DATA ITEM DESCRIPTION

Title: Theory of Compliance (TOC)

Number: DI-ADMN-81599
Approval Date: 5 February 2001
AMSC Number: G7418
Limitation: N/A
DTIC Applicable: N/A
GIDEP Applicable: No

Office of Primary Responsibility: G-X31

Applicable Forms: None

Use/relationship:

The TOC shall provide detailed design information about system security-critical functions. The TOC shall describe the actual implementation of each security-critical function and identify how each system security requirement is satisfied by specific system design details The TOC shall answer two basic questions about the system design: 1) How have security-critical functions been implemented? and 2) How is each individual security requirement satisfied?

Requirements:

1. General. The TOC shall answer the how questions associated with the system critical design. The TOC shall describe each system design feature in enough detail to allow a reader to make decisions about the adequacy of the implementation in satisfying the system security requirements. The general approach and identification of security-critical functions shall have been previously documented in the TEO. The TOC shall be written so that a reader can trace the implementation of system security-critical functions described in the TOC back to the TEO.

2. Format. The TOC shall be in the contractors format unless specified otherwise in the SOW.

3. Page Size. The size of each finished page shall be on 8 1/2 x 11 paper (metric size A4). Drawing and illustration 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.

4. Binding. The TOC shall be bound in such a manner that pages can be removed without damage or mutilation.

5. Changes and Revisions. Changes and revisions to the TOC shall be made in accordance with the requirements of MIL-STD-961D (1).

6. Paragraph Numbering. TOC paragraphs shall be numbered in accordance with the requirements of MIL-STD-961D.

7. Paragraph Identification. TOC paragraphs shall be identified in accordance with the requirements of MIL-STD-961D.

8. Cover and Title Page. The TOC shall contain the following on its cover and title page: report title; date of issue; report number/revision number or letter; contract number; contractor name and address; program title, including program name; security classification, if classified; and distribution statement(s), as applicable.

9. Table of Contents. The TOC shall contain a table of contents which includes the following: the title and starting page of each major section and paragraph of the TOC; and the page, identifying number, and title of each drawing, illustration, figure, and table.

10. Chapters. The TOC shall be divided into two chapters. The first chapter shall describe in detail how each system security-critical function shall be implemented. The second chapter shall describe how each system security requirement shall be satisfied. Liberal use of diagrams and charts to support the written description is encouraged throughout the TOC.

10.1 Chapter 1 - Implementation of Security-critical Functions. The first chapter of the TOC shall provide a detailed description of each system security-critical function and how it has been implemented in the system detailed design. This description shall provide very specific design information. The following list gives an idea of the depth of information required in this chapter; the list is not intended to be exhaustive or to be applicable to each function, but is to be used only as an example: commands and messages; message package description; bit rates; memory: types, usage, mapping, handling (allocation / de-allocation, separation and access); communication protocols; timing characteristics; detailed descriptions of alarm conditions and responses; and detailed descriptions of check functions. If a Government-approved product is to be embedded in the system, the TOC shall include a detailed description of how the security features of that product are to be used. If the system is to include an actual implementation of a cryptographic algorithm, the TOC shall include a description of the algorithm which is limited to a detailed block diagram showing all logical operations and timing delays. The purpose of the diagram is to demonstrate that the contractor correctly understands the function of the algorithm. The TOC shall include separate descriptions of the necessary alarms, checks, and other security-critical functions associated with the algorithm implementation. Where several security-critical functions have identical descriptions, the TOC may include a single, written description with subsequent references to that description. Care shall be taken to identify any name changes or minor variations to the original description to assure that a reader of the TOC can follow the flow of a security-critical function without the need for interpretation.

10.2 Chapter 2 - Security Requirement Compliance. The second chapter of the TOC shall describe in detail how each security requirement and goal, if specified, is satisfied by the system. The level of detail for this chapter shall be the same as for chapter one. Each requirement in the security requirements shall be addressed separately. When an adequate description of the design satisfying a requirement has already been provided in the TOC, that description may be referenced in subsequent TOC paragraphs instead of repeating the description. Care shall be taken to identify any name changes or minor variations to the original description to assure that a reader of the TOC can follow the design implementation without the need for interpretation. If a Government-approved product is to be embedded in the system and that product is to be used to satisfy system security requirements, the TOC shall describe in detail how the system uses and preserves the security integrity of the embedded product. This description shall include detailed discussions of each interface with the embedded product and how the system handles critical information passed to and/or received from the embedded product.

10.3 Justification for Tailoring of Requirements. If, during the detailed design phase of the system development contract, the contractor believes that a requirement stated in the system security requirements is not applicable to the emerging system detailed design, the TOC shall include, in lieu of a detailed design description which addresses the requirement, a justification of why the requirement is not applicable. The purpose of this is to provide a mechanism to tailor security requirements to the system design. If the Government agrees with the justification, the requirement need not be satisfied. However if the Government disagrees with the justification, the contractor shall revise the TOC to provide a description of a design which satisfies the requirement.

11. End of DI-ADMN-81599