MILITARY STANDARD

SYSTEM SECURITY ENGINEERING

PROGRAM MANAGEMENT REQUIREMENTS

AMSC NO. F4729

AREA-MISC

DEPARTMENT OF DEFENSE

WASHINGTON DC 20301

System Security Engineering (SSE) Management Program Requirements
MIL-STD-1785.

1. This military standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may improve this document is addressed to: Headquarters Air Force Systems Command, Office of the Chief of Security Police, Andrews AFB, Washington, DC 20334. Use the self addressed standardized Document Improvement Proposal (DD Form 1426) at the end of this document or send comments by letter.

FOREWORD

The primary objective of the System Security Engineering Management program is to minimize or contain defense system vulnerabilities to known or postulated security threats. Scientific and engineering principles are applied during design and development to identify and reduce these vulnerabilities. Management techniques include life cycle considerations to ensure identified threats and vulnerabilities are contained. The basic premise of SSE philosophy is recognition that an initial investment in "engineering-out" security vulnerabilities and "designing-in" countermeasures is a long term cost saving measure. SSE is integrated with the system acquisition planning process to identify life cycle security threats and vulnerabilities, and concentrate on defense system susceptibility to damage, compromise or destruction.

CONTENTS

CONTENTS (cont'd)

CONTENTS (cont'd)

1. SCOPE

1.1 Purpose. This standard establishes the formats, contents and procedures for a contract SSE Management Program. The purpose of the System Security Engineering Management Program is to establish definitive guidance in the initial acquisition or modification of new or existing systems, equipment, and facilities to analyze security design and engineering vulnerabilities; and develop recommendations for engineering changes to eliminate or mitigate vulnerabilities consistent with other design and operational considerations. SSE supports the development of programs and standards to provide life cycle security for critical defense resources.

1.2 Applicability. Tasks described here are selectively applied in DOD contract specifications, request for proposals, statements of work and Government in-house efforts requiring a system security engineering management program. The word "contractors" include Government activities developing military systems, equipment and facilities. This standard may also apply to initial design of new facilities or modifications to existing ones.

1.2.1 Tailoring Task Descriptions. Task descriptions are tailored as needed and applied to system security engineering management programs. When preparing a proposal the contractor may include additional tasks and modify these tasks as long as supporting rationale is provided.

1.2.2 Application Guidance. Government and industrial organizations responsible for system security engineering management programs must select tasks which can materially aid in attaining overall security objectives in a cost effective manner. Once tasks have been selected, they may be tailored. Further, the timing and depth required during the various acquisition phases are often driven by interface with other ongoing program activities. For these reasons, specific rules are not defined for all task requirements.

2. REFERENCE DOCUMENTS

2.1 Government Documents.

2.1.1 Specifications, Standards and Handbooks. Unless otherwise indicated, specifications, standards, and handbooks listed in the Department of Defense Index of Specification and Standards (DODISS) for solicitations form a part of this standard to the extent cited below.

STANDARDS:

MILITARY

MIL-STD-470	Maintainability Program for System and Equipment
MIL-STD-490	Specification Practice
MIL-STD-499	Engineering Management
MIL-STD-785	Reliability Program for System and Equipment Development and Production
MIL-STD-1388-1	Logistics Support Analysis

2.2 Order of Precedence. In the event of conflict between the text of this standard and the references, the text of this standard takes precedence.

2.3 Source of Documents. Copies of military standards, specifications and associated documents listed in the Department of Defense Index of Specifications and Standards are available from the Department of Defense Single Stock Point, Commanding Officer,Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120. Copies of industry association documents are obtained from the sponsoring industry association. Copies of all listed documents are obtained from the contracting activity or as directed by the contracting officer.

3. DEFINITIONS

3.1 Acquisition Program. A directed effort funded through procurement appropriations; the security assistance program; or through research, development, test and evaluation (RDT&E) appropriations. This program may include development or modifications to existing systems.

3.2 Adversary Scenario. A composite of adversary mission objectives, adversary mission scenarios, and success criteria which could threaten each potential design of an operational or support system.

3.3 Adversary Model. A set of tactics that a potential adversary could use to accomplish a mission objective.

3.4 Carve-Out. A classified contract issued in connection with an approved Special Access Program in which the Defense Investigative Service has been relieved of inspection responsibility in whole or part under the Defense Industrial Security Program.

3.5 Configuration Item (CI). An aggregation of hardware/software, or any of its discrete portions, which satisfies an enduse function and is designated by the Government for configuration management. CIs may vary widely in complexity, size and type, from an aircraft, electronic or ship system to a test meteor round of ammunition. During development and initial production, CIs are only those specification items that are referenced directly in a contract (or an equivalent in-house agreement). During the operation and maintenance period, any repairable item designated for separate procurement is a configuration item.

3.6 Cost Trade-Offs. The trade-offs among non-recurring and recurring cost accrued in system acquisition and the operational life cycle.

3.7 Countermeasure. A design or procedural measure taken in defense against a security threat or vulnerability.

3.8 Electronic Security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and study of friendly non-communications electromagnetic radiations.

3.9 Facilities. Buildings, structures, or other real property improvements separately identified on the real property records and including items of real property. Facilities are categorized as technical support real property, critical subsystems, non-technical support real property (NSRP), and industrial facilities.

3.10 Integrated Logistics Support (ILS). A composite of all the supported considerations necessary to make sure a system is effectively and economically supported for its life cycle. An integral part of all other aspects of system acquisition and operations.

3.11 Life Cycle Cost (LCC). Includes all cost categories, both contract and in-house, and all related appropriations. It is the total cost to the government for a system over its full life, and includes the cost of development, procurement, operating, support, and, where applicable, disposal.

3.12 Logistic Support Analysis (LSA). LSA is a system engineering and design process selectively applied during all life cycle phases of the system/equipment to help ensure supportability objectives are met.

3.13 Maintainability. A measure of the time or maintenance resources needed to keep an item operating or to restore it to operational status (or serviceable status). Maintainability may be expressed as the time to do maintenance (for example, maintenance downtime per sortie), as a usage rate (for example, maintenance work hours per flying hour), as the staff required (for example, maintenance personnel per operational unit), or as the time to restore a system to operational status (for example, mean down time).

3.14 Maintenance Concept. A description of maintenance considerations and constraints. The operating command, with the help of the implementing and supporting commands, develops a preliminary maintenance concept and submits it as part of the preliminary system operational concept for each alternate solution. The preliminary maintenance concept is refined during the validation phase and becomes the system maintenance concept during full-scale engineering development. Then the maintenance concept is expanded in scope and detail and becomes the maintenance plan.

3.15 Operational Test and Evaluation (OT&E). Test and evaluation, initial operational test and evaluation, and follow-on OT&E conducted in as realistic an operational environment as possible to estimate the prospective system military utility, operational effectiveness, and operational suitability. In addition, OT&E provides information on organization, personnel requirements, doctrine, and tactics. Also, it may provide data to support or verify material in operating instructions, publications, and handbooks.

3.16 Security Criteria. The set of requirements that should be met so the security system can provide a maximum degree of effective deterrence at the lowest cost which satisfies the system specifications.

3.17 Security Subsystem. That part of a weapon or defense system which is added specifically for the performance of security functions and not categorized as components of other subsystems.

3.18 Security System. The aggregate of all mechanical and electronic equipment countermeasures and associated software in a system which contributes to its security.

3.19 Subsystem. An element of a system that, in itself, may constitute a system.

3.20 System. A composite, at any level of complexity, of personnel, procedures materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement.

3.21 System Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities. It uses mathematical, physical, and related scientific disciplines, and the principles and methods of engineering design and analysis to specify, predict, and evaluate the vulnerability of the system to security threats.

3.22 System Security Engineering Management. An element of program management that ensures system security tasks are completed. These tasks include developing security requirements and objectives; planning, organizing, identifying, and controlling the efforts that help achieve maximum security and survivability of the system during its life cycle; and interfacing with other program elements to make sure security functions are effectively integrated into the total system engineering effort.

3.23 System Security Management Plan (SSMP). A formal document that fully describes the planned security tasks required to meet system security requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering, design and management activities, and related systems.

3.24 Technology Trade-Offs. Trade-offs among risks; that is, the effect of technology on the development of new hardware, software, or procedures.

3.25 Threat Validation. A documented confirmation by DIA or other DOD intelligence agency that the intelligence contained in the Statement of Operational Need applies to the mission tasks and is consistent with current intelligence community estimates.

3.26 Vulnerability. In security engineering, the susceptibility of systems or components to overt or security threats. Security vulnerability is measured in terms of function or absence of function of design.

4. GENERAL REQUIREMENTS

4.1 System Security Engineering (SSE) Management Program. The contractor shall establish a SSE program to support economical achievement of overall program objectives. To be considered efficient, the SSE program: (1) enhances the operational readiness and mission success of the defense resource; (2) identifies and reduces potential vulnerabilities to security threats; (3) provides management information essential to system security planning and; (4) minimizes its own impact on overall program cost and schedule.

4.2 SSE Program Requirements. Weapon system acquisition is divided into four phases: concept exploration, demonstration and validation, full-scale development, and production and deployment. General SSE requirements accomplished during each of the four phases are as follows:

4.2.1 Concept Exploration Phase. Develop system security criteria, describe the base-line security system design, and conduct security threat and vulnerability studies.

4.2.2 Demonstration and Validation Phase. Through a series of analyses, the baseline security system design described during the concept exploration phase is validated and preliminary performance specifications for security hardware and software prepared. Identified threats and vulnerabilities are processed through system design modifications and risk management.

4.2.3 Full-Scale Development Phase. The security system should be fully designed and integrated. Security system hardware and software should be acquired or developed against the specifications prepared in the demonstration and validation phase.

4.2.4 Production and Deployment Phase. Implement the security system design via production and conduct deployment planning.

5. DETAILED REQUIREMENTS

5.1 Purpose. The SSE program establishes, as part of each acquisition development and upgrade program, appropriate procedures to identify security vulnerabilities and resulting actions to eliminate or contain associated risks. Further, it provides a means to insure necessary security requirements (physical, personnel, technical, communications, operations and information security, etc.) are adequately considered and, when appropriate, incorporated in the overall system development program.

5.2 Application Guidance. SSE requirements exist, in various degrees, throughout the life cycle of a major development and/or upgrade program. As such, the SSE program shall be tailored to facilitate continuation of SSE objectives through each acquisition phase: Concept Exploration, Demonstration and Validation, Full-scale Development, and Production and Deployment. It shall also accommodate class I through V modifications, test and evaluation, and research and development.

5.3 Task Requirements.

5.3.1 Concept Exploration Phase. The primary output of the SSE program during this phase is the identification of a broad range of security criteria and concepts which satisfy operational conditions and mission requirements. These criteria are conceptualized early in the system acquisition process. At the beginning of the Concept Exploration Phase, the managing activity will evaluate available information from operational and program management requirements documentation; i.e., SON, SORD, JSOR, PMD, which is used to explore concepts for integrated security solutions. During this early phase, all possible security requirements shall be consolidated and evaluated to achieve a defined security concept. These system security requirements shall be validated (Validation Phase) as part of the definition of system security criteria.

5.3.1.1 System Security Management Plan (SSMP). A System Security Management Plan shall be developed to describe the contractor's security engineering and management approach, including how the contractor will interact with the Government, subcontractors and vendors, and the anticipated level of contribution for each. The contractor shall also describe methods which shall be implemented to insure program schedules are maintained (See 6.2).

5.3.1.2 Threat Definition and Analysis. Threat definition is, in most cases, provided by intelligence sources in the form of a statement and/or scenarios which identify anticipated adversaries, their skills, capabilities, dedication, and size. A threat analysis is accomplished to further identify adversary mission objectives as they pertain to the system and provide a preliminary estimate of the effect of the threat on each conceptual system baseline or design alternative. This analysis shall include a credible worst case threat extending over the projected life of the system. The threat environment, as defined at this point, represents a best quantitative estimate available, on the basis of current threat information, and is used to validate system security criteria.

5.3.1.3 Preliminary System Security Concept (PSSC). Based on the threat definition, vulnerability analysis and existing security systems already in place, if any, a preliminary system security concept shall be developed. The PSSC is generally prepared by the government and will be provided to the contractor for use and possible update during subsequent program phases. However, the government may task the contractor to prepare this document. The PSSC may be general in nature, but as a minimum shall describe mission task, operational systems, operational environment, and personnel/manpower, equipment and employment issues. The PSSC coupled with threat definitions and operational requirements documents provided by the managing activity, serves as source material for further defining system security requirements (See 6.2).

5.3.1.4 Security Requirements Definition. Security program requirements shall be developed to support the proposed system security concept including a discussion on each security element identified in the System Security Management Plan. Documents made available by the managing activity include threat assessments, operational concepts, mission statements, etc. General system characteristics or capabilities that might be required to adequately secure the system are also identified.

5.3.1.5 Technology Assessments and Cost Studies. Ultimately, security technologies must be deployed which will satisfy defined requirements, support the operational concepts, and secure the system against defined security vulnerabilities. In order to do this, assessments of both DOD developed and commercially available hardware shall be accomplished. Preliminary assessments shall be made of hardware or software applicability, operability, suitability, supportability and/or affordability of various technology options.

5.3.1.6 Logistics Support. Prepare a Logistics Support Plan or an appendix to the overall system logistics support plan. Identify for incorporation into the overall system logistics support plan the management objectives and procedures for accommondating logistics requirements associated with security systems and sub-systems (See 6.2).

5.3.1.7 Security Training Requirements. Training requirements and anticipated skill levels necessary to effectively operate and maintain security systems shall be identified. Course material to support training requirements shall be developed.

5.3.1.8 Reliability and Maintainability Program (R&M). An R&M program shall be developed for implementation throughout the acquisition process. MIL-STD-785 and MIL-STD-470 prescribe tailorable tasks with guidance and rationale for their selection and application.

5.3.1.9 Preliminary Security Vulnerability Analysis. A vulnerability analysis of the preliminary baseline design shall be conducted (See 6.2). This analysis includes:

a. Identifying logical security vulnerabilities of the system in its projected operational environments and addressing general threats stated in the SON and threat definition documents (see 5.3.1.2).

b. Defining security system functional requirements which may effectively secure the system from exploitation.

c. Choosing candidate safeguards and safeguard configurations to mitigate or reduce identified vulnerabilities.

5.3.1.10 Security Classification Requirements. A security classification guide is provided by the government and used to identify specific classification decisions for contractor prepared deliverables.

5.3.2 Demonstration and Validation Phase. The goal of the SSE program Demonstration and Validation Phase is to translate qualitative security criteria, developed during the Concept Exploration Phase, into quantitative security criteria for specifications that can be used during the Full-Scale Development Phase. This phase is concerned with "validating" the system security concept and selecting specific "design-to" requirements on the basis of a series of analyses, trade studies, prototypes, etc.

5.3.2.1 Adversary Mission Analysis. An adversary mission analysis shall be conducted (See 6.2). This analysis shall include:

a. Adversary mission scenarios. Using the information from the threat analysis conducted in the Conceptual Phase (para 5.3.1.2) mission objectives shall be determined and tactics potential adversaries could use shall be described. Physical paths by which the adversary could execute each scenario shall be analyzed.

b. Estimating adversary success criteria.

c. Cataloging adversary mission objectives and success criteria according to each variation in the design of the system.

d. Synthesizing adversary models.

e. Recommending safeguards and configurations for security trade-off analysis.

5.3.2.2 Preliminary System Security Concept (PSSC). The preliminary system security concept prepared during the Conceptual Phase shall be updated and expanded (See 6.2).

5.3.2.3 Review of Security Regulatory Requirements. Government security program regulatory requirements shall be evaluated and potential deviations identified, assessed, and validated.

5.3.2.4 Security Vulnerability Analysis. Update the security vulnerability analysis. Each candidate safeguard and each candidate safeguard configuration shall be evaluated against each adversary model (para 5.3.2.1). Security vulnerabilities of each proposed safeguard shall be evaluated, and candidates ranked according to their effectiveness (See 6.2).

5.3.2.5. Security System Trade-Off Analysis. A security system trade-off analysis shall be conducted using approved candidate safeguards (para 5.3.1.5). Variables to be considered shall include security effectiveness; cost for facilities, manpower, equipment, schedule, system performance impacts, supportability, maintainability, technology, etc.

5.3.2.6 System and Subsystem Specification. Preliminary specification inputs shall be developed to identify general system security requirements, specific security hardware and software definition, and security qualification requirements. These inputs shall be designed to be incorporated into system development and product specifications (See 6.2).

5.3.2.7 Manpower Impact Assessments. Manpower requirements associated with the deployment of security systems shall be identified.

5.3.3 Full-Scale Development Phase. The primary goals of the SSE program in this phase are to develop the hardware, firmware, and software components of the pre-production prototype system according to system specification; verify compliance with the specification requirements supported by engineering development tests; qualify security subsystems; and document the information required to enter the production phase.

5.3.3.1 System Security Requirements Definition. System security requirements shall be defined. This task is part of system requirements analysis which implements the system engineering

objectives of MIL-STD-499, "Engineering Management," and the logistics support analysis objectives of MIL-STD-1388-1, "Logistics Support Analysis." It shall include the SSE program requirements as derived from an operational analysis; a logistic support analysis; a test analysis; and an assembly, installation, and check-out technical analysis. The results of this task shall be included in the system design review.

5.3.3.2 System Security Management Plan (SSMP). This plan, which is initially developed in the Concept Exploration Phase and updated in the Validation Phase, shall be further expanded during Full-Scale Development. The plan describes the contractor's security engineering management approach in detail. It shall include an approach for analytical verification analysis (See 6.2).

5.3.3.3 Subsystem and Interface Specifications. Develop Subsystem and interface specifications. These specifications shall be prepared according to MIL-STD-490. Subsystem and interface specifications detail components and piece parts procured separately and define the design, functional and procedural interfaces among developmental, operational and government furnished equipment (GFE)/subsystem.

5.3.3.4 System Security Design. This task uses system security requirements to perform a preliminary design of the major subsystems which comprise the overall security system. The following analysis and testing shall be performed to validate components which may be required to ensure functional performance of the preliminary designs.

5.3.3.4.1 Component Screening. Candidate GFE and CFE security system components performing given functions shall be identified and selected for analysis to satisfy specification requirements.

5.3.3.4.2 Component Response Analysis. Selected components shall be analyzed to determine if their response to the specified environments and stimuli are acceptable.

5.3.3.4.3 Engineering Tests. At the preliminary design state, tests shall be performed on simulated components such as breadboard circuits, non-production assemblies, etc., to provide data which compliments or supplements the response analysis.

5.3.3.5 Subsystem Verification Analysis. This analysis verifies that each subsystem meets the requirements of the system security criteria and security requirements in applicable subsystem, interface, component and test specifications. It shall be performed to assess the inherent capability of the security system at the sub-system level.

5.3.3.6 Subsystem and System Response Analysis. Subsystem and system response analysis shall be performed to include:

5.3.3.6.1 Threat Rejection Logic. During the Validation Phase, a number of adversary models which might possibly engage the system were required to be synthesized. The number of adversary models used to perform trade-off analysis initially was probably large. However, many alternatives will have since been discarded because they have ceased to be relevant for one of three possible reasons: (a) the adversary mission objective is now out of scope as a practical goal; (b) there are no longer any plausible means to satisfy mission objectives; or (c) the adversary threat is not (or no longer) officially considered viable. The first two reasons may be related to the system design or operational concepts as presently defined. The third is related to the official estimate of the threat and risk assessment incident to vulnerability analysis. Adversary models shall be evaluated and the most viable selected for detailed analysis.

5.3.3.6.2 Detailed Adversary Modeling. The remaining adversary models shall be revised according to current threat projections and developed in sufficient detail to model all the important variables. These models may be used again in system level verification analysis.

5.3.3.6.3 Subsystem Response Modeling. During the period between preliminary design review and critical design review the design of the security system is in a continual state of detailed development. The process of screening components, software, procedures, etc., is an interactive process. Promising components shall be selected for response modeling. This modeling shall be of sufficient detail to permit a thorough description of subsystem critical functional and subsystem responses to specified environments and threat stimuli.

5.3.3.6.4 Subsystem Qualification Testing. Subsystem qualification testing shall be performed as directed by the government.

5.3.3.6.5 System Verification Analysis. This analysis shall be conducted to verify compliance with security requirements in the system specification, and to assess the capability of the system as a whole to counter the specified security threats and contain associated vulnerabilities.

5.3.3.6.6 System Response Modeling. System response modeling shall be conducted. The inputs to these models include the subsystem response models which have been performed in the subsystem verification analysis and modified to account for the physical and functional interfaces between subsystems. Engineering development testing is required to model total system response.

5.3.3.6.7 System Response Analysis. System response analysis shall be conducted using the detailed adversary models of the subsystem verification analysis and the system response models.

5.3.4 Production and Deployment Phase. The goal of the SSE program during this phase is to ensure that defined security requirements are met in the operational system.

5.3.4.1 Acceptance Testing. Acceptance testing shall be monitored and supported as necessary to ensure CIs, including changes, meet security requirements. Test methods, as well as results shall be examined.

5.3.4.2 Training. Initial training on security systems shall be monitored and analyzed to ensure that it is adequate and that personnel with appropriate skill levels can operate and maintain the system.

5.3.4.3 Program Management Responsibility Transfer (PMRT) Support. PMRT shall be supported as necessary. This support shall include:

a. Preparing the security portion of the agreement to transfer program management to the government supporting command or agency.

b. Analyzing feedback from the operational unit's experience in actually operating the system.

5.3.4.4 Product Security. Security must be provided for essential products at key assembly plants and facilities. The government outlines protection criteria for assembly plants, facilities and critical components not yet delivered. The contractor provides input to the Product Security Programs and may be tasked to include product security requirements in the SSMP (See 6.2).

Custodians:

Army -
Navy -
Air Force - 10

Review activities:

Army -
Navy -
Air Force - 11, 19, 26

User activities:

Army -
Navy -
Air Force -

Preparing activity:

Air Force - 10

(Project MISC 0035)

6. NOTES

6.1 Intended Use. This standard is used by government agencies and defense contractors for those programs that require selective application of system security engineering program management.

6.2 Data Requirements. The following data requirements should be considered when this standard is applied on a contract. The applicable Data Item Descriptions (DID's) should be reviewed in conjunction with the specific acquisition to ensure that only essential data are requested/provided and that the DID's are tailored to reflect the requirements of the specific acquisition. To ensure correct contractual application of the data requirements, a Contract Data Requirements List (DD Form 1423) must be prepared to obtain the data, except where DOD FAR Supplement 27.475-1 exempts the requirement for a DD Form 1423.

Paragraph No.	Data Requirement Title	Applicable DID No.
5.3.1.1/ 5.3.3.2	System Security Management Plan	DI-MISC-80839
5.3.1.3/ 5.3.2.2	Preliminary System Security Concept	DI-MISC-80840
5.3.1.6	Logistical Support Plan	DI-S-1817
5.3.1.9/ 5.3.2.4	Security Vulnerability Analysis	DI-MISC-80841
5.3.2.1	Adversary Mission Analysis	DI-MISC-80842
5.3.2.6	System/Subsystem Specification	DI-S-30551B

☆U.S. GOVERNMENT PRINTING OFFICE: 1989 - 604-033/13961

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER	2. DOCUMENT DATE (YYMMDD)
3. DOCUMENT TITLE		

4. NATURE OF CHANGE (Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets if needed.)

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (Last, First, Middle Initial)	b. ORGANIZATION	
c. ADDRESS (Include Zip Code)	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON (If applicable)	7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME	b. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON
c. ADDRESS (Include Zip Code)	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340