DATA ITEM DESCRIPTION
Title: THEORY OF COMPLIANCE (TOC)

Number: DI-MISC-81609 **Approval Date: 9 May 01**
AMSC Number: G7439 **Limitation:**
DTIC Applicable: **GIDEP Applicable:**
Office of Primary Responsibility: G-C12
Applicable Forms:
Use/relationship: The Theory of Compliance describes detailed design and implementation information about system security critical functions. It is used to support NSA evaluations to ensure that system security requirements are met.

a. 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.

b. This DID is applicable to information assurance (IA) systems[1].

c. This DID is related to DI-MISC-81608, Theory of Design & Operation.

d. This DID is related to the system security requirements supplied with the contract.

e. This DID supersedes DI-ADMN-81599, Theory of Compliance.

Requirements:

1. Format. The Theory of Compliance shall be in the contractor's format with the following exceptions:

1.1 Page size. The size of each finished page shall be on 8 1/2" X 11" paper (metric size A4). Fold-outs shall be kept to a minimum; when used they shall not exceed the 8 1/2" x 11" limits when folded. Photo reduction of oversized pages is preferred, provided such reductions are easily readable and reproducible.

1.2 Binding. The Theory of Compliance shall be bound in such a manner that pages can be removed without damage or mutilation.

1.3 Paragraph identification. Each paragraph shall have a unique contractor specified paragraph identifier.

2. Content. The report shall contain front matter as follows:

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

a. Report Title.

b. Date of Issue.

c. Report number/revision number or letter.

d. Contract number.

e. Contractor name and address.

f. Program title, including program name.

[1] Throughout this DID, system is meant in a generic sense to apply to any functionally related group of elements composing the targeted design and its implementation. As examples, that group of elements may form a component, as is the case for a hardware or software embeddable cryptomodule; or it may form an equipment, as is the case for a secure radio; or it may form a hybrid of various equipment and interconnections, as is the case for a worldwide communications network.

g. Security classification, if classified.

h. Distribution statement.

2.2 Revision control page. The revision control page shall list the following information:

a. Each revision number or letter.

b. Date of each revision.

c. Pages affected by each revision.

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

a. The title of and starting page of each major section and paragraph of the report.

b. The page, identifying number, and title of each drawing, illustration, figure and table.

2.4 Chapters. The report shall contain the following chapters of information:

2.4.1 General Information

The Theory of Compliance (TOC) is a report providing detailed design and implementation information about system security critical functions. It describes the actual implementation of each security critical function and identifies how each security requirement and goal is satisfied by specific design details. The TOC is divided into two chapters. It answers two basic questions about the system design: 1) How have security critical functions been implemented? (Chapter 1), and 2) How are individual security requirements and goals satisfied? (Chapter 2)

The TOC is intended to answer the “how” questions associated with a critical design. The report describes each design feature in enough detail to enable a reader to make decisions about the adequacy of the implementation in satisfying the security critical requirements and goals of the system. The general approach and identification of security critical functions have been previously addressed in an associated document, the “Theory of Design and Operation” (TDO). The TOC is written so that a reader is able to trace the implementation of security critical functions described in this report to the TDO document.

Charts and diagrams are included in this report for clarity to support the written description.

2.4.2 Chapter 1. Implementation Description of Security Critical Functions.

The first chapter of the TOC provides a detailed description of each of the system security critical functions and how they have been implemented. This description provides very specific design and implementation information, including information on all off-the-shelf and custom hardware and software depended upon by the system. The following list gives an idea of the type of supportive information and level of detail contained in this chapter. The list is not intended to be exhaustive or to be applicable to each function. It is to be used as an example only.

a. Commands and Messages (e.g., verbal descriptions, protocols/syntax & formats, parameters & parameter definitions, state transitions, checks, error conditions, responses).

b. Bit rates.

c. Memory (e.g., types, usage, mapping, handling -- allocation/deallocation, separation & access).

d. Communication protocols.

e. Timing characteristics.

f. Detailed descriptions of alarm conditions and responses.

g. Detailed descriptions of check functions.

If a government-approved product (either a GOTS or COTS product) is embedded in the system being designed, the TOC provides a detailed description of how the security features of that approved implementation are utilized in the system, including the specific configurations and modes of operation used.

If the system includes the actual implementation of a cryptographic algorithm, the functional description of the algorithm is limited to a detailed block diagram showing all logical operations and timing delays. The purpose of the diagram is to ensure that the contractor correctly understands the function of the algorithm. The necessary alarms, checks, and other security critical functions associated with the algorithm implementation are described in their appropriate functional block description.

Where several functions have identical descriptions, a single written description is included with the first reference to that function. In subsequent references, the original description may be referenced by supplying the appropriate paragraph numbers. Care is taken to identify any name changes, or minor variations to the original description to ensure the reader can follow the flow of a security critical function without misinterpretation.

2.4.3 Chapter 2. Security Requirements Compliance.

The second chapter of the TOC provides a detailed description of how each system security requirement and goal is being satisfied. The level of detail for this chapter is the same as for Chapter 1. This description addresses the interrelationship among the various elements of the system, including all off-the-shelf and custom components (hardware or software), and how they work together to satisfy each requirement.

Each requirement and goal in the system security requirements is addressed separately. If the requirement or goal applies to more than one area of the design, the design approach for each area is addressed separately. Where an adequate description of the design satisfying a requirement or goal has already been provided, that description may be referenced by supplying the appropriate paragraph numbers. Care is taken to identify any name changes, or minor variations to the original description to ensure the reader can follow the design implementation without misinterpretation.

If a government-approved product (either a GOTS or COTS product) is embedded in the design, and that product is being use to satisfy system security requirements, a detailed description of how the host system utilizes and preserves the integrity of the security features of the embedded product is included in this chapter of the TOC. This includes a detailed description of any interfaces and how the host handles critical information passed to and from the embedded product.

3. End of DI-MISC-81609