DATA ITEM DESCRIPTION

Title: Security Evaluation Document (SED)

Number: DI-MISC-81762
AMSC Number: 9056
DTIC Applicable: No
Office of Primary Responsibility: NS/I7
Applicable Forms: N/A

Approval Date: 02 February 2009
Limitation: N/A
GIDEP Applicable: No

Use/Relationship: The purpose of the Security Evaluation Document (SED) is to provide information about the architectural design of an Information Assurance (IA) product and its intended detailed implementation throughout the development/design of the product. Sufficient detail is provided to determine adequacy of the design and ensure that appropriate system security requirements are met, while performing failsafe analysis of unauthorized events upon a system as well as analysis of covert channels and anti-tamper design. The SED is used to support security evaluations, and is a combination of previously used evaluation documentation that included Covert Channel Analysis Report (CCA), Theory of Design and Operation (TDO), Theory of Compliance (TOC), and Fail-Safe Design and Analysis (FSDA).

This Data Item Description (DID) is applicable to IA systems and is related to the system security requirements supplied with the contract that references US Information Security (INFOSEC) Systems C Technical Report 02-00, and the Unified INFOSEC Criteria or the Information Assurance Security Requirements Directive (IASRD).

This 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.

This DID consolidates and supersedes the following documents:

- DI-MISC-81345A, Covert Channel Analysis Report
- DI-MISC-81608, Theory of Design and Operation (TDO)
- DI-MISC-81609, Theory of Compliance (TOC)
- DI-MISC-81692, Fail-Safe Design and Analysis (FSDA)

Requirements:

1. Reference Documents: The applicable issue of the documents cited herein, including their approval dates and dates of any applicable amendments, notices, and revisions, shall be as stated herein. The following documents are available at: Director, National Security Agency, 9800 Savage Road, Fort George G. Meade. MD 20755, Attn: I7.

- Information Assurance Security Requirements Directive (IASRD), current edition, and Unified INFOSEC Criteria (UIC), current edition.
- Fail-Safe Design and Analysis (FSDA) for US INFOSEC Systems, C Technical Report 02-00, the current edition, Library No. S-247, 160.

2. Format. The SED shall be in the contractor's format with the following exceptions:

2.1. Page size. The size of each finished page shall be on 8 1/2" x 11" paper (metric size A4). Foldouts shall be kept to a minimum; when used, foldouts 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.

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

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

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

3. Content. The report shall contain:

3.1. 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.

g. Security classification, if classified.

h. Distribution statement.

3.2. Revision control page. This page shall facilitate tracking of changes between revisions for timeliness and ease of review. Each revision of the SED must include Change Bars to highlight changes from the previous submission. In addition, comments shall be appended to the SED (Appendix B), along with the appropriate response and changes. These responses shall reference

corresponding locations in the body of the document. 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.

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

a. The title of the 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.

3.4. Chapters. The report shall contain the following chapters of information. It is important to note that the chapters would not be necessarily filled out in sequential order, but filled in as information is available and required.

3.4.1. General Information.

The SED is a report providing a view of the architectural design of an information assurance system and analysis of fail-safe mechanisms. At a high level it describes the functional and physical design of the system, interrelationships, and security requirements and goals to be met by the system. On a detailed level it provides detailed design and implementation information about system security critical functions, how they are implemented and how individual security requirements are satisfied. Diagrams and charts are included in the SED for clarity and to support the written description.

3.4.2. Chapter 1. System Requirements and Operational Environment

This chapter provides a concise description of the top-level requirements and goals of the system design to include the customer, purpose, environment, component-level procurement strategy, production quantity, and functionality/interoperability, as well as identifying all critical information (both at rest and in transit) and technology (if applicable) of the system to be protected, a description of the operational environment and constraints (e.g. airborne, command post, access by cleared personnel only), and a statement of the top-level system security requirements and goals.

3.4.3. Chapter 2. Functional and Physical Architecture

This chapter provides a functional and physical description of the system being designed, giving the reader an explanation of the hierarchy of functions within the system and how this functional architecture satisfies the top-level requirements identified in Chapter 1. The description logically flows from the system's top-level functions, down through several layers of functional partitioning, to a functional design level where each function represents an individual task that is

identified as occurring within or by a specific physical element of the system. The description provides the reader with an explanation of the functional and physical elements of the system (i.e. hardware, QUADRANT approach, software, databases, communication paths, etc.) and their relationships to each other (e.g. Master/Slave, sub-element, etc.). The description associates the functions identified in this Chapter to specific elements, explaining the interdependencies among the elements in achieving functionality and providing a functional-to-physical system decomposition as detailed in Step Six of the Fail-Safe Design and Analysis (FSDA) for US INFOSEC Systems, referenced above.

3.4.4. Chapter 3. Security Architecture

3.4.4.1. This chapter discusses the security requirements identified for the system and the adequacy of the proposed design approach. Each of the system security requirements is addressed separately and the design approach proposed for satisfying that requirement is described. This description provides system specific detail on how the design (built with custom or off-the-shelf components) and configuration satisfies the security requirement. The description is not just a restatement of the requirement. It describes how various elements of the system work together to carry out a security requirement, and what each element relies on from the others to do so. If that security requirement applies to more than one area of the design, the design approach for each area is addressed separately. If a stated security design requirement does not apply or is partially applicable to the proposed implementation, it shall be stated and justified as to why. If agreed to by the customer, program manager, and evaluator, it can be removed or modified as a security requirement to be addressed in this development, and can be marked as not applicable or partially applicable in the Security Design Requirements Matrix (Appendix A). If a security requirement applies, but is not able to be met by the chosen implementation, it shall be explained why, and if agreed to by the customer, program manager, and evaluator, will remain identified in the documentation and noted as a “push-up” requirement, and will be marked as not met in Appendix A with a brief explanation. 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.

3.4.4.2. If a government-approved product (either a Government Off The Shelf (GOTS) or Commercial Off The Shelf (COTS) product) is embedded in the design, provide a detailed description of how the security features of that approved product are utilized in the system, including specific configurations, implementations, and modes of operation used. If the embedment is being used 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. This includes a detailed description of any interfaces and how the host handles critical information passed to and from the embedded product.

3.4.4.3. 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, timing delays and mode of operation. 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.

3.4.4.4. 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.

3.4.5. Chapter 4. Fail-Safe Design Analysis

3.4.5.1. This chapter deals with the last three steps of Fail-Safe Design Analysis that address:

a. Unauthorized Events Analysis (Step 7).

b. Multi-Level Data Separation and Physical Pin-to-Pin Analysis (Step 8).

c. Failure Summary (Step 9).

3.4.5.2. Detailed information related to the content of Steps 7 - 9 specified above is provided in the Fail-Safe Design and Analysis (FSDA) for US INFOSEC Systems, referenced above.

3.4.6. Chapter 5. QUADRANT Report

This chapter deals with the physical anti-tamper features within IA products and is applicable to all contracts which require QUADRANT as specified by the Information Assurance Security Requirements Directive (IASRD) or Unified INFOSEC Criteria (UIC). Each QUADRANT-related requirement within the IASRD or UIC shall be addressed and include narrative within Appendix A, mechanical drawings, and electrical schematics to properly explain and illustrate how each requirement is satisfied. If a particular requirement is not implemented, the associated narrative shall detail why, including rationale, security policy, and any other considerations.

3.4.7. Chapter 6. Final Covert Channel Analysis Report

3.4.7.1. This chapter includes a documented description of the covert channel analysis. A covert channel is a method of communicating through or within a system in violation of the information flow policy using paths that are not intended to carry data. Covert channels only exist in the context of systems that require information flow policies to be enforced. Covert channels are characterized as either storage or timing channels as defined below. The covert channel analysis shall address both types of channels.

3.4.7.2. A storage channel is a covert channel that directly or indirectly writes to a storage location in order to pass information. The storage location may correspond to data at rest, such as a file on disk. Example of this would include using steganography to encode a message in the low order bits of an image or modulating the size of a text file. Alternatively a storage channel may write to storage locations corresponding to data in transit, e.g., using protocol header fields (which may bypass filtering or encryption) with non-fixed values to convey information through a network encryptor or a firewall.

3.4.7.3. In contrast, a timing channel is a covert channel where time is the shared resource. In timing channels, processes modulating their own access to a common resource, e.g., a microprocessor, convey information. While one process has access, the other process measures the length of time it must block before it is granted the resource. During a given time slice, the sender may hold access to signal a one or release access immediately to signal a zero.

a. A description of the covert channel protection policy shall be provided that mitigates violations to the information flow requirements. The policy shall document how the assurance required for the system is commensurate with the sensitivity of the information protected and risks associated with the technology and operating environment.

b. The covert channel protection policy shall specify the level of covert channel analysis (CCA), i.e., informal, systematic/formal, or exhaustive, required for the target system.

c. For a systematic CCA, the analysis shall describe how it is structured and repeatable.

d. For an exhaustive CCA the analysis shall describe how it is structured, repeatable, and exercises all possible methods for determining the existence of covert channels.

e. The covert channel protection policy shall specify whether covert channels are to be documented, limited (in terms of capacity), monitored, or eliminated. For a particular system, multiple mitigations may be specified, and the distinction shall be based on the characteristics of an individual channel.

f. The CCA shall document the analysis of each information flow policy specified in the system security policy in terms of a potential covert channel.

g. The CCA shall document the analysis of both the design and implementation of the target system for potential covert channels. Low-level implementation details, including external

interface definitions and source code or hardware logic specification shall be used as inputs to the analysis.

h. The CCA shall document the analysis of all bypass policies for potential creation of covert channels.

i. The CCA shall identify each covert channel and describe a worst-case exploitation scenario for the channel.

j. The CCA shall identify the characteristics of each channel, including but not limited to:

- categorization (storage or timing)
- capacity estimate (including the method used for estimation)
- direction (ingress, egress, bidirectional)
- encoding (direct or indirect)
- reliability (noisy or noiseless)

k. The CCA shall describe all assumptions made during the analysis and provide evidence that the level of analysis and mitigation complies with the specified policy. An example of such an assumption would be the relative physical or logical location of the processes participating in the covert communication. For example, for an inline network encryptor, the processes could be hosts residing on the plaintext and ciphertext networks. Alternatively, a covert channel could require malicious code to be executing in the network processors themselves.

3.4.8. Appendix A. Security Design Requirements

Appendix A of the SED contains the system security requirements, and provides a detailed description of how each system security requirement is being satisfied. 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 in the system security requirements is addressed separately. If the requirement applies to more than one area of the design, the design approach for each area is addressed separately. Where a more detailed description of the design satisfying a requirement has been provided elsewhere in the SED, that description may also be referenced by supplying the appropriate paragraph numbers along with the description which is detailed in Appendix A. 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.

3.4.9. Appendix B. Comment and Response Matrix

Appendix B of the SED tracks comments along with the appropriate response and changes. These responses shall reference corresponding locations in the body of the document, which are also marked by Change Bars. These comments and responses stay with the SED with each revision.

3.5. Submissions.

The submission of the SED chapters shall support timely evaluation of hardware, software and test documentation coinciding with program development milestones. Further submission guidance is defined on form 1423 of the CDRL.

4. END of DI-MISC-81762