions on Using Tailoring and One-Time DIDs

The two defined alternatives to using the standard AMSDL DIDs as they exist on the list are to tailor the DID for the specific operational environment and to develop one-time DIDs for the specific system.

Tailoring of DIDs, using Block 16 of the CDRL, is a very useful tool to procure only the documentation that is needed. However, tailoring can be overused. When a DID is tailored too much, security information that will be needed for certification, accreditation, or operational maintenance may be tailored out of the DID. If the security documentation that is needed during the entire life cycle is not complete, the cost of procuring the documentation at a later date may be prohibitive to the acquisition.

On the other hand, each of the DIDs included with this guideline has the requirements for the full spectrum of TCSEC classes. If the program aims at a particular TCSEC class, then the higher TCSEC class requirements should be tailored out of the DID. Failure to tailor out the higher TCSEC class documentation requirements may provide a prohibitive cost to the program. COTS documentation will not likely provide the assurance for a higher level than the product has been evaluated.

One-time DIDs are useful to address specific operational or environmental requirements. However, a one-time DID can cause the data to be more expensive, especially if the DID is too specific. One-time DIDs should never specify the format that must be used for any documentation. The chances of any COTS documentation complying with a specific format of a one-time DID are remote.

4.4 Tailoring Recommendations

There are general recommendations to be followed when using CDRLs to tailor security DIDs. The tailoring of formatting instructions can be useful and cost effective. However, the archiving of tailoring decisions protects decisions and avoids misunderstandings.

4.4.1 Formatting Tailoring Recommendations

The DID for any data item describes the specific contents of a document. However, when COTS documentation is preferred, the format of the document should not be defined by the government. Whenever it is cost-effective, data should be acquired in the format specified by the contractor rather than that of the government to enable and encourage the delivery of COTS documentation. Much of the basic data are prepared by the contractor in connection with design, development, testing, and manufacturing of a COTS product. In such instances, the cost impact of a government contract requirement for COTS data becomes significant only if the COTS documentation must be reformatted or delivered to meet unrealistic schedules.

4.4.2 Archiving Tailoring Decisions

The tailoring decisions made can be of use to responsible managers in the future and to other project managers who face similar tailoring decisions. A file should be established of the tailoring decisions, rationale for those decisions, and lessons learned as the project proceeds. This file will prevent future managers from inadvertently changing key decisions and will clarify the trade-offs and key considerations made in support of the tailoring decisions. This information should be available to all technical offices working on security.

5 DATA ITEM DESCRIPTION TAILORING INSTRUCTIONS

5.1 Data Item Description Format

The DID form itself consists of 11 blocks. These blocks are expanded in accordance with DoD-STD-963A, Preparation of Military Standard, Data Item

Descriptions. The information needed in the document is included in these blocks and shown in Appendix B. The blocks are:

*Block 1 – Title

*Block 2 – Identification Number

*Block 3 – Description/Purpose

*Block 4 – Approval Date

*Block 5 – Office of Primary Responsibility (OPR)

*Block 6 –Defense Technical Information Center (DTIC) Applicable and Government–Industry Data Exchange Program (GIDEP) Applicable

*Block 7 – Application/Interrelationship

*Block 8 – Approval Limitation

*Block 9 –Applicable Forms and Acquisition Management Systems Control (AMSC) Number

*Block 10 –Preparation Instructions

*Block 11 –Distribution Statement

The security DIDs included with this guideline, except the Test Procedure and Test/Inspection Reports, have a further breakdown to Block 10. [The Test Procedures and Test/Inspection Reports DIDs are generic DIDs that have not been written explicitly for security documentation. They need to be tailored to delete extraneous requirements that are not related to security.] Block 10.1 contains the format of the delivered document, and 10.1.1 contains the specific formatting instructions. All subsequent subsections in Block 10 contain the technical content requirements for the specific document, with Block 10.2 containing the requirements for all TCSEC classes and subsequent subsections containing the different class level specific documentation content requirements.

For CDRL, DID, and SOW correlation at each level of trust identified in the TCSEC, we refer the reader to pg. 41, Volume 2 of this Procurement Guideline series.

5.2 General Tailoring Instructions

There are some general tailoring instructions that apply to the security DIDs included in Appendix B of this guideline. The following subsections discuss the use of tailoring to allow evaluation documentation reuse for an acquisition, the subjective index, and other document referencing in the security documentation. These instructions apply to all of the security DIDs in Appendix B except for the Test Procedures and Test/Inspection Reports DIDs. The Test Procedures and Test/Inspection Reports DIDs are generic DIDs that can be easily applied for security documentation.

5.2.1 Tailoring to Allow NCSC-Approved Documentation

None of the DIDs included, or any of the tailoring instructions presented here, preclude the use of the same documentation accepted by the NCSC during the evaluation of a product. Words should be included either in the SOW or in Block 16 on the CDRL indicating that the format agreed on during evaluation is acceptable for the acquisition.

5.2.2 Subjective Index

A subjective index is required in subsection 10.1, subparagraph l, of all the DIDs written for this guideline. This subjective index can be very useful for the reader of a document to find a specific subject in a large document. However, an extensive index can be very expensive to produce. The cost of the index will be transferred to the government. If the subjective index is determined by the government to be needed, that portion of subsection 10.1 should not be tailored out of the DID. However, if the index is not necessary for the acquisition, "Delete 10.1 subparagraph l" should be included in Block 16 of the CDRL.

5.2.3 Referencing

All of the documents created from the DIDs in this guideline, except the Security Features User's Guide and the Security Test Plan, should use referencing to other documents to satisfy the requirements of the DID. The documents that can be easily referenced are government-furnished documents, prior deliverables of the contract, or commercial documentation. All of this documentation is readily available to the government. Any references should summarize the content of the referenced material. An explicit reference to the original material (e.g., subparagraph, table, figure) should be provided. These reference requirements enable the reader of the security document to determine whether it is worthwhile to refer to the other document prior to referencing it. A note in Block 16 of the CDRL or the SOW can allow/ encourage this referencing.

The SFUG and Security Test Plan should not permit referencing unless authorized by the procuring activity or as specified in the CDRL. The SFUG is a user's guide that would be cumbersome to use if it were not self-contained, and the Security Test Plan would be unmanageable if testers were required to reference other documents during security testing.

5.3 Specific Tailoring Instructions

The following subsections discuss the specific tailoring instructions for each security document. This discussion includes the instructions to tailor the DID at each TCSEC class. Subsection 10.2 of each DID contains the general documentation requirements for all of the TCSEC classes of the document. Any TCSEC documentation requirements that are specific to certain classes are included in the DIDs in subsections 10.3 or higher. Samples CDRLs for each document at each class are included in Appendix A.

5.3.1 Security Features User's Guide (SFUG)

Referencing to other documents should not be allowed in the SFUG. This restriction can be indicated in the SOW or the CDRL for the SFUG. The SFUG is a user's guide that would be cumbersome to use if the user were required to reference other documentation, as described above.

The SFUG is required by the TCSEC at Class C2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class C2 and B1 product or equivalent system, subsections 10.3 and 10.4 should be deleted. For a TCSEC Class B2 product or equivalent system, subsection 10.4 should be deleted. Finally, for a TCSEC Class B3 and A1 product or equivalent system, subsection 10.3 should be deleted. Sample CDRLs for each of these TCSEC Classes are included in Appendix A.

5.3.2 Trusted Facility Manual (TFM)

The TFM is required by the TCSEC at Class C2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For TCSEC Class C2, subsections 10.4 through 10.7 should be deleted. For a TCSEC Class B1 product or equivalent system, subsections 10.5 through 10.7 should be deleted. For TCSEC Class B2, subsections 10.6 and 10.7 should be deleted. For a TCSEC Class B3 product or equivalent system, subsection 10.7 should be deleted. Finally, for TCSEC Class A1, all of the subsections of 10 should be addressed in the TFM. Sample CDRLs for each of these TCSEC Classes are included in Appendix A.

5.3.3 Philosophy of Protection Report

The Philosophy of Protection Report is a good overview security document to require as part of a proposal for a program. Since it describes the security philosophy for the program at a high level without implementation specifics, the report can assist the evaluators in determining the validity of the proposed solution. The requirement for the document should be included in the proposal preparation instructions so that this document is available during proposal evaluation. The document should also be included in the SOW for post-award refinements.

The Philosophy of Protection Report is required in the TCSEC for Class C2 and above classes. No tailoring is required; the document is the same for all TCSEC classes.

5.3.4 Informal Security Policy Model

The Informal Security Policy Model is required by the TCSEC at Class B1 if the Formal Security Policy Model does not exist. It is the responsibility of the procurement initiator to determine whether an informal or formal security policy model should be required. Generally, if formal proofs are envisioned, then the Formal Security Policy Model should be required. Otherwise, the Informal Security Policy Model is sufficient.

No tailoring is required for the Informal Security Policy Model since the document is only applicable at one TCSEC class. A sample CDRL is included in Appendix A.

5.3.5 Formal Security Policy Model

The SOW portion, which calls out the CDRL and corresponding DID for the Formal Security Policy Model, should indicate that an NCSC-endorsed formal specification and verification system should be used at TCSEC Class A1 [TCSEC, Section 4.1.3.2.2]. Refer to pg. 41, Volume 2, of this Procurement Guideline series for associated SOWs which support the use of the Formal Security Policy Model DID. This will ensure the foundation on which this assurance documentation is based. If the developer and the software support activity are not the same, then the government needs to acquire the rights to the formal tools used to develop the formal model. This can be requested through the SOW and a separate CDRL.

The Formal Security Policy Model may be offered as a substitute for the Informal Security Policy Model at the TCSEC Class B1. However, it is required by the TCSEC at Class B2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class B1 product or equivalent system, subsection 10.4 should be deleted. For TCSEC Classes B2, B3, and A1, subsection 10.3 should be deleted. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.6 Descriptive Top-Level Specification (DTLS)

During the documentation of the design of a trusted product at the TCSEC Class B2 and above, the designer and/or documenter should keep in mind that a covert channel analysis will be required. Often the design and document can be written in more than one way at each decision point. If the need for a covert channel analysis is kept in mind when these design and documentation decisions are being made, effort may be saved during the covert channel analysis.

The DTLS is design documentation, and is closely related to the software and hardware design documentation. The requirements for the DTLS document may be satisfied in one of three ways: (1) a separate, stand-alone document in addition to the standard design documentation; (2) a brief document that includes some overview security discussion, and then provides a list of pointers into the standard design documentation; (3) completely subsumed within the standard design documentation, in which case it is necessary to identify clearly which portions of the design documents are part of the security-relevant DTLS. The SOW or the CDRL in Block 16 should indicate which of these options should be used for the DTLS for a specific acquisition.

The DTLS is required by the TCSEC at Class B2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class B2 product or equivalent system, subsections 10.3 and 10.4 should be deleted. For TCSEC Class B3, subsection 10.4 should be deleted. Finally, for a TCSEC Class A1 product or equivalent system, all subsections of 10 should be addressed in the DTLS. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.7 Formal Top-Level Specification (FTLS)

During the documentation of the design of a trusted product in an FTLS, the designer and/or documenter should keep in mind that a covert channel analysis will be required. Often the design and document can be written in a couple of ways at each decision point. If the need for a covert channel analysis is kept in mind when these design and documentation decisions are being made, effort may be saved during the covert channel analysis.

The FTLS is required in the TCSEC for Class A1. No tailoring is required, since the document is only required for the one TCSEC class. A sample CDRL is included in Appendix A.

5.3.8 Design Specification

The Design Specification document contains the security design information requirements in the TCSEC that are not covered in any other security design document. At the lower levels, it is the only design document; therefore, it contains all of the TCSEC-required design information. At the higher levels, some of the design information exists in other documents, therefore, this design information is not contained in the Design Specification.

An example of this partitioning is the documentation of the TCB interfaces. At TCSEC Classes C2 and B1, the documentation of the TCB interfaces is contained in the Design Specification. However, at TCSEC Classes B2 and above, the DTLS is required. The DTLS contains the documentation of the TCB interfaces. Therefore, the Design Specification does not require this information above TCSEC Class B1 level.

The Design Specification is design documentation, and is closely related to the software and hardware design documentation. The requirements for the Design Specification document may be satisfied in one of three ways: (1) a separate, stand-alone document in addition to the standard design documentation; (2) a brief document that includes some overview security discussion, and then provides a list of pointers into the standard design documentation; (3) completely subsumed within the standard design documentation, in which case it is necessary to identify clearly which portions of the design documents are part of the security-relevant Design Specification. The SOW or the CDRL in Block 16 should indicate which of these options should be used for the Design Specification for a specific acquisition.

Subsection 10.2 of the Design Specification contains the general information required at all class levels of the document. For TCSEC Class C2, subsections 10.5 through 10.8 should be deleted. For a TCSEC Class B1 product or equivalent system, subsections 10.6 through 10.8 should be deleted. For TCSEC Class B2, subsections 10.3 through 10.5, 10.7, and 10.8 should be deleted. For a TCSEC Class B3 product or equivalent system, subsections 10.3 through 10.5 and 10.8 should be deleted. Finally, for TCSEC Class A1, subsections 10.3 through 10.5 should be deleted. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.9 Trusted Computing Base (TCB) Verification Report

The TCB Verification Report is required by the TCSEC at Class B3 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class B3 product or equivalent system, subsection 10.4 should be deleted. For a TCSEC Class A1, subsection 10.3 should be deleted. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.10 Covert Channel Analysis Report

The Covert Channel Analysis Report is required by the TCSEC at Class B2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class B2 product or equivalent system, subsections 10.4 and 10.5 should be deleted. For TCSEC Class B3, subsection 10.5 should be deleted. For a TCSEC Class A1 product or equivalent system, all of the subsections in 10 should be addressed in the report. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.11 Trusted Computing Base Configuration Management Plan

The hardware and firmware, which enforce security protection, are considered a part of the TCB at the lower TCSEC classes. However, the hardware and firmware of the TCB are not required to be placed under CM control until at TCSEC Class A1 level. This is the major difference between the B3 and A1 TCB CM Plan included with this guideline.

The TCB CM Plan can be tied to the overall development and CM methodology of a project. The requirements for the TCB CM Plan may be satisfied in one of three ways: (1) a separate, stand-alone document in addition to the program CM plan; (2) a brief document that includes some overview security discussion, and then provides a list of pointers into the program CM plan; (3) completely subsumed within the program CM plan, in which case it is necessary to identify clearly which portions of the CM plan are part of the security-relevant CM plan. The SOW or the CDRL in Block 16 should indicate which of these options should be used for the TCB CM Plan for a specific acquisition.

The TCB CM Plan is required by the TCSEC at Class B2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For a TCSEC Class B2 and B3 product or equivalent system, subsection 10.4 should be deleted. For TCSEC Class A1, subsection 10.3 should be deleted. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.12 Test Documentation

The test documentation DIDs included in this guideline are the Security Test Plan, Test Procedures, and Test Reports. The security test plan DID was created for this guideline. The test procedure and test reports DIDs are generic DIDs that can be used for Security Test Procedures and Test Reports. The following subsections provide the tailoring instructions for these DIDs.

5.3.12.1 Security Test Plan

Referencing to other documents should not be allowed for the Test Plan. This restriction can be indicated in the SOW or the CDRL for the Security Test Plan. It would be unmanageable if testers were required to reference multiple documents during testing, as described above.

Generally, Security Test Plans are produced to support certification and accreditation. This support should be taken into account when calling out the requirement for a Security Test Plan.

The Security Test Plan is required by the TCSEC at Class C2 and above. Subsection 10.2 contains the general information required at all class levels of the document. For TCSEC Class C2, subsections 10.4 through 10.9 should be deleted. For a TCSEC Class B1 product or equivalent system, subsections 10.3, and 10.6 through 10.9 should be deleted. For TCSEC Class B2, subsections 10.3, 10.4, 10.8, and 10.9 should be deleted. For a TCSEC Class B3 product or equivalent system, subsections 10.3, 10.4, 10.6, and 10.9 should be deleted. Finally, for TCSEC Class A1, subsections 10.3, 10.4, 10.6, and 10.7 should be deleted. Sample CDRLs for each of these TCSEC classes are included in Appendix A.

5.3.12.2 Test Procedures

The Test Procedures DID was not specifically developed for this guideline because there are no TCSEC requirements defining the content of Security Test Procedures. The requirement in the TCSEC is to provide procedures for security testing. The DID included in Appendix B for the Test Procedures is a generic DID that covers all types of information that should be included in procedures for security testing. As such, the Test Procedures DID does not need to be tailored specifically for any of the TCSEC classes. The same CDRL and DID, in Appendix A and B respectively, can be used for any TCSEC class test procedure.

However, this DID is all inclusive in nature. For that reason, there may be non-security-related requirements that are not appropriate for a specific acquisition. Therefore, the Test Procedures DID should be examined and tailored accordingly. This tailoring deletes inappropriate requirements, simplifying the resulting document.

One provision that should be included in any Test Procedures for an environment containing sensitive information is the handling of sensitive results (e.g., classified printouts) produced during testing. The SOW for the Test Procedures should include this provision.

5.3.12.3 Test/Investigation Reports

The Test/Investigation Reports DID included in this guideline provide "the results of development, qualification and other tests required by applicable specifications and program test plans, and to show degree of meeting specified performance objectives." From the requirements within the DID itself, the "specified performance objectives" are not the type of performance objectives in the form of timing or throughput objectives. The objectives on which this DID requires reporting are functional performance of specified requirements.

The Test/Investigation Reports DID included in this guideline was not specifically developed for this guideline because there are no TCSEC requirements reporting security testing results. The requirement in the TCSEC is to report the results of security testing. The DID included in Appendix B for Test/Investigation Reports is a generic DID that covers all types of information which should be included to report on security testing. As such, the Test/Investigation Reports DID does not need to be tailored for any of the TCSEC classes. The same CDRL and DID in Appendix A and B respectively can be used for any TCSEC class of Test/Investigation Reports.

However, this DID is all-inclusive in nature. For that reason, there may be non-security-related requirements that are not appropriate for a specific acquisition. Therefore, the Test/Investigation Reports DID should be examined and tailored accordingly. This tailoring deletes inappropriate requirements, simplifying the resulting document.

One provision that should be included in any Test/Investigation Report for an environment containing sensitive information is the handling of sensitive results (e.g., classified printouts) produced during testing. The SOW for the Test Procedures should include this provision.

5.3.12.4 Summary of Specific Tailoring Instructions

Table 2, summarizes the contents of the previous guideline subsections. As has been noted, subsection 10.2 of each DID is applicable at each class level. For each document, subsections 10.3 through 10.9 are either not applicable or should be deleted for certain classes, as indicated in the table. (See table footnote.)

Table 2: Summary of DID Subsections to be Deleted for Each Security Document

DOCUMENT AT TCSEC CLASS	DID SUBSECTIONS TO BE DELETED							
	10.2	10.3	10.4	10.5	10.6	10.7	10.8	10.9
SFUG at TCSEC class C2		X	X	-	-	-	-	-
SFUG at TCSEC Class B1		X	X	-	-	-	-	-
SFUG at TCSEC Class B2			X	-	-	-	-	-
SFUG at TCSEC Class B3		X		-	-	-	-	-
SFUG at TCSEC Class A1		X		-	-	-		-
TFM at TCSEC Clas C2			X	X	X	X	-	-
TFM at TCSEC Class B1				X	X	X	-	-
TFM at TCSEC Class B2					X	X	-	-
TFM at TCSEC Class B3						X	-	-
TFM at TCSEC Class A1							-	-
Philosophy of Protection at All Classes		-	-	-	-	-	-	-
Informal Security Policy Model Class B1			-	-	-	-	-	-
Formal Security Policy Model at B1			X		-	-	-	-
Formal Security Policy Model at B2		X			-	-	-	-
Formal Security Policy Model at B3		X			-	-	-	-
Formal Security Policy Model at A1		X			-	-	-	-
DTLS at TCSEC Class B2		X	X	-	-	-	-	-
DTLS at TCSEC Class B3			X	-	-	-	-	-
DTLS at TCSEC Class A1				-	-	-	-	-
FTLS at TCSEC Class A1		-	-	-	-	-	-	-
Design Specification at C2				X	X	X	X	-
Design Specification at B1					X	X	X	-
Design Specification at B2		X	X	X		X	X	-
Design Specification at B3		X	X	X			X	-
Design Specification at A1		X	X	X				-
TCB Verification Report at B3			X	-	-	-	-	-

TCB Verification Report at A1		X		–	–	–	–	–
Covert Channel Analysis Report at B2			X	X	–	–	–	–
Covert Channel Analysis Report at B3				X	–	–	–	–
Covert Channel Analysis Report at A1					–	–	–	–
TCB CM Plan at TCSEC Class B2			X	–	–	–	–	–
TCB CM Plan at TCSEC Class B3			X	–	–	–	–	–
TCB CM Plan at TCSEC Class A1		X		–	–	–	–	–
Security Test Plan at C2			X	X	X	X	X	X
Security Test Plan at B1		X			X	X	X	X
Security Test Plan at B2		X	X				X	X
Security Test Plan at B3		X	X		X			X
Security Test Plan at A1		X	X		X	X		
Test Procedure at All Classes	–	–	–	–	–	–	–	–
Test/Investigation Reports at All Classes	–	–	–	–	–	–	–	–

X = Delete Subsection

– = Not Applicable

APPENDIX A - SAMPLE CDRLs FOR EACH CLASS

These CDRLs are examples the procurement initiator can use in an RFP. They can be drawn directly into the RFP for each TCSEC class. Section 3 provides a description and guidance on completing all of the blocks on the CDRL form. The blocks containing italicized information must be replaced. Block 4 of the sample uses the corresponding Data Item Description number. Block 5 uses the corresponding Statement(s) of Work (SOW) number that is found on page 41, Volume 2, of the Procurement Guideline series. The SOW number may be different according to your specific RFP numbering scheme. Block 16 of the sample CDRLs is especially noteworthy. This block can be used as is in the sample.

(To view CDRLs, reference the hardcopy.)

APPENDIX B – SECURITY DIDs

Fourteen security DIDs are provided in this appendix containing all of the documentation required by the TCSEC. (Reference the hardcopy to view the DIDs). These DIDs can be included in an RFP, as is, with a corresponding CDRL to tailor the DID for the specific RFP. Section 5 of this guideline provides a description of the DID form itself and tailoring instructions for each of these DIDs. The sample CDRLs in Appendix A illustrate these tailoring instructions.

The following is a list of the 14 security DIDs that are contained in the appendix: Security Features 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, TCB Verification Report, Covert Channel Analysis Report, TCB Configuration Management Plan, Security Test Plan, Test Procedures, and Test/Investigation Reports.

APPENDIX C - REFERENCES

Advisory Memorandum on Office Automation Security Guideline, NTISSAM COMPUSEC, 16 January, 1987. (Supersedes NCSC-WA-002-85)

Commercial Off-The-Shelf (COTS) Manuals, DI-TMSS-80527, 1 February, 1988.

Department of Defense Directive, Defense Acquisition, DoDD 5000.1, 23 February, 1991.

Department of Defense, Computer Security Requirements, Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-003-85, 25 June, 1985.

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

Department of Defense Standard, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 26 December, 1985.

Integrity in Automated Information Systems, C Technical Report 79-91, September, 1991.

List, Contract Data Requirements (DD Form 1423), DI-A-23434C, 28 July, 1977.

Military Handbook, Acquisition Streamlining, MIL-HDBK-248B, 9 February, 1989.

Military Standard, Defense System Software Development, MIL-STD-2167A, 29 February, 1988.

National Computer Security Center, A Guide to Understanding Audit in Trusted Systems, NCSC-TG-001, Version-2, 1 June, 1988.

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

National Computer Security Center, A Guide to Understanding Discretionary Access Control (DAC) in Trusted Systems, NCSC-TG-003, Version-1 30 September, 1987.

National Computer Security Center, Glossary of Computer Security Terms, NCSC-TG-004, 21 October, 1988. (NCSC-WA-001-85 is obsolete)

National Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005, Version-1, 31 July, 1987.

National Computer Security Center, A Guide to Understanding Configuration Management in Trusted Systems, NCSC-TG-006, Version-1, 28 March, 1988.

National Computer Security Center,A Guide to Understanding Design Documentation in Trusted Systems, NCSC-TG-007, Version-1, 2 October, 1988.

National Computer Security Center, A Guide to Understanding Trusted Distribution in Trusted Systems, NCSC-TG-008, Version-1, 15 December, 1988.

National Computer Security Center, Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-009, Version-1, 16 September, 1988.

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

National Computer Security Center, Trusted Network Interpretation Environments Guideline, NCSC-TG-011, Version-1, 1 August,1990.

National Computer Security Center, Guidelines for Formal Verification Systems, NCSC-TG-014, Version-1, 1 April, 1989.

National Computer Security Center, A Guide to Understanding Trusted Facility Management, NCSC-TG-015, Version-1, 18 October, 1989.

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

National Computer Security Center, A Guide to Understanding Identification and Authentication in Trusted Systems, NCSC-TG-017, Version-1, September, 1991.

National Computer Security Center, A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018, Version-1, July, 1992.

National Computer Security Center, Trusted Product Evaluation Questionnaire, NCSC-TG-019, Version-2, 2 May, 1992.

National Computer Security Center, Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-021, Version-1, April, 1991.

National Computer Security Center, A Guide for Understanding Trusted Recovery in Trusted Systems, NCSC-TG-022, Version-1, 30 December, 1991

National Computer Security Center, A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements, NCSC-TG-024, Version-1, Volume 1/4, December, 1992.

National Computer Security Center, A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators, NCSC-TG-024, Version-1, Volume 2/4, 30 June, 1993.

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

National Computer Security Center, A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025, Version-2, September, 1991. (Supersedes CSC-STD-005-85)

National Computer Security Center,A Guide to Writing the Security Features User's Guide for Trusted Systems, NCSC-TG-026, Version-1, September, 1991.

National Computer Security Center, A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems, NCSC-TG-027, Version-1, May, 1992.

National Computer Security Center, Assessing Controlled Access Protection, NCSC-TG-028, Version-1, 25 May, 1992.

Preparation of Data Item Descriptions, DoD-STD-963A, 15 August, 1986.

Supplemental Data for Commercial Off-the-Shelf (COTS) Manuals, DI-TMSS-80528, 1 February, 1988.

The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion, C Technical Report 32-92, June, 1992.

A single complimentary copy of NSA guidelines (CSC-STD- and NCSC-TG-) may be obtained from:

Director
National Security Agency
ATTN: X81, INFOSEC Awareness Division
Fort George G. Meade, MD 20755-6000
(410) 766-8729

Multiple copies of documents may be obtained by contacting:

Superintendent of Documents
U.S. Government Printing Office
Washington, DC 20402
(Mastercard or VISA are accepted) (202) 783-3238

APPENDIX D - GLOSSARY

Accreditation - Formal declaration by a designated approving authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards.

Authenticate - To establish the validity of a claimed identity.

Automated Information System (AIS) - An assembly of computer hardware, firmware, and software configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, storing, and retrieving data with a minimum of human intervention.

Bandwidth - A characteristic of a communication channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in bits per second.

Certification - The technical evaluation of a system's features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified requirements.

Channel - An information transfer path within a system. It may also refer to the mechanism by which the path is effected.

Computer-Based Security Requirements - The types and levels of protection necessary for equipment, data, information, and applications to meet security policy.

Covert Channel - A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel, Covert Timing Channel.

Covert Storage Channel - A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel - A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

Data Integrity - The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Data Requirement - In reference to DIDs, the essential elements needed for the document defined by the DID.

Descriptive Top-Level Specification (DTLS) - A top-level specification that is written in a natural language (e.g., English), an informal program design notation, or a combination of the two.

Discretionary Access Control - A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission, perhaps indirectly, on to any other subject, unless restrained by mandatory access control.

Exploitable Channel - Any channel that is usable or detectable by subjects external to the Trusted Computing Base.

Flaw - An error of commission, omission, or oversight in a system that allows protection mechanisms to be bypassed.

Formal Proof - A complete and convincing mathematical argument presenting the full logical justification for each proof step for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications.

Formal Security Policy Model - A mathematically precise statement of a security policy. To be acceptable as a basis for a TCB, the model must be supported by a formal proof. Some formal modeling techniques include: state transition models, temporal logic models, denotational semantics models, algebraic specification models.

Formal Top-Level Specification (FTLS) - A Top-Level Specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.

Formal Verification - The process of using formal proofs to demonstrate the consistency between a formal specification of a system and a formal security policy model (design verification) or between the formal specification and its program implementation (implementation verification).

Functional Requirements - The types of operations necessary for equipment, information, applications, and facilities to meet operational needs.

Functional Testing - The portion of security testing in which the advertised features of a system are tested for correct operation.

Least Privilege - This principle requires that each subject in a system be granted the most restrictive set of privileges or lowest clearance needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Mandatory Access Control - A means of restricting access to objects based on the sensitivity, as represented by a label, of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains.

Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

Operational Needs - The capabilities required to perform a specific mission or task.

Output - Information that has been exported by a TCB.

Password - A private character string that is used to authenticate an identity.

Penetration Testing - The portion of security testing in which the penetrator attempts to circumvent the security features of a system. The penetrator may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrator works under no constraints other than those that would be applied to ordinary users.

Process - A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.

Protection-Critical Portions of the TCB - Those portions of the TCB whose normal function is to deal with the control of access between subjects and objects.

Protection Philosophy - An informal description of the overall design of a system that delineates each of the protection mechanisms employed. A combination (appropriate to the evaluation class) of formal and informal techniques is used to show that the mechanisms are adequate to enforce the security policy.

Read - A fundamental operation that results only in the flow of information from an object to a subject.

Reference Monitor Concept - An access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.

Resource - Anything used or consumed while performing a function. The categories of resources are: time, information, objects (information containers), or processors (the ability to use information). Specific examples are: CPU time, terminal connect time, amount of directly-addressable memory, disk space, number of I/O requests per minute, etc.

Security Features - The security relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

Security Kernel - The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct.

Security Level - The combination of a hierarchical classification and a set of non-hierarchical categories that represents the sensitivity of information.

Security Mechanisms - The security relevant functions and characteristics of system software.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Policy Model - An informal presentation of a formal security policy model.

Security Relevant Event - Any event that attempts to change the security state of the system, (e.g., change discretionary access controls, change the security level of the subject, change user password). Also, any event that attempts to violate the security policy of the system, (e.g., too many attempts to login, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file).

Security Requirements - The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Security Safeguards - The protective measures and controls that are prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Security Testing - A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also: Functional Testing, Penetration Testing, Verification.

Sensitive Information - Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

Sensitivity Label - A piece of information that represents the security level of an object and that describes the sensitivity (e.g., classification) of the data in the object. Sensitivity labels are used by the TCB as the basis for mandatory access control decisions.

Simple Security Condition - A Bell-LaPadula security model rule allowing a subject read access to an object only if the security level of the subject dominates the security level of the object.

*-Property (Star Property) - A Bell-LaPadula security model rule allowing a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property.

Storage Object - An object that supports both read and write accesses.

Subject - An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair.

Subject Security Level - A subject's security level is equal to the security level of the objects to which it has both read and write access. A subject's security level must always be dominated by the clearance of the user the subject is associated with.

TEMPEST - The study and control of spurious electronic signals emitted from AIS equipment.

Top-Level Specification (TLS) - A non-procedural description of system behavior at the most abstract level. Typically a functional specification that omits all implementation details.

Trap Door - A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented. It is activated in some non-apparent manner (e.g., special "random" key sequence at a terminal).

Trojan Horse - A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. For example, making a "blind copy" of a sensitive file for the creator of the Trojan Horse.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system -- including hardware, firmware, and software -- the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Path - A mechanism by which a person at a terminal can communicate directly with the Trusted Computing Base. This mechanism can only be activated by the person or the Trusted Computing Base and cannot be imitated by untrusted software.

Trusted Software - The software portion of a Trusted Computing Base.

User - Any person who interacts directly with a computer system.

Verification - The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, TLS with source code, or source code with object code). This process may or may not be automated.

Write - A fundamental operation that results only in the flow of information from a subject to an object.

Write Access - Permission to write an object.

APPENDIX E - ACRONYMS

AIS - Automated Information System

AMSC - Acquisition Management Systems Control

AMSDL - Acquisition Management Systems and Data Requirements Control List

APP - Approved

ASREQ - As Required

BAFO - Best and Final Offer

CDRL - Contract Data Requirements List

CCA - Covert Channel Analysis

CDR - Critical Design Review

CM - Configuration Management

COTS - Commercial-Off-The-Shelf

CPU - Central Processing Unit

DAC - Discretionary Access Control

DID - Data Item Description

DoD - Department of Defense

DoDD - DoD Directive

DoD-STD - DoD STandarD

DTIC - Defense Technical Information Center

DTLS - Descriptive Top-Level Specification

EPL - Evaluation Products List

FTLS - Formal Top-Level Specification

GIDEP - Government-Industry Data Exchange Program

I&A - Identification and Authentication

IAC - Integrating Associated Contractor

MAC - Mandatory Access Control

MIL-HDBK - MILitary HanDBooK

MIL-STD - MILitary STandarD

NCSC - National Computer Security Center

OPR - Office of Primary Responsibility

OTIME - One TIME

PDR - Preliminary Design Review

RFP - Request for Proposal

ROM - Read-Only Memory

SFUG - Security Features User's Guide

SDR - System Design Review

SOW - Statement of Work

SRR - System Requirement Review

TCB - Trusted Computing Base

TCSEC - Trusted Computer System Evaluation Criteria

TFM - Trusted Facility Manual

TLS - Top Level Specification

TRR - Test Readiness Review