NCSC-TG-024
VOLUME 3/4
VERSION 1

NATIONAL COMPUTER SECURITY CENTER

A GUIDE TO PROCUREMENT OF TRUSTED SYSTEMS:

Computer Security Contract Data Requirements List and Data Item Description Tutorial

20010802 081

28 FEBRUARY 1994

Approved for Public Release:
Distribution Unlimited

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 De Vilbiss 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.

TABLE OF CONTENTS

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).

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 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 byproduct 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.

2.0 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 design and

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 tradeoff 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.

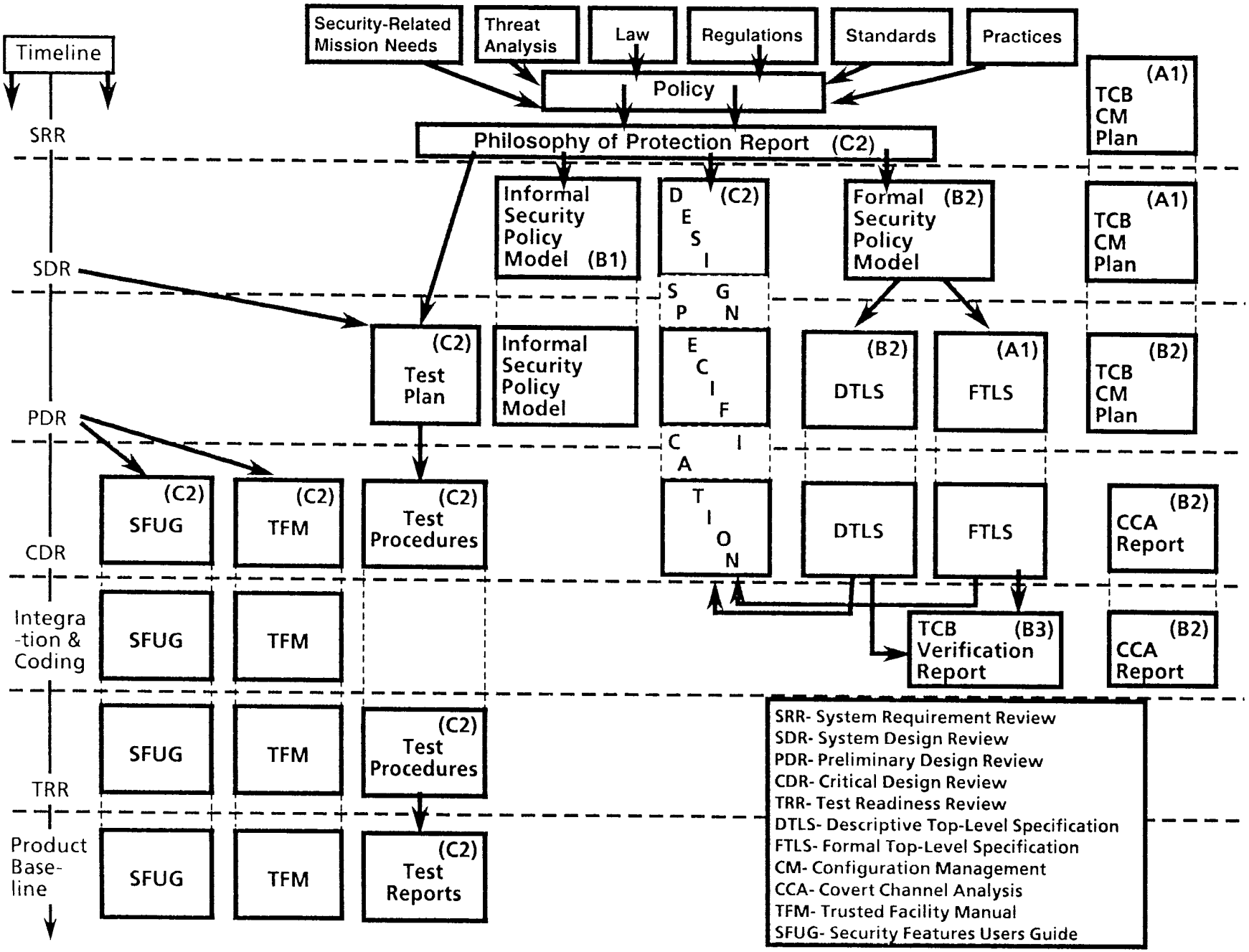

Figure 1. Security Documentation Correspondence

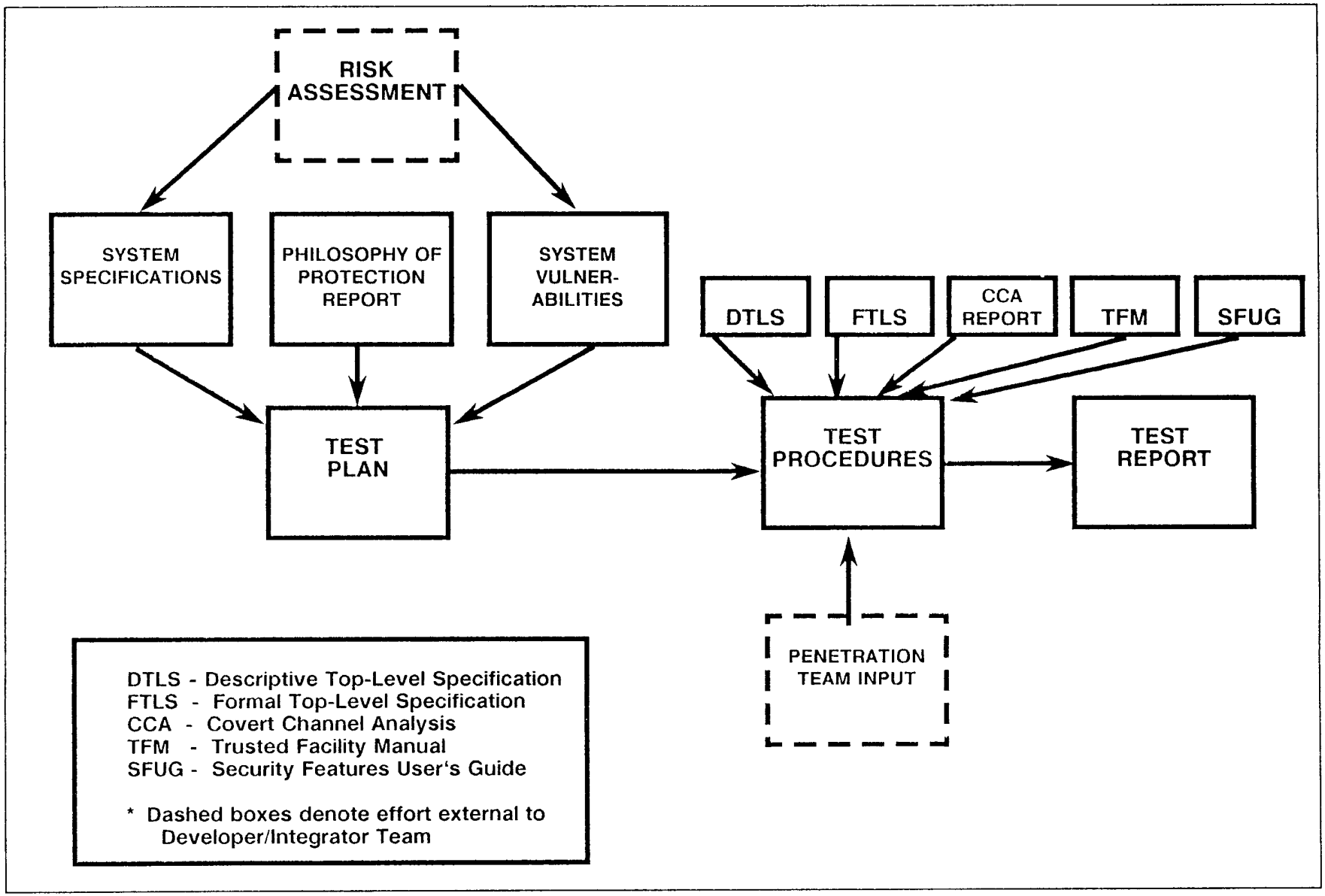

Figure 2. Test Documentation Correspondence

THIS PAGE INTENTIONALLY LEFT BLANK

3.0 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.

ATCH NR	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM
TO CONTRACTOR/P.P.		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST SUBM.	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1.	2. 3.	6.	10.	12.	14.
4.	5.	7. / 8. / 9.	11.	13.	
16. REMARKS					15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

DD Form 1423-1, SEP 86

Page_____of_____Pages

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

Contract Value

Figure 3. Contract Data Requirements List Form (DD Form 1423-1)

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).

THIS PAGE INTENTIONALLY LEFT BLANK

4.0 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.

5.0 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. 4, 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.

5.3.13 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 Class 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		-	-	-	-	-	-	-

X = Delete Subsection
- = Not Applicable

Table 2. Summary of DID Subsections to be Deleted for Each Security Document - Continued

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
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.

THIS PAGE INTENTIONALLY LEFT BLANK

EXAMPLE CDRL FOR SECURITY FEATURES USER'S GUIDE AT TCSEC CLASS C2 TO B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY FEATURES USER'S GUIDE. 3. TCSEC CLASS C2 TO B1	6.			10. OTIME	12. See BLK 16	14.
4. DI-MCCR-81349	5. SOW PARA C.3.7	7.	8.	9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

THIRD SUBMISSION - TRR MINUS 30 DAYS

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3 THROUGH 10.4

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY FEATURES USER'S GUIDE AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY FEATURES USER'S GUIDE. 3. TCSEC CLASS B2	6.	10. OTIME	12. See BLK 16	14.
4. DI-MCCR-81349	5. SOW PARA C.3.7	7. / 8. / 9.	11.	13. See BLK 16	
					15. TOTAL

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY FEATURES USER'S GUIDE AT TCSEC CLASS B3 TO A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)	
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID		
1. *A00X*	2. SECURITY FEATURES USER'S GUIDE. 3. TCSEC CLASS B3 TO A1	6.			10. OTIME	12. See BLK 16	14.	
4. DI-MCCR-81349	5. SOW PARA C.3.7	7.	8.	9.	11.	13. See BLK 16		
								15. TOTAL

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

THIRD SUBMISSION - TRR MINUS 30 DAYS

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TRUSTED FACILITY MANUAL AT TCSEC CLASS C2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. TRUSTED FACILITY MANUAL 3. TCSEC CLASS C2	6.	10. OTIME	12. See BLK 16	14.
4. DI-TMSS-81352	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.8

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4 THROUGH 10.7

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. / 20. / 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. / 20. / 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TRUSTED FACILITY MANUAL AT TCSEC CLASS B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. TRUSTED FACILITY MANUAL 3. TCSEC CLASS B1	6.	10. OTIME	12. See BLK 16	14.
4. DI-TMSS - 81352	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.8

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.5 THROUGH 10.7

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. / 20. / 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. / 20. / 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TRUSTED FACILITY MANUAL AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. TRUSTED FACILITY MANUAL 3. TCSEC CLASS B2	6.	10. OTIME	12. See BLK 16	14.
4. DI-TMSS-81352	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.8

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.6 THROUGH 10.7

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TRUSTED FACILITY MANUAL AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)	
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID		
1. *A00X*	2. TRUSTED FACILITY MANUAL 3. TCSEC CLASS B3	6.	10. OTIME	12. See BLK 16	14.	
4. DI-TMSS-81352	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16		15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.8

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.7

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TRUSTED FACILITY MANUAL AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM1/EVENT ID	
1. *A00X*	2. TRUSTED FACILITY MANUAL 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14.
4. DI-TMSS-81352	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.8

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

THIRD SUBMISSION - TRR MINUS 30 DAYS

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR PHILOSOPHY OF PROTECTION AT TCSEC CLASS C2 TO A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)				SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*				
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY				CONTRACTOR				
1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)			
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID				
1. *A00X*	2. PHILOSOPHY OF PROTECTION REPORT 3. TCSEC CLASS C2 TO A1	6.			10. OTIME	12. See BLK 16	14.			
4. DI-MISC-81348	5. SOW PARA C.3.10	7.	8.	9.	11.	13. See BLK 16				
16. REMARKS BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY FINAL 60 DAYS AFTER GOVERNMENT COMMENTS							15. TOTAL			
PREPARED BY	DATE	APPROVED BY	DATE							

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR INFORMAL SECURITY POLICY MODEL AT TCSEC CLASS B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. INFORMAL SECURITY POLICY MODEL 3. TCSEC CLASS B1	6.	10. OTIME	12. See BLK 16	14.
4. DI-MISC-81341	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR FORMAL SECURITY POLICY MODEL AT TCSEC CLASS B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. FORMAL SECURITY POLICY MODEL 3. TCSEC CLASS B1	6.	10. OTIME	12. See BLK 16	14.
4. DI-MISC-81346	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR FORMAL SECURITY POLICY MODEL AT TCSEC CLASS B2 TO A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)	
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID		
1. *A00X*	2. FORMAL SECURITY POLICY MODEL 3. TCSEC B2 TO A1	6.	10. OTIME	12. See BLK 16	14.	
4. DI-MISC-81346	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16		
16. REMARKS BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10 BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY FINAL 60 DAYS AFTER GOVERNMENT COMMENTS DELETE 10.4					15. TOTAL	

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESCRIPTIVE TOP-LEVEL SPECIFICATION AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. DESCRIPTIVE TOP-LEVEL SPECIFICATION 3. TCSEC CLASS B2	6.	10. OTIME	12. See BLK 16	14.
4. DI-MISC-81342	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3 THROUGH 10.4

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. / 20. / 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. / 20. / 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESCRIPTIVE TOP-LEVEL SPECIFICATION AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. DESCRIPTIVE TOP-LEVEL SPECIFICATION 3. TCSEC CLASS B3	6.	10. OTIME	12. See BLK 16	14.

4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID
4. DI-MISC-81342	5. See BLK 16	7.	8.	9.	11.	13. See BLK 16

16. REMARKS

BLOCK 5: C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESCRIPTIVE TOP-LEVEL SPECIFICATION AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. DESCRIPTIVE TOP-LEVEL SPECIFICATION 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14.

4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID
4. DI-MISC-81342	5. See BLK 16	7.	8.	9.	11.	13. See BLK 16

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. 20. 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. 20. 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR FORMAL TOP-LEVEL SPECIFICATION AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. FORMAL TOP-LEVEL SPECIFICATION 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14. / 15. TOTAL
4. DI-MISC-81347	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188	
17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. / 20. / 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. / 20. / 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESIGN SPECIFICATION AT TCSEC CLASS C2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. DESIGN SPECIFICATION 3. TCSEC CLASS C2	6.	10. OTIME	12. See BLK 16	14.
4. DI-MCCR-81344	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.5 THROUGH 10.8

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESIGN SPECIFICATION AT TCSEC CLASS B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. DESIGN SPECIFICATION 3. TCSEC CLASS B1	6.	10. OTIME	12. See BLK 16	14.
4. DI-MCCR-81344	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.6 THROUGH 10.8

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESIGN SPECIFICATION AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	6. TECHNICAL OFFICE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	10. FREQUENCY	11. AS OF DATE	12. DATE FOR 1ST Submission	13 DATE OF SUBSEQUENT SUBM/EVENT ID	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2...DESIGN SPECIFICATION 3. TCSEC CLASS B2			6.				10. OTIME		12. See BLK 16		14.
		4. DI-MCCR-81344	5. See BLK 16	7.	8.	9.		11.		13. See BLK 16		

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3 THROUGH 10.5

DELETE 10.7 THROUGH 10.8

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESIGN SPECIFICATION AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. DESIGN SPECIFICATION 3. TCSEC CLASS B3	6.	10. OTIME	12. See BLK 16	14.
4. DI-MCCR-81344	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3 THROUGH 10.5

DELETE 10.8

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER	23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER	24. ESTIMATED NUMBER OF PAGES
19. / 20. / 21.	25. PRICE GROUP
22. RESERVED FOR ADP	26. ESTIMATED TOTAL PRICE
17.	23.
18.	24.
19. / 20. / 21.	25.
22.	26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR DESIGN SPECIFICATION AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. DESIGN SPECIFICATION 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14. / 15. TOTAL
4. DI-MCCR-81344	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.4, C.3.10

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3 THROUGH 10.5

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TCB VERIFICATION REPORT AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	6. TECHNICAL OFFICE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	10. FREQUENCY	11. AS OF DATE	12. DATE FOR 1ST Submission	13 DATE OF SUBSEQUENT SUBM/EVENT ID	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. TCB VERIFICATION REPORT 3. TCSEC CLASS B3			6.				10. OTIME		12. See BLK 16		14.
		4. DI-MISC-81350	5. SOW PARA C.3.4		7.	8.	9.		11.		13. See BLK 16	

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TCB VERIFICATION REPORT AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. TCB VERIFICATION REPORT 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14.

4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. DI-MISC-81350	5. SOW PARA C.3.4	7.	8.	9.	11.	13. See BLK 16	14.

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR COVERT CHANNEL ANALYSIS REPORT AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. COVERT CHANNEL ANALYSIS REPORT 3. TCSEC CLASS B2	6.	10. OTIME	12. See BLK 16	14.

4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID
4. DI-MISC-81345	5. SOW PARA C.3.1	7.	8.	9.	11.	13. See BLK 16

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4 THROUGH 10.5

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR COVERT CHANNEL ANALYSIS REPORT AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)				SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*					
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY				CONTRACTOR					
1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE		6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)			
4. AUTHORITY (Data Item Number)		5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID				
1. *A00X*	2. COVERT CHANNEL ANALYSIS REPORT 3. TCSEC CLASS B3		6.			10. OTIME	12. See BLK 16	14.			
4. DI-MISC-81345		5. SOW PARA C.3.1	7.	8.	9.	11.	13. See BLK 16				
									15. TOTAL		

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.5

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

Contract value

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR COVERT CHANNEL ANALYSIS REPORT AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. COVERT CHANNEL ANALYSIS REPORT 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14.
4. DI-MISC-81345	5. SOW PARA C.3.1	7. / 8. / 9.	11.	13. See BLK 16	
16. REMARKS BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY FINAL 60 DAYS AFTER GOVERNMENT COMMENTS					15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TCB CONFIGURATION MANAGEMENT PLAN AT TCSEC CLASS B2 AND B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	6. TECHNICAL OFFICE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	10. FREQUENCY	11. AS OF DATE	12. DATE FOR 1ST Submission	13 DATE OF SUBSEQUENT SUBM/EVENT ID	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
1. *A00X*	2. CONFIGURATION MANAGEMENT PLAN 3. TCSEC CLASS B2 TO B3			6.				10. OTIME		12. See BLK 16		14.
		4. DI-CMAN-81343	5. See BLK 16	7.	8.	9.		11.		13. See BLK 16		

16. REMARKS

BLOCK 5: SOW PARA C.3.5, C.3.6

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR TCB CONFIGURATION MANAGEMENT PLAN AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. CONFIGURATION MANAGEMENT PLAN 3. TCSEC CLASS A1	6.	10. OTIME	12. See BLK 16	14.
4. DI-CMAN-81343	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.5, C.3.6

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
THIRD SUBMISSION - TRR MINUS 30 DAYS
GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST PLAN AT TCSEC CLASS C2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)	
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID		
1. *A00X*	2. SECURITY TEST PLAN 3. TCSEC CLASS C2	6.			10. OTIME	12. See BLK 16	14.	
4. DI-NDTI-81351	5. See BLK 16	7.	8.	9.	11.	13. See BLK 16		
								15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.9

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.4 THROUGH 10.9

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST PLAN AT TCSEC CLASS B1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY TEST PLAN 3. TCSEC CLASS B1	6.	10. OTIME	12. See BLK 16	14.
4. DI-NDTI-81351	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.9

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3

DELETE 10.6 THROUGH 10.9

15. TOTAL

PREPARED BY	DATE	APPROVED BY	DATE

DD Form 1423-1, SEP 86

Page_____of_____Pages

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

EXAMPLE CDRL FOR SECURITY TEST PLAN AT TCSEC CLASS B2

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY TEST PLAN 3. TCSEC CLASS B2	6.	10. OTIME	12. See BLK 16	14.
4. DI-NDTI-81351	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.9

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3,10.4, 10.8, AND 10.9

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST PLAN AT TCSEC CLASS B3

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY TEST PLAN. 3. TCSEC CLASS B3	6.	10. OTIME	12. See BLK 16	14.
4. DI-NDTI-81351	5. See BLK 16	7. / 8. / 9.	11.	13. See BLK 16	15. TOTAL

16. REMARKS

BLOCK 5: SOW PARA C.3.2, C.3.9

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

DELETE 10.3, 10.4, 10.6, AND 10.9

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST PLAN AT TCSEC CLASS A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)					SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*						
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY					CONTRACTOR						
1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE		6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)					
4. AUTHORITY (Data Item Number)		5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID						
1. *A00X*	2. SECURITY TEST PLAN 3. TCSEC CLASS A1		6.			10. OTIME	12. See BLK 16	14.					
4. DI-NDTI-81351		5. See BLK 16	7.	8.	9.	11.	13. See BLK 16						
16. REMARKS BLOCK 5: SOW PARA C.3.2, C.3.9 BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY FINAL 60 DAYS AFTER GOVERNMENT COMMENTS DELETE 10.3, 10.4, 10.6, AND 10.7												15. TOTAL	
PREPARED BY		DATE	APPROVED BY			DATE							

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST PROCEDURES AT TCSEC CLASS C2 TO A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE	10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ / 8. APP CODE (A) / 9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID	
1. *A00X*	2. SECURITY TEST PROCEDURES 3. TCSEC CLASS C2 TO A1	6.	10. OTIME	12. See BLK 16	14.
4. DI-NDTI-80603	5. SOW PARA C.3.9	7. / 8. / 9.	11.	13. See BLK 16	
					15. TOTAL

16. REMARKS

BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS

BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

SECOND SUBMISSION - COMPLETION OF INTEGRATION/CODING

GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY

FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED
OMB NO. 0704-0188

17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

EXAMPLE CDRL FOR SECURITY TEST/INSPECTION REPORTS AT TCSEC CLASS C2 TO A1

ATCH NR *00-X*	TO EXHIBIT	CONTRACT DATA REQUIREMENTS LIST (1 Data Item)	SYSTEM/ITEM *(EXAMPLE XX SYSTEM)*
TO CONTRACTOR/P.P. *xxxx00-99-c-0000*		CATEGORY	CONTRACTOR

1. SEQUENCE NUMBER	2. TITLE OR DESCRIPTION OF DATA 3. SUBTITLE	6. TECHNICAL OFFICE			10. FREQUENCY	12. DATE FOR 1ST Submission	14. DISTRIBUTION AND ADDRESSEES (Addressee Regular Copies/Repro. Copies)	
4. AUTHORITY (Data Item Number)	5. CONTRACT REFERENCE	7. DD 250 REQ	8. APP CODE (A)	9. INPUT TO IAC (X)	11. AS OF DATE	13 DATE OF SUBSEQUENT SUBM/EVENT ID		
1. *A00X*	2. TEST/INSPECTION REPORTS 3. TCSEC CLASS C2 TO A1	6.			10. OTIME	12. See BLK 16	14.	
4. DI-NDTI-80809A	5. See BLK 16	7.	8.	9.	11.	13. See BLK 16		
								15. TOTAL

16. REMARKS
BLOCK 5: SOW PARA C.3.3, C.3.9
BLOCK 12: FIRST SUBMISSION OF DRAFT - CDR MINUS 30 DAYS
BLOCK 13: GOVERNMENT COMMENTS 45 DAYS AFTER DRAFT DELIVERY
FINAL 60 DAYS AFTER GOVERNMENT COMMENTS

PREPARED BY	DATE	APPROVED BY	DATE

FORM APPROVED OMB NO. 0704-0188			
17. EVENT/CEI NUMBER			23. CONTRACTOR FILE/ DOCUMENT NUMBER
18. OMB APPROVAL/ FORM NUMBER			24. ESTIMATED NUMBER OF PAGES
19.	20.	21.	25. PRICE GROUP
22. RESERVED FOR ADP			26. ESTIMATED TOTAL PRICE
17.			23.
18.			24.
19.	20.	21.	25.
22.			26.

CONTRACT VALUE

DD Form 1423-1, SEP 86

Page_____of_____Pages

APPENDIX B - SECURITY DIDs

Fourteen security DIDs are provided in this appendix containing all of the documentation required by the TCSEC. 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.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
SECURITY FEATURES USER'S GUIDE	DI-MCCR-81349

3. DESCRIPTION/PURPOSE

3.1 The Security Features User's Guide informs users on how to make effective use of security features. It provides the necessary information to understand and effectively use the security protection mechanism(s) that secure processed or stored information.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.2.4.1 and 3.2.2.1.1 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that requires user documentation for the security features as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria, Classes C1 (Discretionary Security Protection), and above, products or their equivalent systems.

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6939

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the Security Features User's Guide as follows:

a Cover Sheet: Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous version(s).

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly summarizes the Security Features User's Guide.

g. Introduction.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-MCCR-81349

Block 7, APPLICATION/INTERRELATIONSHIP (Continued)

7.3 The information required by 10.3 and 10.4 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.4.1 and 10.4.2 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

h. Body of the Guide.
i. Attachments.
j. Appendices.
k. Bibliography. List references and all applicable documents.
l. Subjective index. An exhaustive index of the key word or theme in each paragraph shall be provided.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right-handed) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 inch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or jagged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around to allow for drilling and binding.

i. Either single-or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

j. The guide shall be provided in standard three ring notebook binders for ease of maintenance.

10.3. General The level of trust enforced by the Trusted Computing Base (TCB) shall determine the depth and size of the Security Features User's Guide (SFUG). This level determines the security functions needed. The SFUG shall describe the security functions used by operational users who are not specially trained as operators, security administrators, or system administrators.

10.4 Content. The SFUG shall be prepared as follows:

a. A description of the prominent features of each security protection mechanism(s) (e.g., I&A, DAC, MAC, and Object Manipulation Facilities) which pertain to the operational users shall be provided.

b. A description of the interface between the security protection mechanism(s) and the operational user. It shall also describe the use of the security protection features by the operational users. The SFUG shall include cautions and precautions concerning the consistent and effective use of the described protection features.

DI-MCCR-81349

Block 10. PREPARATION INSTRUCTIONS (Continued)

c. The SFUG shall address the relationships between the operators, system administrators, or security administrators, and the operational user (e.g., the security administrator may control user password generation features). Interface(s) necessary for the user to understand his or her use of each security protection mechanism shall be completely described in the SFUG.

d. The SFUG shall include a description of expected reaction to security-related events (e.g., access violations, security- related failures). Every advisory or other response from each security protection mechanism(s) shall be documented, using the exact electronic text produced. Both affirmative and negative responses shall be illustrated by example dialogue (e.g., [User] Log-In Password Verified; [User] Access Denied; (User] Discretionary Permission Exceeded for File xxxx).

e. Cross-references to relevant documentation containing a more detailed description of the security protection mechanism(s) and their relationships shall be provided, where applicable, in the SFUG. All cross-references shall be to the subparagraph level in the referenced document.

f. Charts, figures, and caricatures should be used in the SFUG whenever possible to illustrate complex concepts, relationships, or interfaces to operational users not specially trained in security.

10.4.1 Class B2 products and their equivalent systems. The procedures for the operational user to utilize the trusted communication path between the TCB and the user for initial login and authentication shall be explicitly defined in the SFUG. The SFUG shall describe how the communications via this path are initiated exclusively by the user.

10.4.2 Class B3 and above products and their equivalent systems. The procedures for the operational user to utilize the trusted communication path between the TCB and the user for use when a positive TCB-to-user connection is required (e.g., login, change subject security level) shall be explicitly defined in the SFUG. The SFUG shall describe how the communications via this trusted path are activated exclusively by the user or the TCB. The SFUG shall describe how the trusted path is logically isolated and unmistakably distinguishable by the user from other paths.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
TRUSTED FACILITY MANUAL	DI-TMSS-81352

3. DESCRIPTION/PURPOSE

3.1 The Trusted Facility Manual (TFM) explains how the security administrator, system administrator, or operator establish, operate, and maintain a secure environment. The security administrator is responsible for the secure administration of the environment. The system administrator is responsible for the overall functioning of the environment. Finally, the operator is responsible for the day-to-day operation of the environment.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.1.3.1.2, 2.1.4.2, 2.2.4.2, 3.1.2.2, 3.1.4.2, 3.2.2.1.1, 3.2.3.1.4, 3.2.4.2, 3.3.2.1.1, 3.3.2.2, 3.3.3.1.4, 3.3.3.1.5, 3.3.4.2 and 4.1.3.2.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that requires administrator-oriented documentation as prescribed by DOD-5200.28-STD, Department of Defense Trusted

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6942

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. The TFM shall contain:

a. Cover Sheet. Include Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version, number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Provide sheet delimiting cumulative page changes from previous version(s).

c. Table of Contents. Include paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly summarizes the Trusted Facility Manual.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-TMSS-81352

Block 7. APPLICATION/INTERRELATIONSHIP (Continued)

Computer System Evaluation Criteria, Classes C1 (Discretionary Security Protection), and above, products or their equivalent systems.

7.3 The information required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1, 10.3.2, 10.3.3, 10.3.4, and 10.3.5 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Manual.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective Index. An exhaustive index of the key word or theme in each paragraph shall be provided.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right hand) page.
e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.
f. Fold out pages shall be kept to a minimum.
g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or jagged right (left justified only) shall be used.
h. At least one inch margins shall be provided all around to allow for drilling and binding.
i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.
j. The manual shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The Trusted Facility Manual (TFM) shall describe procedures for selecting security options that are needed to meet operational requirements in a secure manner. The level of detail should span the gap between the user-oriented Security Features User's Guide and the security engineer-oriented design documentation. The TFM shall be addressed to the system administrator, security administrator, or operator and provide the following information:

a. The TFM shall briefly identify and describe the computer acquisition for which the TFM applies. It shall identify and describe any peripheral equipment necessary for either a secure or functional application. The TFM shall also discuss, if appropriate, use in all possible different environments.

DI-TMSS-81352

Block 10. PREPARATION INSTRUCTIONS (Continued)

b. The TFM shall describe all of the security mechanisms for the computer environment as these features involve the administrator: the communication (e.g., communications links and network connections); TEMPEST; hardware; software; and storage media.

c. The TFM shall describe the cautions about functions and privileges that should be controlled when running a secure facility.

d. The TFM shall describe the procedures (for hardware and software features) that must be used to periodically validate the correct operation of the on-site operational TCB hardware and firmware elements.

10.3.1 Classes C2 and above products and their equivalent systems. The following shall be included:

a. Identification of the audit files. It shall describe the procedures for examining and maintaining the audit files.

b. Identification of the audited events. It shall describe the detailed audit record structure for each type of audit event.

10.3.2 Classes B1 and above products and their equivalent systems. The following shall be included:

a. A description of the duties, responsibilities, functions, privileges, and interrelationships of the system user, operator, and administrator related to security. This shall include the actions required to change the security characteristics of a user/administrator.

b. The guidelines on the consistent and effective use of the facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner.

c. The guidelines on the consistent and effective use of the protection features (e.g., controlling access, initialization of storage objects, importation of data without labels, label designation of communications channels, exportation of labels, labeling of human-readable output, identification and authentication of users). This shall include how the protection features interact.

d. A description of the procedures used to generate a new TCB. The steps necessary to validate and ensure that all changes which are incorporated conform to the requirements for the TCB class shall be described in the TFM.

e. A description of how the audit mechanism audits the override of human readable output markings.

10.3.3 Classes B2 and above products and their equivalent systems. The following shall be included:

a. The TCB modules that contain the reference validation mechanism shall be identified in the TFM.

b. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described in the TFM.

c. The separation of operator and administrator functions.

d. The procedures that the administrator/user must follow to reach the trusted communication path between the administrator/user and the TCB.

DI-TMSS-81352

Block 10. PREPARATION INSTRUCTIONS (Continued)

e. The guidelines on the consistent and effective use of the protection features (e.g., change of terminal user security level during interactive session, assignment of security levels to attached devices, identification of covert storage channels in audit data, and safeguards to ensure least privilege). This shall include how the protection features interact.

10.3.4 Classes B3 and above products and their equivalent systems. The following shall be included:

a. Operational procedures necessary to achieve the initial secure processing state. Include any instructions necessary to maintain the secure state.

b. The functions performed in the role of a security administrator shall be identified in the TFM. The TFM shall describe the procedure (a distinct auditable action) that allows a user to access the security administrator role. The TFM shall identify the means by which non-security functions (e.g., those essential to performing the security role effectively) can be performed in the security administration role.

c. The mechanism that monitors the occurrence or accumulation of security auditable events that may indicate an imminent violation of security policy. The TFM shall describe how the security administrator will be notified when thresholds are exceeded. The TFM shall also identify the security administrator's role in the action which will occur to terminate the events, if the occurrence or accumulation of these security relevant events continues.

d. The procedures for the administrator/user to utilize the trusted communication path between the TCB and the administrator/ user, for use when a positive TCB-to-user connection is required (e.g., login, change subject security level), shall be explicitly defined in the TFM. The TFM shall describe how the communications via this trusted path is activated exclusively by the administrator/user or the TCB. The TFM shall describe how the trusted path is logically isolated and unmistakably distinguishable by the administrator/user from other paths.

e. The guidelines on the consistent and effective use of the protection features (e.g., listing individuals or groups with access to specific objects, and identification of covert channels in audit data). This shall include how the protection features interact.

f. The TFM shall include the description of procedures necessary to resume secure operation after any lapse of operation. The following items shall be included in the TFM to be assigned exclusively to administrative personnel with security-relevant responsibility.

1) Procedures for analysis of dumps, for consistency checking of TCB objects, and for cold start and emergency restart.

2) A description of the types of tolerated failures and examples of the recommended procedures for responding to such failures.

3) Procedures for running periodic integrity checks on the TCB database and for repairing damaged security labels.

4) Procedures for handling inconsistencies of the objects (e.g., duplicate allocation of disk blocks to objects, inconsistent object links).

5)Lists of commands, TCB calls, and function definitions for trusted recovery (whenever these aren't documented in the DTLS).

6) Examples of, and warnings about, potential misuse of trusted recovery procedures.

10.3.5 Classes A1 products and their equivalent systems. The following shall be included:

a. A description of the distribution facility procedures provided for maintaining the integrity of the on-site operational TCB master copy.

b. A description of the procedures that ensure that the TCB software, firmware, and hardware updates distributed are exactly as specified by the master copies.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
PHILOSOPHY OF PROTECTION REPORT	DI-MISC-81348

3. DESCRIPTION/PURPOSE

3.1 This report details an informal description of a security policy and the overall high level design of a Trusted Computing Base (TCB) delineating each of the protection mechanisms (both TCB and non-TCB) employed to enforce the policy.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.1.4.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2. This DID is applicable to any computer acquisition that calls for a Philosophy of Protection Report as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria for a TCB Class C1 (Discretionary Security Protection), or

(Continued on page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b AMSC NUMBER
		G6938

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the Philosophy of Protection Report as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version, number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distributed Statement A: This DID is approved for public release; distribution is unlimited.

DI-MISC-81348

Block 7, APPLICATION/INTERRELATIONSHIP (Continued)

above, products or their equivalent systems. The Philosophy of Protection Report is based on the security policy enforced by the TCB derived from U.S. Government laws, regulations, standards, and practices.

Block 10, PREPARATION INSTRUCTIONS (Continued)

f. Executive Summary, not to exceed two pages, that briefly describes the TCB's security-related capabilities.
g. Introduction.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective index.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right hand) page.
e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.
f. fold out pages shall be kept to a minimum.
g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.
h. At least one inch margins shall be provided all around to allow for drilling and binding.
i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.
j. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The following shall be included in the Philosophy of Protection Report:

a. The Philosophy of Protection Report shall provide a description of the explicit and well-defined security policy enforced by the TCB and the environment, as appropriate The discussion shall include the applicable laws, rules, and regulations. This description shall be in enough detail to form the background for the philosophy of protection discussions.
b. The Philosophy of Protection Report shall describe the high-level TCB protection mechanisms derived from the policy. It shall describe the philosophy of protection for the TCB. This encompasses the enumeration of any assumptions and constraints, with the rationale and justification for using each. These assumptions and constraints may be applicable for justifying distribution of the security requirements through the TCB.

DI-MISC-81348

Block 10, PREPARATION INSTRUCTIONS (Continued)

c. The Philosophy of Protection Report shall describe the environmental mechanisms supporting the policy. It shall provide an explanation of how the security policy is translated into environmental constraints, connectivity constraints, and the specific TCB protection mechanism(s). This discussion shall include any entity that enforces the security policy, either external or internal to the computer itself (e.g., physical access control, TCB access control).

d. The Philosophy of Protection Report shall describe the TCB mechanisms supporting the policy. It shall show how the philosophy of protection is translated into the TCB hardware, software, and firmware; as appropriate. The Philosophy of Protection Report shall relate the security requirements to the architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
INFORMAL SECURITY POLICY MODEL	DI-MISC-81341

3. DESCRIPTION/PURPOSE

3.1 An informal security policy model provides an abstract representation of a trusted computing base (TCB) and the security policy enforced by the TCB.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.1.4.4 and 3.1.3.2.2 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for an informal security policy model as specified by DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Class B1 (Labeled Security Protection)

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6931

10. PREPARATION INSTRUCTIONS

10.1 Source Document . The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document an Informal Security Policy Model as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited

DI-MISC-81341

Block 7, APPLICATION/INTERRELATIONSHIP (Continued)

products or their equivalent systems. The TCSEC Class B1 requirement is for either an Informal Security Policy Model or a Formal Security Policy Model. If a Formal Security Policy Model is required and is available, then the Informal Security Policy Model is redundant and not necessary. Then Informal Security Model is based upon the Philosophy of Protection Report.

Block 10. PREPARATION INSTRUCTIONS (Continued)

f. Executive Summary, not to exceed two pages, that briefly describes the security model, including its assumptions and limitations.
g. Introduction.
h. Body of the Report.
i. Attachments.
1. Subjective index.
j. Appendices.
k. Bibliography. List of reference sources and applicable documents.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right hand) page.
e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.
f. Fold out pages shall be kept to a minimum.
g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.
h. At least one inch margins shall be provided all around each page to allow for drilling and binding.
i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.
j. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The Informal Security Policy Model document shall contain 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 which 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 shall include the representation of subjects objects, modes of access, and security labels; the set of security properties enforced by the TCB; the representation of the initial state of the TCB; and the representations of the operations performed.

DI-MISC-81341

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.3.1 General. The Informal Security Policy Model document shall provide background information supporting the modeling effort. All of this background information is informal in nature and may be presented in English text, and graphic representations where appropriate. The following information shall be included as part of this information:

a. Summarization of the security policy to be modeled, how this policy relates to the overall security policy (if the policy modeled is some subset of the overall policy), and the source of the policy. This discussion shall be in enough detail to form the background for the model.

b. Discussion of the model chosen, and the rationale for why this model was chosen.

c. Discussion of the modeling technique/methodology chosen, and the rationale for why this technique/methodology was selected over other possible techniques.

d. Expansion of the security policy into security policy statements. These security policy statements may be brief, but they must explicitly and thoroughly describe the security policy. Each policy statement shall be mapped to the Philosophy of Protection Report.

e. Introduction to the kinds of assurance arguments that are provided, along with a rationale that explains why these arguments are sufficient to demonstrate that the TCB is secure with respect to the security properties modeled.

10.3.2 Policy segment. The Informal Security Policy Model document shall provide an informally stated mathematical description of the policy enforced by the TCB. Also, an English language description of the policy model and each of its segments shall be provided. Supporting material shall be provided in the following sequence:

a. All assumptions used in the model, using an English language description. The Informal Security Policy Model document shall state the assumptions derived from the Philosophy of Protection Report, and explain why the assumptions are necessary to the model. It shall also explain why all identified assumptions are required, and the consequences of violating the assumptions.

b. All axioms used in the model, using an English language description. The Informal Security Policy Model document shall provide supporting rationale for including each axiom.

c. The actual model of the policy. Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics shall be annotated with brief English language descriptions. Supporting material shall be provided to describe each of the following:

(1) The classes of subjects and objects controlled by the TCB. Examples of subjects are people, processes, or devices; and objects are records, blocks, pages, components, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

(2) How subjects are related to users.

(3) How subjects are assigned privileged conditions (trusted subjects).

(4) How users identify themselves to the TCB.

(5) How the TCB records events.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.3.3 Abstract mechanisms segment. The Informal Security Policy Model document shall describe the abstract TCB protection mechanism(s). The following supporting material shall be provided:

a. The actual model of the abstract TCB protection mechanism(s). Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics shall be augmented with brief English language descriptions. The model shall include the following abstract mechanism(s), for example:

(1) All the rules which permit, as well as constrain, how a subject is allowed access to an object.

(2) All privileged conditions under which certain kinds of subjects are allowed to bypass the identified mandatory and discretionary access control rules.

(3) All controls on assigning subjects privileged conditions.

(4) All the controls on identifying users to the TCB.

(5) All the rules that generate an audit event.

b. The explanation of how the abstract protection mechanism(s) satisfy the security policy model. Each mechanism shall be discussed separately. The explanation shall include a description of how each element within a mechanism supports other elements of the mechanism.

10.3.4 Segment integration. The integration of the policy and abstract protection mechanism segments of the model shall provide the assurance arguments of the Informal Security Policy Model document. It shall include the following:

a. An explanation to show that the model is consistent with its axioms. The explanation shall provide rationale sufficient to demonstrate consistency.

b. A description of the relationship of each axiom to the model's segments and specific security-enforcement abstract mechanism(s) in the model.

c. An explanation which shows that the TCB is sufficient to enforce the security policy. The explanation shall provide rationale sufficient to demonstrate consistency.

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
FORMAL SECURITY POLICY MODEL	DI-MISC-81346

3. DESCRIPTION/PURPOSE

3.1 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 trusted computing base (TCB), the model must be supported by formal proof. This Data Item Description (DID) describes both the requirements for the model itself and the document in which the model will be delivered.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.1.4.4, 3.1.3.2.2, 3.2, 3.2.3.2.2, 3.2.4.4, 3.3.3.2.2 and 3.3.4.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for a formal security policy model as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B1 (Labeled Security Protection), B2

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6936

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document a Formal Computer Security Policy Model as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, and any other appropriate descriptive data.

b. Errata Sheet. Errata sheets shall contain delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly describes the security model, including its assumptions and limitations.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited

DI-MISC-81346

Block 7 APPLICATION/INTERRELATIONSHIP (Continued)

(Structured Protection), B3 (Security Domains), or A1 (Verified Design) products or their equivalent systems. The Formal Security Policy Model is an optional requirement at TCSEC Class B1. If an Informal Security Policy Model is required and available at TCSEC CLASS B1, then the Formal Security Policy Model is redundant and not necessary. The Formal Security Policy Model is based on the Philosophy of Protection Report.

Block 10, PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective index.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Black pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 12 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around each page to allow for drilling and binding.

i. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

j. The report shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 General. The formal Security Policy Model document shall contains the formal security policy model, it s 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 which is to be enforced by the TCB, and 2) a mathematical representation of the abstract protection mechanism(s) within the TCB which enforce the described policy. The model shall include the representation of subjects, objects, modes of access, and security labels; the set of security properties enforced by the TCB; the representation of the initial state of TCB; and the representations of the operations performed.

DI-MISC-81346

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4 Content. The Formal Security Policy Model document shall provide background information supporting the modeling effort. All of this background information is informal in nature and may be presented in English text, and graphic representations where appropriate. The following items shall be included as part of this information:

a. Summarization of the security policy to be modeled, how this policy relates to the overall security policy (if the policy modeled is some subset of the overall policy), and the source of the policy. This discussion shall be in enough detail to form the background for the model.

b. Discussion in detail of the type of model chosen, and explanation of why this type was selected over other types.

c. Identification of the modeling technique/methodology chosen, and why it was chosen.

d. Expansion of the security policy into security policy statements. These security policy statements may be brief, but they must explicitly and thoroughly describe the security policy. Each policy statement shall be mapped to the Philosophy of Protection Report.

10.4.1 Policy segment. The Formal Security Policy Model document shall provide a formal mathematical description of the policy enforced by the TCB. Also, an English language description of the formal security policy model and each of its segments shall be provided. Supporting material should be provided in the following sequence:

a. All assumptions used in the model, provided as both mathematical statements (if any) and an English language description. Sufficient supporting rationale to prove the validity of the assumptions shall be provided. An explanation of why the assumptions are necessary to the model and the consequences of violating the assumptions shall also be provided.

b.All axioms used in the model, using both mathematical statements and an English language description. This discussion shall include the rationale as to why these axioms are needed and how the axioms are justified. Supporting rationale for each axiom shall be provided by describing its relationship to the model's segments and specific security-enforcement abstract mechanisms in the model.

c. The actual model of the policy. Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics shall be annotated with English language descriptions. Supporting material shall be provided to describe each of the following:

(1) The classes of subjects and objects controlled by the TCB. Examples of subjects are people, processes, or devices; and objects are records, blocks, pages, components, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

(2) How subjects are related to users.

(3) How subjects are assigned privileged conditions (trusted subjects).

(4) How users identify themselves to the TCB.

(5) How the TCB records events.

DI-MISC-81346

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.2 Abstract mechanism segment. The actual model of the abstract TCB protection mechanism(s). Graphic representations of the model's segments may be included (e.g., diagrams and tables). These graphics may be annotated with English language descriptions. Supporting material shall be provided to describe each of the following:

a. All the rules that permit, as well as constrain, how a subject is allowed access to an object.
b. All privileged conditions under which certain kinds of subjects are allowed to bypass the identified mandatory and discretionary access control rules.
c. All controls on assigning privileged conditions to subjects.
d. All the controls on identifying users to the TCB.
e. All the rules that generate an audit event.
f. All TCB responses to failures.

10.4.3 Class B1 products and their equivalent systems. The following shall be included in this section:

10.4.3.1 General. There is no change to the general requirements of the Formal Security Policy Model document for TCB Class B1 products and their equivalent systems.

10.4.3.2 Policy segment. There is no change to the policy requirements of the Formal Security Policy Model document for TCB Class B1 products and their equivalent systems.

10.4.3.3 Abstract mechanism segment. The Formal Security Policy Model document shall identify the abstract TCB protection mechanism(s) and explain how these mechanisms satisfy the security policy model. Each abstract mechanism shall be discussed separately. Cross-reference these mechanisms to the policy portion of the Philosophy of Protection Report. The explanation shall include a description of how each element within a mechanism supports other elements of the mechanism, if any.

10.4.3.4 Segment integration. The integration of the policy and abstract mechanism segments of the model shall include the following:

a. An explanation to show that the formal security policy model is consistent with its axioms. The explanation shall provide rationale sufficient to demonstrate consistency.
b. A description of the relationship of each axiom to the model's segments and specific security-enforcement mechanism(s) in the model.
c. An explanation that shows that the TCB is sufficient to enforce the security policy. The explanation shall provide rationale sufficient to demonstrate consistency.

10.4.4 Classes B2 and above products and their equivalent systems. The following shall be included in this section:

10.4.4.1 General. The TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in Class B1 TCBs to be extended to all subjects and objects.

DI-MISC-81346

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.4.2 Policy segment. The Formal Security Policy Model document shall provide all theorems used in the model for each security policy segment, using both mathematical statements and an English language description. Supporting rationale for including the theorems shall be provided. The Formal Security Policy Model shall discuss how these theorems represent enforcement of the security policy.

10.4.4.3 Mechanisms segment The Formal Security Policy Model shall provide all theorems used in the model for the TCB protection mechanism(s), using both mathematical statements and an English language description. Supporting rationale for including the theorems shall be provided. The Formal Security Policy Model shall discuss how these theorems represent the TCB protection mechanism(s) and their enforcement of the security policy.

10.4.5 Segment integration. The Formal Security Policy Model document shall include an introduction to the kinds of proofs that are provided, along with a rationale that explains why these proofs are sufficient to demonstrate that the TCB is secure with respect to the security properties modeled. The integration of the policy and abstract mechanism segments of the model shall include the following proofs:

a. Proof that the model is consistent with its axioms, providing both the mathematical proofs and an English language description of the proofs.

b. Proof that shows that the TCB represented in the model is sufficient to enforce the security policy. The Formal Security Policy Model document shall trace each of the following:

(1) The security policy statements in the Philosophy of Protection Report to a formal mathematical statement. A cross reference matrix chart with detailed explanatory text may be used.

(2) The formal mathematical statements back to its security policy statements in the Philosophy of Protection Report. A cross reference matrix chart with detailed explanatory text may be used.

c. Proof for each of the theorems used in the model, both the mathematical proof and an English language description of the proof.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
DESCRIPTIVE TOP LEVEL SPECIFICATION	DI-MISC-81342

3. DESCRIPTION/PURPOSE

3.1 The Descriptive Top Level Specification (DTLS) is a top level specification using English language descriptions. It completely and accurately describes the trusted computing base (TCB) in terms of exceptions, error messages, and effects. The DTLS is an accurate description of the TCB interface.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.2.3.1.1, 3.2.3.2.2, 3.2.4.4, 3.3.3.2.3, and 4.1.3.2.2 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for a DTLS as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B2 (Structured Protection), B3 (Security Domains), or A1 (Verified Design) products and their equivalent systems. (Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6932

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the DTLS as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version, number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous versions.

c. Table of Contents. Include paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly describes the TCB's security-related capabilities.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-MISC-81342

Block 7. APPLICATION/INTERRELATIONSHIP (Continued)

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1, 10.3.2, and 10.3.3 are necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the specification.
i. Attachments
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective index

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right hand) page.
e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.
f. Fold out pages shall be kept to a minimum.
g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.
h. At least one inch margins shall be provided all around to allow for drilling and binding.
i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.
j. The specification shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The DTLS shall describe the security capabilities in functional terms and concepts, and therefore takes the broad form of a "security features functional description." It is traceable to the Formal Security Policy Model. The DTLS shall contain the following items:

a. A summary of the security policy. This discussion shall be in enough detail to form the background for the following discussions.
b An overview of the TCB design which describes how the reference monitor concept is implemented, gives an explanation of why the TCB is tamper-resistant, cannot be bypassed, and is correctly implemented.
c. Description of all TCB functions and features that enforce the security policy. The description shall completely and accurately describe the TCB in terms of exceptions, error messages, and effects, and include:

DI-MISC-81342

Block 10. PREPARATION INSTRUCTIONS (Continued)

(1) Mandatory access controls.
(2) Discretionary access controls.
(3) Security labels associated with subjects and objects.
(4) Markings applied to external media.
(5) TCB internal data bases.
(6) Mapping between physical entities (e.g., users, files) and their logical representations (e.g., subjects, objects).
(7) Policy rules used by the TCB to grant or deny access by subjects to objects (e.g., a subject's clearance must dominate an object's classification in order to be granted access).

d. An accurate description of the TCB interface.
e. A complete description of the user interface.

10.3.1 Classes B3 and A1 products and their equivalent systems. The following shall be included in this section:

a. A convincing argument shall be presented in the document to show that the DTLS is consistent with the Formal Security Policy Model.
b. A description of the specific TCB protection mechanisms used to ensure trusted recovery functions. It shall also describe the TCB modules implementing interfaces of trusted recovery.

10.3.2 Class A1 products and their equivalent systems. The DTLS shall include those components of the TCB that are implemented as hardware and/or firmware, if their properties are visible at the TCB interface.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
FORMAL TOP LEVEL SPECIFICATION	DI-MISC-81347

3. DESCRIPTION/PURPOSE

3.1 The Formal Top Level Specification (FTLS) is a mathematically precise abstract representation of the trusted computing base (TCB). The FTLS provides an accurate description of the TCB interface in terms of exceptions, error messages and effects. The FTLS includes hardware and firmware elements if their properties are visible at the TCB interface.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 4.1 and 4.1.3.2.2 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for an FTLS as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Class A1 (Verified Design) products and their equivalent systems.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6937

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the FTLS as follows:

a. Cover sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definition. List reference sources and applicable documents.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-MISC-81347

Block 10. PREPARATION INSTRUCTIONS (Continued)

f. Executive Summary, not to exceed two pages.
g. Introduction.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography.
l. Subjective index.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right hand) page.

e. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

10.3 General. The FTLS document shall contain the formal top level specification, its associated proofs and assurance arguments, and supporting explanations and documentation for the specification, proofs, and assurance arguments.

10.4 Content.

10.4.1 Supporting documentation. The FTLS shall provide background information supporting the specification effort. All of this background information is informal in nature and may be presented in English text, and graphic representation where appropriate. The following items shall be included as part of this information:

a. An overview of the FTLS that explains the approach taken, the structure of the specification, what has been included and excluded in the specification, and how the specification relates to the Formal Security Policy Model.

b. Identification of the portions of the FTLS that are implemented in hardware, software, and in firmware if their properties are visible at the TCB interface.

c. A description of the specification/verification methodology chosen, and why it was selected.

d. An introduction to the specification itself, to include identification of the users, subjects, objects, access modes, security labels, security properties, initial state, and operations that are part of the specification.

e. Identification of the assumptions required by the specification, an explanation as to why they are required, and the consequences of violating the assumptions.

f. A combination of formal and informal techniques (e.g., proofs and assurance arguments) that show that the FTLS is consistent with the Formal Security Policy Model.

g. Identification of the axioms used in the proofs, why these axioms are needed, and how they are justified.

DI-MISC-81347

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.4.2 The formal top level specification. The following shall be included in this section:

a. As part of the FTLS document, the specification itself shall be presented in the formal mathematical notation of the specification technique chosen. The specification shall include abstract definitions of the functions the TCB performs and the unified protection mechanism required to satisfy the security policy (TCSEC Section 4.1), to include the following:

(1) Representation of subjects, objects, modes of access, and security labels as they are implemented in the TCB.
(2) Representation of hardware and firmware components of the TCB if their properties are visible at the TCB interface.
(3) The set of security properties enforced by the TCB.
(4) Representation of the initial state of the TCB.
(5) Representations of the operations performed by the TCB, including the effects, exceptions, and error messages for interface operations.
(6) A (possibly empty) set of axioms used in the proofs.

b. The FTLS shall include the abstract definitions of the hardware and firmware mechanisms that are used to support separate execution domains.

10.4.3 Proofs and arguments. this section shall contain, a combination of formal techniques (e.g., where verification tools exist) and informal techniques (e.g., convincing assurance arguments) to demonstrate that the FTLS is consistent with the Formal Security Policy Model.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
DESIGN SPECIFICATION	DI-MCCR-81344

3. DESCRIPTION/PURPOSE

3.1 The Design Specification demonstrates the correct implementation and enforcement of the security policy throughout the trusted computing base (TCB). It shall explain the protection mechanisms of the TCB to the extent that the effect a change may have on the TCB can be evaluated prior to a technical change performed.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.1.3.1.1, 2.1.4.4, 2.2.3.1.1, 3.1.3.1.1, 3.1.4.4, 3.2.3.1.1, 3.2.3.1.4, 3.2.4.4, 3.3.3.1.1, 3.3.4.4, and 4.1.4.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2. This DID is applicable to any computer acquisition that calls for a Design Specification as specified by DOD-5200.28 STD, Department of Defense Trusted Computer

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6934

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the Design Specification as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version, number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly describes the TCB's security-related capabilities.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release; distribution is unlimited.

DI-MCCR-81344

Block 7, APPLICATION/INTERRELATIONSHIP (Continued)

System Evaluation Criteria (TCSEC) for TCB Classes C1 (Discretionary Security Protection),and above, products or their equivalent systems. The Design Specification identifies and describes the TCB and its security features.

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DDI as a whole. In addition, the information required in 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5 and 10.3.6 are necessary for various classes of products and their equivalent systems.

Block 10, PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Specification
i. Attachments.
l. Subjective index.
j. Appendices
k. Bibliography. List reference sources and applicable documents.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right hand) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around to allow for drilling and binding.

i. Either single or double sided printing may be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

j. The specification shall be provided in standard three-ring notebook binders for ease of maintenance.

10.3 Content. The Design Specification shall contain the following items:

a. A statement of the security policy. This description shall be in enough detail to form the background for the design discussions.

b. The Design Specification shall relate the security requirements to the architecture.

c. An explanation of how the security policy is translated into a technical solution through the TCB hardware, software, and firmware.

DI-MCCR-81344

Block 10, PREPARATION INSTRUCTIONS (Continued)

10.3.1 Classes C1, C2, and B1 products and their equivalent systems. The following shall be included in this section:

a. Description of how the TCB is modularized (if modular).
b. Description of all interfaces between the TCB modules (if modular).
c. Description of how the TCB protects itself from external interference or tampering.
d. Description of the resources which are controlled by the TCB. These resources may be a defined subset of the subjects and objects.

10.3.2 Classes C2 and B1 products and their equivalent systems. The Design Specification shall describe how the TCB isolates the resources to be protected so that they are subject to the access control and auditing requirements.

10.3.3 Classes B1 products and their equivalent systems. The following shall be included in this section:

a. Identification and description of the TCB protection mechanisms.
b. An explanation to show that the TCB protection mechanisms satisfy the model.
c. Description of how the TCB maintains process isolation through the provision of distinct address spaces under its control.

10.3.4 Classes B2 and above products and their equivalent systems. The following shall be included in this section:

a. Description of how the TCB is structured to facilitate testing.
b. Description of the different sets of privileges assigned to differing roles (e.g., users, administrators).
c. Description of the design techniques involved in restricting covert storage channels.
d. Description of the interfaces between the TCB modules.
e. Description of how the TCB complies with additional B2 architecture requirements. The following requirements shall be described:
1) TCB maintenance of a domain for its own execution that protects it from external interference or tampering.
2) TCB maintenance of process isolation through the provision of distinct address spaces under its control.
3) Features in hardware, such as segmentation, used to support logically distinct storage objects with separate attributes (namely: readable, writable).
4) TCB modules structured such that the principle of least privilege is enforced.
5) TCB internally structured into well-defined largely independent modules.
6) Effective use of available hardware by TCB to separate those elements that are protection-critical from those that are not.
f. Description of the trusted communication path between the TCB and user.

DI-MCCR-81344

Block 10, PREPARATION INSTRUCTIONS (Continued)

10.3.5 Classes B3 and above products and their equivalent systems. The following shall be included in this section:

a. Description of the design techniques involved in restricting covert timing channels.

b. Description of how the TCB complies with additional B3 architecture requirements. The following requirements shall be described:

1) Complete, conceptually simple protection mechanism with precisely defined semantics. The Design Specification shall describe how this mechanism plays a central role in enforcing the internal structuring of the TCB.

2) Significant use of layering, abstraction, and data hiding by the TCB.

3) Minimization of the complexity of the TCB, excluding the modules that are not protection-critical.

c. The Design Specification shall describe the following for trusted recovery:

1) Anticipated classes of failures and discontinuities of operation handled by trusted recovery, automatically or using administrative procedures.

2) Trusted recovery philosophy (e.g., use of failure-atomicity in the design of TCB primitives, of non-atomic actions which allow recovery).

3) Warnings concerning the 'unanticipated' (i.e., rare) failures that can't be handled in a routine manner.

d. Description of how the specific TCB protection mechanisms used ensuring trusted-recovery functions are available only to administrative users.

10.3.6 Class A1 products and their equivalent systems. The Design Specification shall describe the hardware, software, and firmware mechanisms not dealt with in the FTLS but strictly internal to the TCB (e.g., mapping registers, direct memory access I/O).

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
TRUSTED COMPUTING BASE VERIFICATION REPORT	DI-MISC-81350

3. DESCRIPTION/PURPOSE

3.1 The Trusted Computing Base (TCB) Verification Report documents the results of verifying the correlation between the Descriptive Top Level Specification (DTLS) or the Formal Top Level Specification (FTLS) of a TCB and its implementing programming language source statements.

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.3.4.4 and 4.1.3.2.2 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for the verification of the correspondence/mapping between an implemented TCB and a TLS as specified by DOD-

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6940

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the outcome of a verification of the implementing source language statements to the TLS as follows:

a. Cover Sheet: Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.
b. Errata Sheet. Shall contain sheet delimiting cumulative page changes from previous version(s).
c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.
d. List of illustrations, diagrams, charts and figures.
e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-MISC-81350

Block 7, APPLICATION/INTERRELATIONSHIP(Continued)

5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B3 (Security Domains) and A1 (Verified Design) products and their equivalent systems.

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1 and 10.3.2 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
f. Executive Summary, not to exceed two pages, that briefly summarizes the TCB Verification Report.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography. List references and all applicable documents.
l. Subjective index.

10.2.1 Specific format instructions.

a. Abbreviations acronyms shall be defined when first used in the text and shall be placed in the glossary.
b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.
c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.
d. Chapters shall begin on an odd-numbered (right-handed) page.
e. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

10.3 Content. At TCB Class B3 level, the TCB Verification Report provides the correspondence between the Descriptive Top Level Specification (DTLS) and the TCB implementing source code to demonstrate that the DTLS has been correctly and accurately implemented. At TCB Class A1 level, the Formal Top Level Specification (FTLS) is mapped to the source code to demonstrate that the FTLS has been accurately implemented in the selected programming language (and hardware). The TCB Verification Report shall include:

a. The TCB Verification Report shall briefly describe the TCB whose implementation will be verified in the report.
b. The TCB Verification Report shall describe and illustrate the techniques and rules used.

10.3.1 Class B3 products and their equivalent systems. The DTLS is a top level specification informally written. From the design in the DTLS, the implementing program is written using source language statements. The correspondence called for here shall show that these source language statements correctly and accurately reflect the DTLS.

Block 10, PREPARATION INSTRUCTIONS (Continued)

a. The TCB Verification Report shall informally show that the TCB implementation (i.e., in hardware, firmware, and software) is consistent with the DTLS.

b. The TCB Verification Report shall show, using informal techniques, that the elements of the DTLS correspond to the elements of the TCB.

c. For every portion of the TCB software which does not correspond to the DTLS, a convincing rationale shall be provided that this "residual" code is consistent with the DTLS, does not violate the design of the DTLS, and has a valid function within the TCB (i.e., the TCB does not contain any "Trojan Horse" code).

10.3.2 Class A1 products and their equivalent systems. The FTLS is a top level specification written and verified in a formal language. The following shall be included:

From the FTLS, the implementing program is written using source language statements from the selected programming language. The mapping called for here provides evidence of the accurate implementation of the FTLS to the TCB source code.

a. A description of how the specification language constructs relate to the selected programming language constructs.

b. A detailed mapping of the TCB implementation in software, firmware, or hardware to the FTLS. This mapping shall demonstrate that the TCB implementation is consistent with the FTLS.

c. The TCB Verification Report shall show, using informal techniques, that the elements of the FTLS correspond to the elements of the TCB.

d. For every portion of the TCB software, which does not correspond to the FTLS, a convincing rationale shall be provided that this "residual" code is consistent with the FTLS, does not violate the properties of the FTLS, and has a valid function within the TCB (i.e., the TCB does not contain any "Trojan Horse" code).

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
TRUSTED COMPUTING BASE CONFIGURATION MANAGEMENT PLAN	DI-CMAN-81343

3. DESCRIPTION/PURPOSE

3.1 The Trusted Computing Base (TCB) Configuration Management (CM) Plan details the TCB configuration control process, configuration management procedures, and review and approval procedures for changes to the security design implementation of the TCB. It addresses hardware, firmware, software, testing and documentation at the various levels of

(Continued on Page 2)

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.2.3.2.3, 4.1.3.2.3, 4.1.3.2.4 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that calls for a TCB Configuration Management Plan as specified by DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) for TCB Classes B2 (Structured Protection), and above, products and their equivalent systems.

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6933

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document a TCB Configuration Management Plan as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-CMAN-81343

Block 3, DESCRIPTION/PURPOSE (Continued)

trust. The TCB CM Plan indicates how the security requirements baseline will be maintained during the operational life of the TCB and 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 TCB.

Block 7,APPLICATION/INTERRELATIONSHIP (Continued)

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1 and 10.3.2 is necessary for various classes of products and their equivalent systems.

Block 10, PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Plan.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents.
l. Subjective index.

10.2.1 Specific format instructions.

a Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right hand) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. Standard 10 pitch pica or courier, 12 pitch elite, or equivalent font shall be used. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around to allow for drilling and binding.

i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

j. The plan shall be provided in standard 3 - ring binders for ease of maintenance.

10.3 Content. The TCB CM Plan shall contain the following items:

a. Description of the methods available to certify that only the approved, intended changes are made in the code that will be used as the new version of the TCB.

b. Identification of methods that ensure that any change in the approved design documentation is developed under configuration control.

DI-CMAN-81343

Block 10, PREPARATION INSTRUCTIONS (Continued)

c. Description of how the configuration management system ensures consistent mapping among all documentation and code associated with the current version of the TCB.

d. Description of the auditing methods which will be used by the configuration management system to maintain a history of all changes made to the TCB.

e. Description of the tools that are provided for generation of a new version of the TCB from source code.

f. Description of the tools that are provided for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

10.3.1 Classes B2 and B3 products and their equivalent systems. The following shall be included in this section:

a. Description of the tools that ensure that only approved changes are made over the life cycle. These tools should provide for comparing a newly generated version of the TCB with the previous TCB version, and include the steps to be taken if the comparison indicates non-approved changes to the TCB.

b. Description of the configuration controls in place, during the development and maintenance of the TCB, to maintain changes to the descriptive top-level specification, other design data, implementation documentation, source code, and running versions of the object code, and test fixtures and documentation.

10.3.2 Class A1 products and their equivalent systems.. The following shall be included in this section:

a. Description of the tools, maintained under strict configuration control, for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB.

b. Description of the procedures in place, during the design, development and maintenance of the TCB, to maintain changes to all security relevant hardware, firmware, and software. These procedures should maintain control of changes to the formal model, the descriptive and formal top-level specifications, other design data, implementation documentation, source language, and running versions of the object code, and test fixtures and documentation.

c. Description of the technical, physical, and procedural safeguards which are used to protect from unauthorized modification or destruction of the master copy or copies of all material used to generate the TCB.

d. Description of the procedures for assuring that the TCB software, firmware, and hardware updates distributed are exactly as specified by the master copies.

e. Description of the procedures to maintain any configuration management tools under strict configuration control.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
COVERT CHANNEL ANALYSIS REPORT	DI-MISC-81345

3. DESCRIPTION/PURPOSE

3.1 The Covert Channel Analysis Report documents the results of a covert channel analysis on a trusted computing base (TCB).

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 3.2.3.1.3, 3.2.4.4, 3.3.3.1.3, 4.1 and 4.1.3.1.3 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any trusted computer acquisition that calls for a Covert Channel Analysis Report as specified by DOD-5200.28 STD, Department of Defense Trusted

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6935

10. PREPARATION INSTRUCTIONS

10.1 Source Document . The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract.

10.2 Format. Document the Covert Channel Analysis as follows:

a. Cover Sheet. Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous versions.

c. Table of Contents. Shall contain paragraph numbers, paragraph names, and page numbers.

d. List of illustrations, diagrams, charts, and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly describes the Covert Channel Analysis Report.

(Continued on page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-MISC-81345

Block 7, APPLICATION/INTERRELATIONSHIP (Continued)

Computer System Evaluation Criteria (TCSEC) for TCB Classes B2 (Structured Protection), B3 (Security Domains), or A1 (Verified Design) products and their equivalent systems.

7.3 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1, 10.3.2, and 10.3.3 are necessary for various classes of products and their equivalent systems.

Block 10, PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Report.
i. Attachments.
j. Appendices.
k. Bibliography. List reference sources and applicable documents
l. Subjective index..

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right hand) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. The type font shall be standard 10 pitch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or ragged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around to allow for drilling and binding.

i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

j. The report shall be provided in standard three-ring binders for ease of maintenance.

10.3 Content. The Covert Channel Analysis Report shall contain the following:

a. A brief description of the TCB on which the analysis is performed. It shall also provide a synopsis of the analysis performed. A series of charts, diagrams, lists and/or figures may be used to illustrate the major points.

DI-MISC-81345

Block 10, PREPARATION INSTRUCTIONS (Continued)

b. Identification and description of the techniques used to determine the existence of covert channels (e.g., actual measurement, engineering estimates, mathematical projections).

10.3.1 Classes B2 and above products and their equivalent systems. A Covert Channel Analysis Report is required at the B2 level and above. At this level, the analysis is restricted to covert storage channels. The following shall be included in this section:

a. A description of the identified covert storage channels and the determination of the maximum bandwidth of each identified covert storage channel.
b. Identification of trade-offs involved in restricting the use of identified covert channels.
c. A list of all the auditable events that may be used to detect the exploitation of a known storage channel.
d. The bandwidths of known covert storage channels whose use is not detectable by the TCB's auditing mechanisms.

10.3.2 Classes B3 and above products and their equivalent systems. At the B3 level, the scope of the covert channel analysis is expanded to include timing channels in addition to storage channels. The following shall be included in this section:

a. The identified covert timing channels and the determination of the maximum bandwidth of each identified covert timing channel.
b. The identified trade-offs involved in restricting the use of identified covert timing channels.
c. A list of all the auditable events that may be used to detect the exploitation of a known timing channel.
d. The bandwidths of known covert timing channels whose use is not detectable by the TCB's auditing mechanisms.

10.3.3 Class A1 products and their equivalent systems. At this level the Covert Channel Analysis Report shall include:

a. Formal methods in the analysis of the channels.
b. Justification of the continued existence of identified covert channels.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
SECURITY TEST PLAN	DI-NDTI-81351

3. DESCRIPTION/PURPOSE

3.1 The Security Test Plan outlines the test plans and security objectives for a set of specific security tests to be performed. It provides the test concept, reasons, objectives and requirements to be satisfied, support needed, responsible activities associated with the testing, and analysis techniques to be used. It shall provide the strategy to test the security mechanisms of the trusted computing base (TCB).

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
930702	G/C71		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated under the work task described by 2.2.3.2.1, 3.1.3.2.1, 3.2.3.2.1, 3.3.3.2.1 and 4.1.3.2.1 of DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria.

7.2 This DID is applicable to any computer acquisition that requires test documentation for the security features as specified by DOD-5200.28 STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), Classes C1 (Discretionary Security

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G6941

10. PREPARATION INSTRUCTIONS

10.1 Source Document. The applicable issue of the documents cited herein, including their approval date, and dates of any applicable amendments and revisions shall be reflected in the contract

.

10.2 Format. Document a Security Test Plan as follows:

a. Cover Sheet: Shall contain Title, Contract Number, Procuring Activity, Contractor Identification, Acquisition Program Name, disclaimers (as provided by the procuring activity contracting officer), date, version number, security classification, and any other appropriate descriptive data.

b. Errata Sheet. Shall contain sheets delimiting cumulative page changes from previous version(s).

c. Table of Contents. Shall contain paragraph numbers, paragraph names,and page numbers.

d. List of illustrations, diagrams, charts and figures.

e. Glossary of abbreviations, acronyms, terms, symbols, and notation used, and their definitions.

f. Executive Summary, not to exceed two pages, that briefly summarizes the Security Test Plan.

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: This DID is approved for public release. Distribution is unlimited.

DI-NDTI-81351

Block 7 APPLICATION/INTERRELATIONSHIP (Continued)

Protection), and above, products or their equivalent systems.

7.3 The Security Test Plan is generally produced to support certification and accreditation.

7.4 The information required by 10.3 is required for all class products and their equivalent systems applicable to the DID as a whole. In addition, the information required in 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.3.5, 10.3.6 and 10.3.7 is necessary for various classes of products and their equivalent systems.

Block 10. PREPARATION INSTRUCTIONS (Continued)

g. Introduction.
h. Body of the Plan.
i. Attachments.
j. Appendices.
k. Bibliography. List references and all applicable documents.
l. Subjective index.

10.2.1 Specific format instructions.

a. Abbreviations and acronyms shall be defined when first used in the text and shall be placed in the glossary.

b. Pages shall be numbered separately and consecutively using Arabic numerals. Blank pages shall be numbered.

c. Paragraphs shall have a short descriptive title and shall be numbered consecutively using Arabic Numerals. Numbering schemes beyond the fourth level (e.g., 4.1.2.5.8) are not permitted.

d. Chapters shall begin on an odd-numbered (right-handed) page.

e. Column headings shall be repeated on subsequent pages if tabular material exceeds one page.

f. Fold out pages shall be kept to a minimum.

g. Paper shall be standard 8 1/2 x 11 inches, white, with black type. Use standard 10 inch pica or courier, 12 pitch elite, or equivalent font. Either blocked text (left and right justified) or jagged right (left justified only) shall be used.

h. At least one inch margins shall be provided all around each page to allow for drilling and binding.

i. Either single- or double-sided printing shall be used. If double-sided, the document shall be printed or typed head-to-head, front-to-back.

j. The plan shall be provided in standard three ring notebook binders for ease of maintenance.

10.3 Content. The Security Test Plan shall include the method by which testing will be performed to determine whether the TCB works as claimed in the documentation. It shall describe how testing will be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. The Security Test Plan shall include the following:

a. An overview of the TCB that will be tested. It shall briefly describe the security protection mechanism(s).

b. A description of the objectives of the test plan, including the following:

Block 10. PREPARATION INSTRUCTIONS (Continued)

1) A functional description of the security test program.
2) Government and contractor participation roles and responsibilities.
3) Facilities where the testing will be performed.
4) Support requirements for the tests (e.g., communications, equipment, test data, etc).
5) Schedule of when testing will be performed.

c. A list of all tests to be accomplished in the order they are to be performed. The list shall include a test for each security protection function (e.g., unauthorized access to audit data). Each listing shall include the following:

1) Name and brief description of test to be performed.
2) Reason for performing test.
3) Functional requirements which will be tested.
4) Objective to be satisfied by each test, including the pass/fail criteria, baseline, duration, and number of times each test should be performed.
5) Specific test support requirements for each test performed.
6) Start and expected completion dates of each test to be performed.

d. Description of the data reduction and analysis techniques that will be used to interpret the data.
e. An overview of the procedures that will be used to validate the test results.

10.3.1 Class C2 products and their equivalent systems. The Security Test Plan shall include a plan for the search for obvious flaws that would:

a. Allow violation of resource isolation.
b. Permit unauthorized access to the audit or authentication data.

10.3.2 Class B1 products and their equivalent systems. The Security Test Plan shall describe the test program's approach to identify and report flaws so that the flaws may be removed or neutralized. It shall include the approach to retest identified flaws to demonstrate that they have been eliminated. This approach shall include regression testing to ascertain whether new flaws have been introduced when removing the originally discovered flaw.

10.3.3 Class B1 and above products and their equivalent systems. The following shall be included:

a. A description of how the design documentation, source code, and object code will be thoroughly analyzed and tested.
b. The plan for tests to:

1) Uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB.
2) Assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users.

10.3.4 Class B2 products and their equivalent systems. The following shall be included: regression testing to ascertain whether new flaws have been introduced when removing the originally discovered flaw.

DI-NDTI-81351

BLOCK 10. PREPARATION INSTRUCTIONS (Continued)

a. A description of the technique to demonstrate that the TCB is relatively resistant to penetration.

b. A description of the test program's approach to retest identified flaws to demonstrate that they have been corrected. This approach shall include the originally discovered flaw.

10.3.5 Class B2 and B3 products and their equivalent systems. The Security Test Plan shall describe the technique to demonstrate that the TCB implementation is consistent with the Descriptive Top Level Specification.

10.3.6 Class B3 and above products and their equivalent systems. The following shall be included:

a. A description of the technique that will be used to determine that the TCB is resistant to penetration.

b. A description of the approach that will be used to prevent design flaws and limit implementation flaws from being found during the final security testing. This approach shall provide a reasonable confidence that few flaws remain for security testing.

c. The Security Test Plan shall include the following test planning for trusted recovery:

1) Test conditions; i.e., a list of discontinuities of operation that can be generated through administrative interfaces and their effects.

2) Test data, consisting of the following:

a) Environment setup; e.g., the TCB and user-level data structures and objects needed to generate the planned discontinuity.

b) Parameters and commands used by the administrators to generate the discontinuity.

c) Expected outcome; e.g., the type of procedures that are started automatically or manually for handling the generated discontinuity and the effect of those procedures on the TCB state.

3) Coverage analysis; e.g., this includes a list of failures, or classes of failures, whose effect is covered by the generated discontinuities, and a list of spontaneous failures, or classes of failures, whose effect isn't covered by the test.

10.3.7 Class A1 products and their equivalent systems. The following shall be included:

a. A description of the technique to demonstrate that the TCB implementation is consistent with the Formal Top Level Specification (FTLS).

b. A description of how the mapping of the FTLS to the source code may form a basis for penetration testing.

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
TEST PROCEDURE	DI-NDTI-80603

3. DESCRIPTION/PURPOSE

3.1 The test procedure identifies the step-by-step testing operations to be performed on items under going developmental, qualification, or acceptance testing. It identifies 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

(Continued on Page 2)

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
880601	G/T2137		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) contains the format and content preparation instructions for the data product generated by the specific and discrete task requirements as delineated in the contract.

7.2 This DID is applicable to contracts requiring tests to be performed for the purpose of developmental or environmental evaluation, acceptance testing, and item qualification testing.

7.3 This DID supersedes DI-T-5248 and DI-T-5301.

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		G4428

10. PREPARATION INSTRUCTIONS

10.1 Format Requirements. The test procedure shall be in the contractor's format on 8 1/2 x 11 inch paper. It shall be bound in such a manner that pages may be removed or inserted without damage or mutilation.

10.2 Content requirements. The test procedure shall contain the following:

10.2.1 Front matter.

10.2.1.1 Cover and title page. The following information shall be included on the cover and title page:

a. Date of issue.
b. Revision date (if applicable).
c. Procedure document identification number.
d. Contract number.
e. Contractor's name and address.
f. Type of procedure, including purpose (e.g., first article test, developmental evaluation, qualification, environmental (specify), acceptance, or other).
g. Identification of the system, subsystem, or equipment to be tested.
h. Security classification (if applicable).

(Continued on page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: Approved for public release, distribution is unlimited.

DI-NDTI-80603

Block 3. DESCRIPTION/PURPOSE (Continued)

results will be measured. The document is a compilation of individual test procedures for related elements of a system, subsystem, or equipment.

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.2.1.2 Record of changes. A record of change pages shall be included to provide for tracking of changes to the test procedures.

10.2.1.3 Table of contents. A table of contents is required when more than one test procedure is included in the test procedures document. It shall identify the page location of each procedure number, procedure title, and related equipment nomenclature.

10.2.2 Body of document. For each test procedure, the following information is required:

10.2.2.1 Procedure number. Each procedure shall have a unique number assigned to it.

10.2.2.2 Title of procedure. The title should relate to the purpose of the test.

10.2.2.3 Introduction. The following shall be addressed in the introduction:

10.2.2.3.1 Purpose of test. (As specified in the contract tasking document.)

10.2.2..3.2 System, subsystem, or equipment to be tested. The following identification information shall be provided:

a. Nomenclature.
b. Model or part number.
c. Type of test item (prototype, production item, laboratory model, etc.)
d. Applicable specification.

10.2.2.3.3 Test requirements. Includes the following, each related to the prescribing contract requirement paragraph (specification, standard, plan, or work statement).

a. Required tests, and parameters to be measured.
b Performance requirements, acceptance or compliance limits. and environmental criteria.

10.2.2.3.4 Referenced documents. A list by title, number, date, and source of those documents cited in the test procedure.

DI-NDTI-80603

Block 10. PREPARATION INSTRUCTIONS (Continued)

10.2.2.4 Required test equipment. Includes the following for each piece of test equipment to perform the procedure:

a. Nomenclature.
b. Use of test equipment.
c. Model number (if applicable).
d. Manufacturer (if applicable).
e. Accuracy and calibration requirements.
f. Range of spectrum of measurements required.

10.2.2.5 Table of tests. This table lists each test performed under the procedure in the sequence it is to be performed, identified to the procedure paragraph and the related specification/contract requirement.

10.2.2.6 Step-by-step procedure. The following shall be included for each step of the test procedure:

a. Test set-up diagrams, including test equipment connections.
b. Input and output instrumentation points.
c. Test item operating limits and test conditions to be imposed.
d. Performance parameters to be measured.
e. Step-by-step operations to obtain the required data.
f. Caution and safety warnings as appropriate.

10.2.2.7 Data sheets. Data sheets shall be included with the procedure, or be separately attached at the end of all procedures. They shall provide for:

a. Identification of item tested, including model and serial numbers.
b. Recording of test measurements.
c. Identification of required or objective performance values, with tolerances.
d. Identification of applicable procedure paragraph.
e. Date of test.
f. Signature of technician or inspector performing the tests.

10.2.2.8 Support requirements. Any special support requirements would be included in this section, such as:

a. Use of special facilities or test ranges.
b. Personnel requirements (numbers, types, qualifications).
c. Unusual electrical, hydraulic, pneumatic, etc. requirements.
d. Support equipment requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

DATA ITEM DESCRIPTION

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. TITLE	2. IDENTIFICATION NUMBER
TEST/INSPECTION REPORTS	DI-NDTI-80809A

3. DESCRIPTION/PURPOSE

3.1 The test/inspection report is used to determine compliance with system requirements, performance objectives, specifications, or test/inspection plans; whether the test/inspections are conducted at contractor, government or independent facilities.

(Continued on page 2)

4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
910325	F/AFSC-TE		

7. APPLICATION/INTERRELATIONSHIP

7.1 This Data Item Description (DID) is a broad consolidation of a number of superseded DIDs that specifies a uniform content and format to be used in the preparation of test/inspection reports covering test/inspections on systems, subsystems, components, parts, materials, processes, and equipments as applicable.

(Continued on Page 2)

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
		F6040

10. PREPARATION INSTRUCTIONS

10.1 Format requirements. The test/inspection report format shall be contractor selected consistent with the following requirements:

10.1.1 Media. The test/inspection report shall be provided by electronic transmission or on either magnetic media or durable quality paper, and shall present the data in a clean and legible manner. The text and numeric data shall be capable of being typewritten or printed, using non-exotic typefaces, on 8 1/2 by 11 inch standard white paper. Photographs, pictorials, graphics and drawings shall be presented in high contrast black and white or color. If the media is paper, black ink should be used on white bond paper, and the report shall be bound such that pages may be removed or inserted without damage or mutilation. The media shall be in the Computer Aided logistics Support (CALS) format as specified in MIL-STD-1840.

10.1.2 Format. The test/inspection report format shall present the data in an effective and logically organized arrangement. The text shall be single spaced and shall use correct English grammar, spelling, capitalization, and punctuation. Numerical data shall use Arabic numerals and the units of

(Continued on Page 2)

11. DISTRIBUTION STATEMENT

Distribution Statement A: Approved for public release; distribution is unlimited.

Block 3. DESCRIPTION/PURPOSE (Continued)

3.2 The report should document test/inspection results, findings, and analyses that will enable government or contracting agency to evaluate and determine subsequent actions.

Block 7. APPLICATION/INTERRELATIONSHIP (Continued)

7.2 This DID contains the format and content preparation instructions for the data product generated by the specific and discrete task requirement as delineated in the contract.

7.3 This DID is applicable to contracts requiring tests/inspections to be performed for the purpose of developmental, operational, or environmental evaluation, acceptance or quality conformance inspection, an item qualification.

7.4 This DID should by tailored on the DD Form 1423 Contract Data Requirements List (CDRL) to the application program requirements, when requiring media prepared in the Computer Aided Logistics Support (CALS) format as specified in MIL-STD-1840A and its related specifications. This DID is applicable whenever success criteria and test/inspection methods have been prescribed (i.e., where there is a specification or comparable document). This Data Item Description is applicable to both flight and ground tests/inspections.

7.5 This DID is normally used for engineering test and evaluation, pre-qualification, qualification, and other developmental tests/inspections in the specifications as well as quick look, interim, and final summary reports of test/inspection results, and findings related to the completion of a program milestone period (such as the completion of demonstration/validation and the start of full scale development).

7.6 The requirements contained in the DID should be tailored consistent with the program phase and the contractual testing/inspection requirements.

7.7 This DID supersedes DID's DI-E-1150, DI-T-1780, DI-T-1787, DI-T-1906, DI-R-2057, DI-R-2063, DI-T-2072, DI-T-5329, DI-T-5426, DI-T-5439A, UDI-T-21332, UDI-T-23668, UDI-T-23790, DI-T-30720, DI-T-30736, DI-QCIC-80139, DI-QCIC-80140, DI-QCIC-80141, DI-NDTI-80604, DI-MISC-80654, DI-NDTI-80809, and DI-RELI-80939.

Block 10. PREPARATION INSTRUCTIONS (Continued)

measure shall be identified and defined. Acronyms, codes, abbreviations, signs, and symbols shall be defined. Photographic, pictorial, graphic, and tables, figures, footnotes, and illustration shall be identified and referenced in the text. Oversize pages shall be capable of being folded to the dimensions of the volume. Unless effective presentation would be degraded, the initial format arrangement shall be used for all subsequent submission.

10.1.3 Reproduction. The test/inspection report shall be capable of being photographically reproduced in black on white copy sufficiently clear and sharp for further reproduction. Ditto, hectograph, color or reproduction processes not reproducible photographically shall not be required for reproduction of the test/inspection report.

10.2 Content requirements. The test/inspection report shall contain the following information:

10.2.1 Cover and title page. The following information shall appear on the outside front cover and title page:

a. Report date.
b. Report number (contractors or government, if assigned).
c. Contract number/CLIN number or sequence number (if applicable).
d. contractors name and address, and commercial and government entity (CAGE) code.
e. Type of test/inspection (e.g., first article, quality conformance, developmental evaluation, qualification, environmental (specify); acceptance,,or other).
f. Identification (e.g., national stock number (NSN), nomenclature, model/part/serial number) of item tested/inspected.
g. Name and address of test/inspection facility.
h. Date or period of test/inspection.
i. Name and address of requiring government activity.
j. Security classification, downgrading and declassifying information (if applicable).

10.2.2 Table of contents. The table of contents shall identify the following:

a. The title and starting page of each major section, paragraph, and appendix of the report.
b. The page, identifying number, and title of each illustration (e.g., figure, table photograph, chart, and drawing).

10.2.3 Introduction. The introduction shall include the following information:

10.2.3.1 Purpose of the test/inspection. The specific purpose of the test/inspection as specified in the contract tasking document if the contract does not identify a specific test/inspection purpose, the contractors purpose shall be stated.

10.2.3.2 Item tested/inspected. Complete identification of the item tested/inspected including the following:

a. Nomenclature.
b. National stock number (NSN).
c. Model/part/serial number.
d. Type of item (e.g., prototype, production item, laboratory model).
e. Serial or lot number.
f. Applicable engineering changes.
g. Production item specification (if applicable).
h. Date of manufacture.

10.2.3.3. Test/inspection requirements. Complete identification of the test/inspection requirements correlated to contractual requirements and the requirements documentation, including the following:

a. Required test/inspection parameters measured.
b. Performance requirements, acceptance or compliance limits, and environmental criteria.

10.2.4 Summary. Complete test/inspection report summary including the following:

a. A brief discussion of the significant test/inspection results, observations, conclusions, and recommendations covered in greater detail elsewhere in the report.
b. Proposed corrective actions and schedules for failures or problems encountered.
c. Identification of deviations, departures, or limitations encountered, referenced to the contract requirements.
d. Tables, graphs, illustrations, or charts as appropriate to simplify the summary data.

10.2.5 Reference documents. Complete identification of all documents referenced in the test/inspection report including the following (as applicable):

a. Prior test/inspection reports on the same item.
b. Test/inspection plan and procedure documents.
c. Requirements specifications and standards.
d. Prior certifications of compliance.
e. Contractors file designation where test/inspection records are maintained.
f. Input parameter used.

The applicable issue of the documents cited therein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as specified in the contract.

10.2.6 Body of report. The body of the test/inspection report shall be as follows:

10.2.6.1 Test equipment identification. Complete identification for each item of test equipment used in the test/inspection including the following:

a. Nomenclature.
b. Model number.
c. Serial number.
d. Manufacturer.
e. Calibration status.
f. Accuracy data.
g. Comments (if applicable).

10.2.6.2 Test/inspection facility installation and setup. Drawing, illustrations, and photographs may be used for clarification. Complete description of the physical setup (e.g., item, test/inspection facility, and equipment used in conducting the test/inspection) to include the following:

a. Location/orientation of item.
b. Location/orientation/settings of test equipment and instrumentation.
c. Location/orientation/settings of sensors and probes.
d. Location/orientation of interconnections, cables, and hookups.
e. Electrical power, pneumatic, fluidics, and hydraulic requirements.

10.2.6.3 Test/inspection procedures. Complete description of the procedures used in conducting the test/inspection to include the following:

a. Item selection and inspection that verified suitability for test/inspection.
b. Summarized sequence of testing/inspection steps, including a description of how the item was operated during the test/inspection, and any control conditions imposed.
c. Data reduction techniques employed.

10.2.6.4 Test/inspection results and analysis. A copy of all test/inspection results and analysis to include the following:

10.2.6.4.1 Recorded data. The actual recorded date (e.g., log book entries, oscillographs, instrument readings, and plotter graphs). If the recorded data is extensive, provide it in an appendix.

10.2.6.4.2 Test/inspection results. Identification of all test/inspection results to include the following:

a. Matrices comparing results achieved against test/inspection objectives or requirements.
b. A discussion of these matrices as to their significance, and how they compare to any prior test/inspection.
c. Calculation examples.
d. Tabulation of the recorded date (reference 10.2.6.4.1) reduced the related test/inspection procedure generating the data and test requirements.
e. Discussion of anomalies, deviations, discrepancies or failures, including their impact, causes and proposed correctable actions. The discussion shall address discrepancies between design requirements and the test/inspection configuration.

10.2.6.5 Conclusions. Test/inspection conclusions distinguish between objective and subjective to include the following:

a. The effectiveness of the test/inspection procedures in measuring item performance.
b. The success or failure of the item to meet required test/inspection objectives.
c. The need for repeat, additional, or alternative testing/inspection.
d. The need for item redesign or further development.
e. The need for improved test/inspection procedures, techniques, or facilities.
f. The adequacy and completeness of the test/inspection requirements.

10.2.6.6 Recommendations. Recommendations appropriate to the test/inspection results and conclusions including the following:

a. Acceptability of the item tested/inspected (pass or fail).
b. Additional testing/inspection required.
c. Redesign required.
d. Problem resolution.
e. Test/inspection procedure or facility improvements.
f. Disposition of items tested/inspected.
g. Documentation changes required.
h. Testing/inspecting improvements.

10.2.7 Authentication. The following certifications shall be included, as applicable:

10.2.7.1 Authentication of test/inspection results. A statement that the test/inspection was performed in accordance with applicable specifications, test/inspection plans, and procedures, and that the results are true and accurate. The authentication shall include the signature of the contractor personnel that performed the test(s)/inspection(s). Any government witnesses, and a contractor representative authorized to make such certification.

10.2.7.2 Authentication of prior validation. A statement identifying those requirements not tested/inspected or measured that were previously validated. Include identification of the date and method employed for such validation (e.g., prior test/inspection, analytical verification, equivalent item, etc.). The authorization shall include the signature of a contractor representative authorized to make such authentication and any government witness.

10.2.7.3 Authentication of acceptability. A statement that the item tested/inspected either passed or failed item acceptability requirements as delineated in applicable specifications. This authentication shall include the signature of a contractor representative authorized to make such authentication and any government witness.

10.2.8 Appendices. Appendices shall be used to append detailed test/inspection data, drawings, photographs, or other documentation too voluminous to include in the main body of the report. This includes referenced documentation not previously provided by the Government, and test/inspection reports from any associated test/inspection activity that may have performed some of the testing/inspecting requirements.

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

THIS PAGE INTENTIONALLY LEFT BLANK

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.

THIS PAGE INTENTIONALLY LEFT BLANK

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

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highways, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

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

4. TITLE AND SUBTITLE
A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Security Agency
Attention: I94; Standards, Criteria, and Guidelines Division
9800 Savage Road
Fort George G. Meade, MD 20755-6000

8. PERFORMING ORGANIZATION REPORT NUMBER
NCSC-TG-024, Volume 3/4, Version 1

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

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
Library No., S-239.689

11. SUPPLEMENTARY NOTES

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

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial, Volume 3 of 4 in the Procurement Guideline Series, is written to be used by Federal Agencies to help facilitate the definition of computer security deliverables required in the acquisition of trusted products 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. The emphasis of this guideline is on the data requirements for products. 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).

14. SUBJECT TERMS	15. NUMBER OF PAGES
National Computer Security Center, Acquisition, Computer Security Requirements, Contract Data Requirements List, Data Item Description and Computer Security Tutorial.	160
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None