NATIONAL SECURITY AGENCY

USER PARTNERSHIP PROGRAM

with

UNITED STATES AIR FORCE
653rd ELECTRONIC SYSTEMS WING (ELSW)
5 EGLIN STREET, BLDG 1642
HANSCOM AFB, MA 01731

Telecommunications Security Requirements Document (TSRD)

for

MINUTEMAN MINIMUM ESSENTIAL EMERGENCY COMMUNICATIONS NETWORK (MEECN) PROGRAM UPGRADE (MMP-U) INITIATIVE
Hardware - The contractor shall establish and maintain an adequate system for generating and controlling changes and variances to INFOSEC-Boundary hardware CIs. The system shall be subject to NSA review at any time during the performance of the UPA. Hardware changes shall be accompanied by supporting documentation (graphics and text).

Software - Requests identifying changes or modifications to INFOSEC-Boundary software CIs shall be IAW IEEE/EIA 12207.1-1997, clause 6.2. Software changes shall be supported by electronic submissions (CD-ROM or disk) of the new source code and the version description document (see Software Version Description) updated as a result of the change.

20. Engineering Drawings, Software and Configuration Item (CI) Database.
CI technical documentation consisting of 1) engineering drawings that accurately reflect the custom CIs comprising the INFOSEC-Boundary; 2) executable software and source files for operational and custom support software utilized within the INFOSEC-Boundary, including any batch, command, data or other software files needed to successfully install/operate the software, and a version description of the software (see Software Products Specification); and 3) a CI database reflecting the INFOSEC-Boundary shall be produced and maintained by the contractor. The contractor shall use NSA assigned “0N” numbers to identify all custom hardware, firmware, and software CIs within or related to the INFOSEC-Boundary. The contractor shall ensure that the assigned “0N” number is also reflected on custom CI technical documentation. The contractor shall update custom CI engineering drawings, executable software and source files, and the CI database, as applicable, incorporating those changes approved by the NSA.

Hardware - Engineering drawings of custom hardware CIs shall be submitted in the Initial Graphics Exchange Specification (IGES) format. The contractor shall be responsible for conducting IGES Compatibility testing using the test data and instructions provided by the NSA. Engineering drawings containing classified, restricted or proprietary information shall reflect the appropriate caveat and clearly identify the information requiring special handling, as applicable. Classification (SECRET, CONFIDENTIAL, etc.) and Dissemination (NOT RELEASABLE TO FOREIGN NATIONALS, FOR OFFICIAL USE ONLY, etc.) markings shall appear in the upper left and lower right corners, in the margin area. Proprietary markings shall be located adjacent to the drawing title block and shall be of sufficient size/style so as to be readily evident. The contractor is responsible for ensuring that all information requiring special handling is properly identified and appropriately marked. Format is per Dl DI-SESS-81000C. Product Drawings / Models and Associated Lists, and delivery requirements are described in CDRL UP10.

Software - Executable object code and software configuration index records for custom software CIs shall be IAW IEEE/EIA 12207.1-1997, clause 6.7 and 6.13, respectively. If the software configuration index records do not include the executable software, source files, and compilation, build and modification procedures, the contractor shall submit these “files” under separate cover. All magnetic media shall be appropriately labeled with identification number(s), title(s), date(s), version number(s), and release number(s). In addition, all magnetic media containing classified, restricted or proprietary information shall be appropriately labeled with applicable caveat(s). All identification markings shall be annotated on label(s) and applied to the face of the media. The contractor shall ensure that the software configuration index records include an inventory of the software contents and a list of all of the changes incorporated into the software version since the previous version including, as applicable, problem reports, change requests and
modifications, and the effects, if any, of each change on system operation and on interfaces with other hardware and software. The list of changes does not apply to the initial software version. Format is per DID DI-IPSC-81441A, Software Product Specification, and DID IPSC-81442A, Software Version Description. The delivery requirements are described in CDRL UP10.

The CI database (composite listing reflecting all CIs comprising the INFOSEC-Boundary) shall be prepared in a flat-file validated format using the Flat-File Validation Software and Users Manual provided by the NSA. Format is per DID DI-CMAN-90072 , Engineering Database and Configuration Information, delivery requirements are described in CDRL UP10.

The contractor shall complete and enclose a copy of the following affirmation of conformance, signed by an officer of the company, with each delivery of engineering drawings or software:

**Affirmation of Conformance**

"I affirm that on [insert date], [insert contractor's name] furnished custom engineering drawings or software required by TSRD No. [insert TSRD No.] via a letter of transmittal.

I further affirm that all classified, restricted or proprietary custom engineering drawings or software have been properly isolated and submitted on separate media."

**Date of Execution:** [insert date]

**Signature:** [insert contractor's signature]

**Title:** [insert contractor's title]

21. **Physical Configuration Audit (CA) Plan and Report.**

The contractor shall submit a PCA Plan addressing custom hardware and software, as applicable, describing when and how the initial PCA shall be conducted. The PCA Plan must be approved by the NSA prior to the actual performance of the PCA by a team consisting of NSA and contractor personnel. The PCA validates the deliverable executable software file(s) and verifies the accuracy of the "as-built" configuration of the INFOSEC-Boundary against the technical documentation package. All changes required as a result of the initial PCA shall have been incorporated prior to NSA approval of the PCA. Subsequent to the successful completion of the initial PCA required for certification, the executable custom software file(s), the INFOSEC-Boundary custom engineering drawings and the CI database shall be considered to be baselined. At this point, any/all changes to these baselines require NSA approval. Formats are per DIDs DI-SESS-81646, Configuration Audit Plan and DI-CMAN-81022C, Configuration Audit Summary Report. The delivery requirements are described in CDRL UP11.

**Hardware** - The hardware PCA compares every assembly, subassembly, and piece part within the INFOSEC-Boundary against the technical documentation (engineering drawings, parts lists, specifications, acceptance test procedure, manuals, etc.) used in the production of the custom CI. The contractor shall be responsible for the disassembly and subsequent reassembly of the product/system unit audited during the hardware PCA. The hardware PCA shall be performed after the successful completion of all required testing and prior to the initiation of production efforts. Subsequent to certification, aperiodic hardware PCAs may be performed to ensure that the technical data accurately and completely describes all changes made to the custom CIs, to verify the security integrity and assure the continued certification of the product/system.
Software - The software PCA compares the deliverable executable custom software file(s) to an executable file(s) made by the PCA team from the development database source code using the developer's system build document(s). The software PCA shall be performed after successful completion of required functional testing and prior to establishing the as-built hardware baseline. At the NSA’s option, the software PCA may be performed by the contractor and witnessed by the Government. After certification, software PCAs shall be performed each time that an approved change is incorporated into the software baseline to verify the security integrity of the custom CI and assure the continued certification of the product/system.

Subsequent to the completion of each PCA, the contractor shall provide the NSA with a report containing:

a. Audit identification including the name and nomenclature of the system, subsystem, equipment, or parts; name of the Vendor and date the PCA was conducted;

b. A list of all documentation subjected to the PCA along with agreed-upon revision levels, assembly description, software identification numbers and serial numbers;

c. A list of discrepancies found during the PCA and a description of how the discrepancy shall be specifically resolved including actual or projected completion date; and

d. A list of all unincorporated changes in drawing/software number order.

(The following software requirements are applicable for all software efforts including custom Automatic Test Equipment and Test Monitor Units !)

22. Software:

a) System Subsystem Specification (SSS)

The System/Subsystem Specification (SSS) specifies the requirements for a system or subsystem and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the system or subsystem's external interfaces may be presented in the SSS or in one or more Interface Requirements Specifications (IRSs) (DI-IPSC081434A) referenced from the SSS.

The SSS, possibly supplemented by IRSs, is used as the basis for design and qualification testing of a system or subsystem. Throughout this Data Item Description (DID), the term "system" may be interpreted to mean "subsystem" as applicable. The resulting document should be titled System Specification or Subsystem Specification (SSS). Format is per DID DI-IPSC-81431A (Supersedes DI-IPSC-81431A). System Subsystem Specification (SSS) and delivery requirements are described in CDRL UP31.

b) Software Requirements Specification (SRS)

Software is documented in the SRS to provide traceability of the functional, performance, design, interface, and security requirements for the software CIs. Security functions implemented in software shall be clearly mapped to the UIC. The content of the SRS shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1 - 1997, clause 6.22. If other than IEEE 12207 compliant standards are used, then a matrix shall be prepared with the deliverable that shows how the deliverable maps to the IEEE/EIA 12207.1, clause 6.22. See IEEE Std 830-1998, 20 Oct. 1998 for guidance. Format is per DID DI-IPSC-81433A. Software Requirements Specification (SRS) and delivery requirements are described in CDRL UP18.
c) Software Test Plan (STP)
During software program design, the contractor shall prepare a STP which describes plans for qualification testing of software CIs and software systems. It describes the software test environment to be used for testing, identifies the tests to be performed, and the schedules for test activities. The STP shall clearly map testing of the UIC security functions implemented in software. The content of the STP shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997, clause 6.27. See IEEE Std 829-1998, 16 Sep 1998 for guidance. Format is per DID DI-IPSC-81438A, Software Test Plan, and delivery requirements are described in CDRL UP19.

d) Software Test Report (STR)
Following the completion of qualification testing, the contractor shall submit a STR. The STR is a record of qualification testing performed on a software CI, a software system/subsystem, or other software-related items. The STP shall clearly map the test results of the UIC security functions implemented in software. The content of the STR shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997, clause 6.29. See IEEE Std 829-1998, 16 Sep. 1998 for guidance. Format is per DID DI-IPSC-81440A, Software Test Plan, and delivery requirements are described in CDRL UP20.

e) Software Products Specification (SPS)
The SPS is the primary support document for a software CI and can be used to order the executable software and/or source files for the software CI (see Engineering Drawings, Software and CI Database). It contains or references the executable software, source files, and software support information including "as built" design information and compilation, build, and modification procedures for the software CI. The content of the SPS shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997, clause 5.1. Format is per DID DI-IPSC-81441A, Software Product Specification (SPS), and delivery requirements are described in CDRL UP22.

f) Software Version Description (SVD)
The SVD identifies and describes a software version consisting of one or more software CIs. It is used to release, track, and control software versions (see Configuration Control Documentation). The content of the SVD shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997, clause 6.13. Format is per DID DI-IPSC-81442A, Software Version Description (SVD), and delivery requirements are described in CDRL UP25.

g) Software Development Plan (SDP)
The SDP outlines the vendor's plans for producing and controlling the development of software. Upon NSA approval of the baselined SDP, the vendor shall manage the development of software for the project IAW the approved plan. The content of the SDP shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997, clause 6.5. Format is per DID DI-81427A, Software Development Plan (SDP) and delivery requirements are described in CDRL UP21. The configuration management portion of the SDP shall be bound and delivered separately.
h) Software Design Description (SDD)
The SDD describes the design of a software CI including software CI-wide design decisions, software CI architectural design, and the detailed design needed to implement the software requirements as delineated in the SRS. The design also confirms that the implementation of the requirements and goals specified in the TOC are being met. This information shall be documented in the SDD. The SDD then becomes the baseline document from which code will be produced. The content of the SDD shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997 clause 6.16. See IEEE Std 1016-1998, 23 Sept. 1998 for guidance. Format is per DID DL-IPSC-81435A, Software Design Description (SDD) and delivery requirements are described in CDRL UP24.

i) Software Test Description (STD)
Following approval of the STP, the vendor shall initiate preparation of the STD. The STD describes the test preparations, test cases, and test procedures to be used to perform qualification testing of a software CI or a software system or subsystem. It enables the acquirer to assess the adequacy of the qualification testing to be performed as it relates to the SRS and the UIC. The content of the STD shall be IAW an appropriate IEEE 12207 compliant standard or best practice that includes proof of compliance with IEEE/EIA 12207.1-1997 clause 6.28. See IEEE Std 829-1998, 16 Sept. 1998 for guidance. Format is per DID DL-81439A, Software Test Description (STD), and delivery requirements are described in CDRL UP23.
SECTION 4 - ADDITIONAL REQUIREMENTS

Timely availability of the NSA's labor resources to support the program is a significant factor in ensuring the success of the program. The NSA's awareness of the contractors program plans is essential for the NSA to adequately plan and schedule its resources. Updated copies of the contractor's milestones chart, or similar management tool for the program, is needed by the NSA for planning and scheduling the NSA's workforce and activities. Include work completed against planned milestones accomplished, problems encountered, specific actions taken by the contractor or the NSA, and the plans for the next period. Format is per DID DI-MGMT-80368, Status Report, and delivery requirements are described in CDRL UP01.

24. TEMPEST Documentation.
The contractor must develop the following plans and report for controlling and testing TEMPEST aspects of the product/system.

   a) TEMPEST Control Plan
A Control Plan must be prepared as specified below and approved by the NSA not later than final review or approval. Format is per DID DI-EMCS-90005A Tempest Control Plan, and delivery requirements are described in CDRL UP06. A Control Plan must include at least the following information:

   (1) Title Page
   (2) Management Control
   (3) General Description of product/system
   (4) Statement of TEMPEST Requirements
   (5) Mechanical Design which shall include the following:
       (a) Construction Techniques
           - Housing material
           - Compartmentalization (RED/BLACK)
           - Penetration (windows, air vents, access plates)
           - Drawings, including an exploded view
           - RF Gasketing
       (b) Interface Techniques
           - Signal filtering
           - Power filtering
           - Location and mounting of filters
           - Connectors/Junction Boxes
       (c) Other Design Features
           - List any other mechanical design features which may have an impact on the TEMPEST characteristic of the unit.
   (6) RED/BLACK Design which shall include the following:
(a) RED/BLACK signals
- RED/BLACK signal flow description and block flow diagram
- RED/BLACK power distribution description and block flow diagram
- RED/BLACK Logic (type, signal amplitude, and signal transition times)
- RED/BLACK Interfaces (signal amplitude, transition times, design considerations)

(b) Other RED/BLACK Design Features
- Physical RED/BLACK circuit layout (multi-layer PWAs, partitioning of circuits)
- Type of cabling
- Grounding
- Clocking

b) TEMPEST Test Plan
A Test Plan must be submitted at least 90 days prior to the start of TEMPEST testing. The TEMPEST Test Plan shall be prepared as specified in NSTISSAM TEMPEST/1-92, paragraph 6.2 and Appendix L. If a NONSTOP Test Plan is required, it shall be prepared as specified in NASCEM 5112, paragraph 5.2, and combined with the TEMPEST Test Plan. If a HIJACK Test Plan is required, it shall be prepared as specified in KAG-30A, paragraph 6.1.1.6.2 and G2.0, and combined with the TEMPEST Test Plan. Format is per Did DI-EMCS-90000A, Tempest Test Plan, and delivery requirements are described in CDRL UP07.

c) TEMPEST Test Report
A Test Report must be submitted after completion. The report must contain only original photographs and signatures. The TEMPEST Test Report shall be prepared as specified in NSTISSAM TEMPEST/1-92, paragraph 6.7, and shall include the certification requirements of paragraphs 6.4, 6.5, and 6.6. If a NONSTOP Test Report is required, it shall be prepared as specified in NASCEM 5112, paragraph 5.4, and shall include the certification requirements of paragraph 5.3 and combined with the TEMPEST Test Report. If a HIJACK Test Report is required, it shall be prepared as specified in KAG-30A, paragraph 6.1.1.6.4 and H2.2, and shall include certification requirements of paragraph 6.1.1.6.3 and combined with the TEMPEST Test Report. Format is per Did DI-EMCS-90000A, Tempest Test Evaluation Report and delivery requirements are described in CDRL UP08.

25. Anti-Tamper Protection Requirements.
Anti-tamper protection is the collection of mechanisms, design features, and manufacturing techniques which minimize the probability of undetected penetration of an equipment and compromise of classified information.
Defense mechanisms are required to protect communication equipment against forced disclosure of classified or sensitive information. These mechanisms are also appropriate for implementation in ancillary or peripheral devices which may also be exploited to obtain the same information. The equipment design and physical security controls afforded these devices must be sufficient to assure a very high probability of detecting tampering attacks and thwarting attempts to obtain classified or
sensitive information either directly or indirectly. Further, there must not be any recoverable sensitive information remnant in the protected device following a penetration.

All anti-tamper protection security specifications that are outlined in the UIC, must be met for the product to be approved by NSA. A detailed description of the Anti-Tamper design features that fulfill each requirement stated in the UIC shall be given in the appropriate sections of the Theories of Design Operation and Compliance (CDRLs UP03 and UP04). The full text of each UIC requirement shall not be re-stated in these reports, rather, each UIC section shall be referenced by paragraph number.

The Interface and Operators Guide is divided into Parts I and II, and shall be submitted as a separate manual for each part. Format and delivery requirements are described in CDRL UP14. Part I consists of the type of information that would normally be included in an interface specification. Part II consists of the type of information that would normally be included in an operators guide. Each manual shall be completed as described below for Part I and Part II.

PART I: INTERFACE INFORMATION - This section must contain sufficient detail to enable thorough evaluation and control of the physical and functional design interrelationships of interdependent components, equipment, subsystems, segments, systems, or facilities. This requirement applies, but is not limited to, custom INFOSEC integrated-circuit (IC) packages, printed wiring assemblies (PWA), modules, or equipment.

This section shall include, as applicable, but not necessarily be limited to:

a. configuration and all interface data applicable to the envelope, mounting, and mating of the assemblies and subsystems; and
b. complete interface engineering requirements, interconnecting data, timing diagrams, signals, and design limitations such as mechanical, electrical, electronic, hydraulic, pneumatic, optical, etc., which affect the physical or functional characteristics of co-functioning assemblies.

PART II: OPERATING INSTRUCTIONS - Operating instructions are required for the INFOSEC product/system whenever controls, switches, straps, plug-in modules, etc., affect the function, mode of operation, or repair of the INFOSEC product/system. This document must be complete in its description of the item and the procedures required to operate it.

a. It is the contractors responsibility to provide documentation necessary to support operation of the item for the life of the item.

b. The following information must be included as part of the documentation for operation of the INFOSEC product/system:

(1) The item and its inter-operation within a system, if applicable, must be clearly described.
(2) Step-by-step operating instructions for the item must be given.
(3) An operator’s problem solving guide shall be provided.
(4) Detailed or specific information concerning the cryptologic or internal critical cryptographic functions must not be included.
(5) As the configuration of the item changes, any associated changes in the operating procedures must be reflected in the instructions.

27. INFOSEC Security Awareness Training.

Per the National Security Telecommunications and Information Systems Security Instruction for the maintenance and training of INFOSEC equipment (NSTISSI 4000) the following minimum requirements have been established:

a. Contractor Maintenance Training - The contractor is responsible for ensuring that all Users (unless User training is permitted) and contractor service technicians that perform maintenance on the INFOSEC product/system receive formal maintenance training from the contractor commensurate to the level of maintenance they will be performing. The formal maintenance training shall meet the requirements specified below. Format and delivery requirements are described in CDRL UP15. The contractor shall maintain a tracking system to ensure that maintenance performed by Users and contractor service technicians is done by technicians who have satisfactorily completed the contractor formal maintenance training course. On-the-job training (OJT) does not meet the requirements of this document.

b. Contractor Maintenance Training Plan - The plan shall be prepared and submitted IAW the User Partner requirements and include INFOSEC Security awareness training as a minimum. The INFOSEC awareness training shall include:

   (1) INFOSEC doctrine, policy and procedures;
   (2) Principles and applications of TEMPEST;
   (3) Security and technical threat awareness;
   (4) Awareness of special hardware protective technology (where appropriate);
   (5) Unique security requirements pertaining to the equipment or system;
   (6) Documents and related reference material;
   (7) Physical handling, accounting, and destruction requirements;
   (8) Applicable Federal Government department and/or regulations; and
   (9) Standard operating procedures.

c. Contractor Formal Maintenance Training Course of instruction (COI) - Criterion referenced formal maintenance training COIs shall be prepared for teaching maintenance of certified product/systems and must be submitted to the NSA for review and approval of INFOSEC portions prior to being made available to Users or implemented at the contractors facility. These COIs shall be prepared IAW the User partner requirements, and shall:

   (1) be designed to enable maintenance technicians to diagnose and repair the INFOSEC product/system;
   (2) include appropriate INFOSEC paragraphs, illustrations, etc., from the manual(s) to be used by the technicians;
(3) include all required security precautions, etc., set forth by the UPA and identify
unique restrictions or precautions necessary to maintain the security integrity (such as
TEMPEST) of the INFOSEC product/system;
(4) include instruction on any special equipment required to be used in maintaining the
INFOSEC product/system.

d. **Follow-On Training** - A system of follow-on training and testing is recommended to
ensure that technicians retain the skills required to maintain the equipment. Additional
formal maintenance training shall be required if the configuration of the product/system
undergoes a major change.

28. **Maintenance Manuals.**
Maintenance manuals prepared to provide documentation necessary to support maintenance of
INFOSEC portions of the UPP approved product/systems must be submitted to the NSA for review
and approval. Format and delivery requirements are described in CDRL UP16. As a minimum, these
manuals shall adhere to the following guidelines:

a. be complete in their description of the procedures required to maintain the INFOSEC
   product/system.
b. be clear, concise, and logical, and written for the education level of the technicians who
   will be performing maintenance of the product/system.
c. contain sufficient theory of operation to give the technician the level of understanding
   necessary to perform required maintenance of the INFOSEC product/system.
d. include all procedures, including accompanying troubleshooting charts, schematics,
   wiring diagrams, illustrations, etc., necessary to perform required maintenance on the
   INFOSEC product/system. The INFOSEC portions of these product/systems must be
   identified for technician reference.
e. include all required security precautions, handling instructions, etc., in the manuals.
f. identify unique restrictions or precautions necessary to maintain the INFOSEC
   product/system.
g. incorporate all changes in maintenance procedures resulting from changes in
   configuration of the INFOSEC product/system.
h. any deviation in the above requirements for CCI product/systems must have approval of
   the NSA.

29. **Security Production Assurance (SPA).**
The contractor shall prepare and implement a SPA program that ensures the security integrity of the
UPP product/system. The SPA shall address both the Physical Configuration and the Functional
Performance of the product/system and shall be based on a comprehensive review of the
requirements utilizing drawings, specifications, component screening, testing, and assembly. The
SPA shall consider the complete manufacturing process and identify the essential HW/SW security
checkpoints, making reference to the contractor's documents that provide the criteria for inspection
and test which validate and protect the security integrity of the UPP product/system. The contractor
shall ensure that the SPA is maintained in a current status satisfying the requirements of the UPA,
and as specified herein, to assure continued approval for use of the UPP product/system. Format and
delivery requirements are described in CDRL UP17. The SPA shall be submitted to the NSA for approval, and as a minimum, shall contain the following:

a. **Organizational Structure** - A block diagram of key personnel, including their applicable element, to identify and facilitate points of contact.

b. **Product/System Flow Diagram** - A production flow diagram that identifies the HW/SW security inspection/test checkpoints and references applicable contractor documents that specify inspection and test criteria/procedures used throughout the manufacturing process. The flow diagram, as a minimum, includes the following.
   1. A list of the types of inspection and testing that the contractor plans to perform during the manufacture and assembly of the product/system.
   2. A list of the security features that shall be tested and a description stating how the contractor plans to implement the test(s).
   3. A list of the test equipment that shall be used to perform the testing and a brief technical description of their capabilities.

c. **Parts Control Program** - A program to ensure the security integrity of the INFOSEC subsystem. The program shall, as a minimum, include the contractor’s system implemented to ensure that the INFOSEC subsystem contains the authorized/proper parts.

d. **Configuration Control System** - A control system for implementing product/system configuration changes to the UPP product/system. The system shall include procedures to ensure that engineering changes, variances and modifications are submitted to the NSA IAW their applicable CDRL, and that the proposed changes receive a Security Assessment, including appropriate technical and management concurrence, prior to their being submitted. Documentation changes shall be made prior to the product/system being changed. Periodically, after product/system approval for use, the NSA Product Assurance representative will use the current NSA baseline documentation to perform an INFOSEC product/system audit of the contractor’s current production hardware, firmware, software, and documentation at the contractor’s facility.

30. **INFOSEC-Boundary Verification Test (IVT).**

The contractor shall generate and implement the IVT, which is a test or series of tests used to verify that the INFOSEC-Boundary is functioning as intended (including protective alarms and security features). The HW/SW security functions contained in the product/system’s INFOSEC-Boundary must pass all levels of the IVT (IVT-I and IVT-II) as part of the continuing evaluation process. The contractor, in conjunction with the NSA, shall select the test(s) that are to be performed by the IVT based on the following areas: (1) the Security Verification Plan, (2) the Fail Safe Design and Analysis, (3) the cryptographic algorithm to be used, (4) the UIC requirements, (5) the INFOSEC-Boundary, (6) the anti-tamper requirements, (7) keying methods, and (8) any in-process production testing used (IC wafer and package test, PWA tests, etc.). The IVT shall be nondestructive.

a. The IVT, whenever possible, shall be written for and implemented on commercially available automated test equipment. While some manual intervention/testing may be required, the IVT shall be implemented so as to minimize operator intervention.
b. Whenever possible, INFOSEC-Boundary circuitry (custom IC’s, PWAs, modules, assemblies, etc.) shall be designed to be testable on commercially available automated test equipment.

c. The IVT shall be developed for two levels of testing with each level based on a cumulative effort that shall build confidence in the overall security integrity of the product/system.

(1) IVT-I test routines shall be developed and performed by the contractor on 100% of the INFOSEC-Boundary circuitry produced and/or embedded in the product/system. IVT-I testing shall incorporate all agreed upon production line testing used by the contractor (which may include IC tests, module tests, PWA tests, etc.). The IVT-I shall include a test that uses a test key(s) and word(s) to verify the HW/SW security features of the product/system and selected tests from the areas described in the IVT introductory paragraph.

(2) At the NSA’s option, IVT-II test routines may be developed and performed by the NSA on a periodic sample of the product/system. IVT-II shall include any testing performed in IVT-I and selected tests from the areas described in the IVT introductory paragraph.

d. As part of the continuing evaluation process, the contractor shall perform the IVT at all approved levels, with the NSA reserving the right to witness the testing. The contractor shall provide the necessary personnel, documentation, hardware, and facilities (including test equipment and training) to perform this effort. The NSA also reserves the right to perform the IVT tests at the NSA’s facilities.

e. The IVT documentation shall be included as an appendix to the SPA and prepared IAW CDRL UP17. The IVT documentation shall be submitted for approval prior to initial evaluation and shall, as a minimum, include the following:

(1) A description of each test, the method/technique used to test and/or verify each specific function and HW/SW security feature (i.e., LSI test, shift register test, randomizer test, etc.) and the sequence in which the tests are applied.

(2) A cross-reference list that shows where each test resides in the software routines and test flow.

(3) A listing of the expected results of each test.

(4) A functional description of the test setup and test equipment that is to be used.

(5) A copy of all the software that is necessary to perform the test.

(6) A copy of the programmer’s and User’s manual for any custom (contractor-generated) automatic test equipment (ATE) that shall be used to perform the IVT. If using a commercially available ATE system, a part and/or identification number for the programmer’s and User’s manual must be provided.

f. Successful completion of the IVT shall be based on: (1) performance of the product when using test data with a test or maintenance key and (2) the performance of the IVT versus the expected results as reported in the Security Verification Report, the Fail Safe Design and Analysis, and the IVT.

g. The NSA shall be included in the approval cycle for changes that affect the functionality of IVT procedures.
The vendor shall generate and submit integrated circuit design data used to fabricate custom Application Specific Integrated Circuit (ASIC) devices to NSA for review and approval. The ASIC data shall be in accordance with the following requirements:

a) Integrated Circuit Graphics Database
This database documents all geometric and associated layout information used in the fabrication of the ASIC device(s). Format is per DID DI-IPSC-80409, Integrated Circuit Graphics Database, and delivery requirements are described in CDRL UP26. The database shall include the following:

(1) Uncompressed GDSII stream format database.
(2) Chip name/project name.
(3) Company name.
(4) MOA number.
(5) Name(s) of library or libraries.
(6) Date created.
(7) Name of graphic cell or structure containing the chip description.
(8) Cross reference of graphic layers as they correspond to fabrication – Note: for clarification – this is the “Layer Map Table”.
(9) Listing of the line code table used to resolve polygons (if applicable).
(10) Data scale in design units (e.g. – mils, microns, etc.) per GDS.
(11) Revision date of chip and/or cells (as appropriate).
(12) Number of files.
(13) Classification.

b) Computer Aided Chip Development Data
(This data item is not required if the Trusted Foundry is utilized.) This data documents the fabrication of an ASIC device using computer aids. Format is per DID DI-MCCR-80499, Computer Aided Chip Development Data, and delivery requirements are described in CDRL UP27. The data shall include the following information:

(1) Chip name and Alphanumeric text.
(2) Cell connectivity data (e.g. – Net list), which may be derived from the logic description – Note: Net list shall be provided as a simulation model, preferable in Verilog or VHDL formats. Other formats shall be considered, with approval, at the discretion of the Government Program Manager.
(3) Chip specification (mechanical) to include bonding pad identification, bonding diagram and package specifications – Note: format for chip specification (mechanical) data shall be in the form of electronic drawings.
(4) Test vector set (test stimulus input) with corresponding test output data.

c) Computer Aided Cell Development Data
(This data item is not required if the Trusted Foundry is utilized.) This data documents the process for fabricating integrated circuit cells using computer aids. Format is per DID DI-MCCR-80500, Computer Aided Cell Development Data, and delivery requirements are described in CDRL UP28. The data shall include the following information:

(1) Chip name.
32. **Field Programmable Gate Array (FPGA) Documentation**

For each FPGA provide documentation/artifacts including the documentation plan, requirements, preliminary design information, detailed design information, VHDL code, verification methods and results (e.g. Simulation/Timing Diagrams), test results, review minutes and action items, problem reports, accomplishment summary and lessons learned. Documentation/Artifacts can be provided in the contractors format. Delivery requirements are described in CDRL UP30.
SECTION 5 - CONTRACTOR GUIDELINES FOR ACQUIRING KEYING MATERIAL

33. Guidelines For Obtaining Key:
   a. WHAT IS KEY?
      (1) Information (usually a sequence of random binary digits) used initially to set up and periodically change the operations performed in crypto-equipment for the purpose of encrypting/decrypting, determining electronic countermeasures (TRANSEC) patterns, producing other key, etc.
      (2) Keys perform specific functions:
            (a) Traffic Encryption Key (TEK), used to secure traffic
            (b) Seed Key, used for generating other keys
            (c) Key Encryption Key (KEK), used for encrypting other keys
            (d) Transmission Security Key (TRANSEC key), used in the control of transmission security processes (frequency hopping, spread spectrum, etc.)
            (e) Message Signature Key (MSK) - Cryptographic material used in a digital signature process.
      (3) The four major categories of use are as follows. Some keys, such as the MSK, may not be provided in a developmental or maintenance form.
            (a) Developmental - This type of key is used early in the development of a cryptodevice or algorithm. Frequently classified and used indefinitely, the distribution of this key shall be limited to test personnel with the need to know.
            (b) Test - This type of key is used for testing where signal radiation is permitted. It is classified IAW the level of classification of the data to be protected and is always assigned a specific period of use.
            (c) Operational - This type of key is used to protect operational data. It is classified to the level of the data which it shall be used to protect and a specified period of use.
            (d) Maintenance - This type of key is used for maintenance of the device or system, as well as early bench or loopback testing. In general, this key must not be used when any signals are transmitted, may be unclassified, and may be allowed an indefinite period of use.
            (e) Other types of key exist (exercise, training, etc.) but shall not concern the contractor.
   b. WHAT YOU MUST PROVIDE TO THE NSA TO GET KEY:
      (1) Key Management Plan - In addition to the design information required for evaluation, the plan shall discuss what keys and key products are required by the device, and suggestions for eventual operational implementation.
      (2) Key Specification
            (a) Specifications shall be as complete as possible, designating and describing all types, uses, formats and media of key to be required by the system. Even if it is not possible to give details of operational key formats at the time the key specification is first written, all key shall at least appear as a “placeholder” to allow the NSA programmer to consider its existence in the overall organization.
of the code. The specification is the interface control document between the contractor and the keying material programmer. If the specification is ambiguous, incomplete, or erroneous, the end product shall reflect those errors. Frequent changes to the code result in a waste of developer resources as well as the danger that code errors will occur. Therefore, the key specification must be complete and correct before NSA can begin to program new keying material.

(b) The programming and production of key in nonstandard formats or using new algorithms shall be validated by known input/output.

(c) The program manager/project engineer should also arrange to have test versions of the key validated with the end equipment or User system to insure the key loads and is used properly.

(3) Key Acquisition Plan - The contractor shall provide development, test, and delivery schedules in conjunction with key requirements. The plan provides details as to dates, types of key needed and program milestones to help forecast key orders.

c. WHEN MUST YOU PROVIDE THE REQUIRED ITEMS AND REQUEST KEY

(1) All of the above items must be provided, reviewed, and approved before NSA can begin to program and/or order any key. Usually, revision and review is an iterative process. The key acquisition process can be a long one and should be begun as soon as the cryptologic component is identified.

(2) For standard key on current standard media only, or key made from existing programming and existing part stock: no less than 90 days before the key is needed. This 90 day time period begins AFTER final approval of a key specification by the NSA.

(3) For new or changed key, new or changed media, or new or changed protective packaging: from 90 days up to two years before the key is needed, depending on the characteristics of the new or changed key.

d. ELECTRONIC KEY POLICY STATEMENT

All new programs shall be designed to support Electronic Key Management. NSTDSSIP No. 4 states “U.S. Government departments and agencies shall establish and implement electronic keying programs with the objective of virtually eliminating, by the year 2000, their dependence on paper-based/electronic keying methods and with a goal of implementing benign keying where appropriate.”

e. MINIMUM REQUIREMENTS FOR A KEY SPECIFICATION

Below are listed the minimum requirements for information that must be provided in a Key Specification. Unique requirements may necessitate that additional information be provided before a particular specification can be approved.

(1) System Architecture

(a) INFOSEC Architecture - Briefly describe the system or equipment in which the key shall be used, identifying the basic key management in general terms.

(b) Environment - Describe the physical and security environment in which this key shall be used.

(c) Classification - State the classification level of the traffic being processed, of the key, of the crypto-equipment both keyed and unkeyed.

(2) Key Architecture
(a) Keys Needed and Relationship - Identify all keys (KEKs, TEKs, etc.) needed. Describe the relationship of the keys to any other keys (A encrypted by B, etc.), the sequence of their use, and any requirement to store in a history file for later use. Diagrams and flow charts are very useful.

(b) Key Functions - Identify all types of key needed (Developmental, test, operational, etc.).

(3) General Requirements

(a) Physical Form - Describe the form of key media to be used (e.g., EPROM, 3.5 inch double-sided, high density floppy disk, etc.). Also state whether any new or different key media will be required in the future (if known) and the approximate date for the requirement (if known). New types of key media must be approved in advance by the NSA. Avoid substantial lead time required to provide key in a new medium by selecting from the NSA Standard Physical Key Media Products List of Preferred Standard Media.

(b) Protective Packaging - Identify any protective packaging that will be required for the keying material. Note that if the key is a new type of media, it may require a new protective packaging technique. If so, the lead time for providing key to the User will increase greatly.

(c) Fill Device Compatibility - Identify the specific fill device to be used to load the key into the equipment. The common fill devices are KOI-18, KYK-13, and KYX-15A. Also, the AN/CYZ-10, Data Transfer Device (DTD), may be used to read and transfer keys of any length.

(d) Other Requirements - Describe any unique factors for supply, support, maintenance, etc., which will influence the design of the key.

(4) Rules for Generation for Plaintext or Underlying Key

(a) Standards - Reference all standards used for this particular application.

(b) Data Format of Key - Specify the overall key length, number of random bits, number and location of parity or checksum bits, identify field names and values within the key, the number of bits or characters per field, and the most and least significant bits. Remember that when specifying values for fields of the key, significant bit is extremely important. Identify which fields will be encrypted.

(c) Constraints - Identify any constraints or exclusions, e.g., random portion of key must not be all zeroes or all ones.

(d) Parity Generation - Identify the parity bits (bit position in key format, overall length, significant bit, etc.) and how they are generated. Describe constraints, e.g., no 0 parity.

(e) Checksum Generation - Identify the checksum field (bit position in key format, overall length, significant bit, etc.) and how it is generated.

(f) Product Configuration - Detail how many keys will be required per medium (e.g., 100 keys per floppy disk) and, if appropriate, number of copies of each key. Describe if special formatting is required.

(g) Required System Data - Provide any equipment or system specific header information.

(h) Key Tags - Identify how the keys will be tagged and if those tags will be encrypted or unencrypted.
(i) Positive Access Control - Describe the Positive Access Control (PAC) utilized, if applicable.

(5) Rules for Encrypting Keys

(a) Algorithm Specification - Reference the algorithm specification (by title, serial number, and date) for any and all algorithms used with the key. If algorithm specification is unpublished or inadequate, provide a logic diagram showing how the algorithm will be implemented, plus additional information as required.

(b) Provide at least two sets of known inputs and expected outputs that should result from the known inputs for the algorithm for a specified key and a given set of initial conditions (e.g., the initial state of the logic). If a fill device will be used, state whether the bits must be negated, reversed, negated and reversed, or nothing.

(c) Standards - Reference all standards used for the particular application.

(d) Identify Input to Encryption Algorithm

(i) Identify sections of the key which will be encrypted (if applicable).

(ii) Identify the algorithm which will be used to perform the encryption and the KEK.

(iii) Identify which bit is the Least Significant Bit (LSB) and which is the Most Significant Bit (MSB), by the convention employed by the algorithm documentation.

(6) Identify products which must be generated at the same time as others, and which must contain exactly the same key bits as others.

(7) Printed Products

(a) Handling Instructions - State the handling constraints. Reference the doctrine issued for this system. NSA needs the doctrine for classification, accounting, and distribution issues involved with the key.

(b) Operating Instructions - Describe from the User’s point of view how the key will be selected from the medium and how loaded into the end INFOSEC equipment.

(c) Provide sample pages of Handling and Operating Instructions.
STANDARD PHYSICAL KEY MEDIA PRODUCTS
LIST OF PREFERRED STANDARD KEY MEDIA

1. ELECTRONIC FORM
   * PROMs (Commercial Grade only):
     DM74S288J - 256 bit (32 x 8)
     82S126/BEA - 1,024 bit (256 x 4)
     DM87S191J - 16,384 bit (2,048 x 8)
     N82S191N - 16,384 bit (2,048 x 8)
   * ULTRAVIOLET EPROMs (UVEEPROMs):
     NMC27C16Q45 - 16 kilobit
     (2,048 x 8) D2764A - 64 kilobit (8,192 x 8)
   * EEPROMs:
     DQ2864-300 - 64 kilobit (8,192 x 8)
     Key Storage Device KSD-64-A
     DATAKEY - 64K (8,192 x 8)

NOTE: The parts for the above integrated circuit-type media are currently in the NSA stock system. Any other
parts which are supported by the DATA I/O Corporation, Model 29B Programmer with version 17 firmware, can
be programmed but will require longer lead times for the software development and purchasing.

2. CARTRIDGE MEDIA
   * DC-600 - 9 track, 50+ megabytes (IAW Industry standard QIC-24
     physical format. Data interpreted per NSA Standard Cartridge System.

3. DISK MEDIA
   * 5-1/4 inch - 40 track; 9 sector double sided double density (DSDD)
     MS/PC DOS format, 360 kilobyte.
   * 3-1/2 inch - 80 track, 9 sector double sided double density (DSDD) MS/PC DOS format,
     720 kilobyte.
   * 3-1/2 inch - 80 track, 18 sector double sided high density (DSHD) MS/PC DOS format,
     1.44 megabyte.

4. MAGNETIC TAPE
   * ANSI STD X3.39, 1600 Bits Per Inch, 9 track.

5. MICROPROCESSOR BASED
   * SMART KEY - ULTRON, red key fill device.
   * SMART CARD - Microcard, 64 kilobyte, EPROM type.

6. PAPER TAPE (in canister)
   * Punched Standard Hole (8-level)
     * Printed Key List

Additional information concerning the various standard media may be obtained from NSA.
APPENDIX A

CONTRACT DATA REQUIREMENTS LIST

1. Applicable technical data named in this Contract Data Requirements List (CDRL) must be prepared and delivered to the NSA by the contractor, as part of the product/system and security-evaluation process. Delivery requirements are stated in the individual CDRLs. Satisfactory data submissions are required for NSA approval of the one particular product/system named in the User Partnership Agreement (UPA).

2. Each Data Item Number identifies the Quantity, Delivery Schedule and the Media of the data that must be delivered. The Telecommunications Security Requirements Document (TSRD) describes the requirements in detail.

3. Preparation and format of all data may be IAW best commercial practice; however, the technical requirements of the data must be satisfied. Certain other forms of data submission (such as that used to satisfy Data Item Descriptions, used for Government contracts) are acceptable, providing that the technical requirements of the data are satisfied.

4. All transmittal letters must be sent to the Business Manager of the NSA’s Program Management Office.

5. The NSA will notify the Partner of acceptable documentation. For the certification program to continue, the contractor must resubmit corrected/updated documentation to the Partner within ten days after receipt of Contractor notification, unless otherwise stated in the notification.

6. Questions pertaining to this CDRL and/or particular items should be directed to the NSA’s Program Manager named below.

Approved by: ____________________________  Date: _________________

Program Manager Name: ____________________________

Organization/Phone Number: ____________________________
GENERAL REQUIREMENTS

All deliverables shall be submitted electronically.

Applications/Formats:

All deliverables, unless otherwise specified, shall be prepared using Microsoft Word. Other acceptable applications/formats, listed below in the preferred order, include:

- ASCII Format
- Rich Text Format (RTF)
- Frame Maker

Media:

Engineering Drawings shall be delivered in Initial Graphic Exchange Specification (IGES) format on a Standard CD-ROM.

Configuration Control Documentation shall be delivered in C1 Raster format on a Standard CD-ROM or 3.5" HD Disk.

ALL Other Deliverables shall be delivered as follows:

1) Deliverables comprised predominantly of text/numbers shall be delivered on a Standard CD-ROM or 3.5" HD Disk. 2) Deliverables comprised predominantly of graphics, an equal mixture of text and graphics, shall be delivered on a Standard CD-ROM or 3.5" HD Disk. 3) Custom Integrated Circuit Design Validation Data deliverables shall be delivered on a Standard CD-ROM, 8mm Helical Scan Tape OR 4mm Digital Audio Tape (listed in order of preference). Magnetic Tape shall only be used as the media of last resort.

Miscellaneous:

Classified, restricted or proprietary information shall be isolated, by category, and submitted on separate media.

NSTISSI 4000, INFOSEC Maintenance and Maintenance Training applies if the equipment is going to be maintained.

NSTISSP 300, National Policy on Control of Compromising Emanations applies when required by User.

Appropriate National policy applies for TEMPEST Requirements.
## CONTRACT DATA REQUIREMENTS LIST

<table>
<thead>
<tr>
<th>Data Item Number</th>
<th>Title</th>
<th>TSRD Paragraph</th>
<th>Minimum Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>UP01</td>
<td>Contractor’s Target Program Status Report</td>
<td>23</td>
<td>NSA</td>
</tr>
<tr>
<td>UP02</td>
<td>Fail Safe Design and Analysis (FSDA) Documentation</td>
<td>16</td>
<td>NSA</td>
</tr>
<tr>
<td>UP03</td>
<td>Theory of Design &amp; Operation (TDO) Documentation</td>
<td>12</td>
<td>NSA</td>
</tr>
<tr>
<td>UP04</td>
<td>Theory of Compliance (TOC) Documentation</td>
<td>13</td>
<td>NSA</td>
</tr>
<tr>
<td>UP05</td>
<td>Security Verification (SV) Plan &amp; Procedures</td>
<td>17</td>
<td>NSA</td>
</tr>
<tr>
<td>UP06</td>
<td>TEMPEST Control Plan</td>
<td>24.a)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP07</td>
<td>TEMPEST Test Plan</td>
<td>24.b)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP08</td>
<td>TEMPEST Test Report</td>
<td>24.c)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP09</td>
<td>Configuration Control Documentation</td>
<td>19</td>
<td>NSA</td>
</tr>
<tr>
<td>UP10</td>
<td>Engineering Drawings, Software and Configuration Item Database</td>
<td>20</td>
<td>NSA</td>
</tr>
<tr>
<td>UP11</td>
<td>Configuration Audit Plan &amp; Report</td>
<td>21</td>
<td>NSA</td>
</tr>
<tr>
<td>UP12</td>
<td>In-Process Accounting Procedures Documentation</td>
<td>18</td>
<td>NSA</td>
</tr>
<tr>
<td>UP13</td>
<td>Key Management Plan</td>
<td>15.a)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP14</td>
<td>Interface &amp; Operators Guide</td>
<td>26</td>
<td>NSA</td>
</tr>
<tr>
<td>UP15</td>
<td>INFOSEC Security Awareness Training</td>
<td>27</td>
<td>NSA</td>
</tr>
<tr>
<td>UP16</td>
<td>Maintenance Manuals</td>
<td>28</td>
<td>NSA</td>
</tr>
<tr>
<td>UP17</td>
<td>Security Production Assurance</td>
<td>29</td>
<td>NSA</td>
</tr>
<tr>
<td>UP18</td>
<td>Software Requirements Specification</td>
<td>22.b)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP19</td>
<td>Software Test Plan</td>
<td>22.c)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP20</td>
<td>Software Test Report</td>
<td>22.d)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP21</td>
<td>Software Development Plan</td>
<td>22.g)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP22</td>
<td>Software Product Specification</td>
<td>22.e)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP23</td>
<td>Software Test Description</td>
<td>22.i)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP24</td>
<td>Software Design Description</td>
<td>22.h)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP25</td>
<td>Software Version Description</td>
<td>22.f)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP26</td>
<td>Integrated Circuit Graphics Database</td>
<td>31.a)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP27</td>
<td>Computer Aided Chip Development Data</td>
<td>31.b)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP28</td>
<td>Computer Aided Cell Development Data</td>
<td>31.c)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP29</td>
<td>Key Specification</td>
<td>15.b)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP30</td>
<td>FPGA Documentation/Artifacts</td>
<td>32</td>
<td>NSA</td>
</tr>
<tr>
<td>UP31</td>
<td>System Subsystem Specification (SSS)</td>
<td>22.a)</td>
<td>NSA</td>
</tr>
<tr>
<td>UP32</td>
<td>Security Verification Test Report</td>
<td>17</td>
<td>NSA</td>
</tr>
<tr>
<td>UP33</td>
<td>Covert Channel Analysis</td>
<td>14</td>
<td>NSA</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

## SECTION 1 - INTRODUCTION
1. Purpose.......................................................... 1
2. General Description of Product/System.......................... 1
3. Applicable Documents............................................. 2
   a) User Partnership Agreement.................................. 2
   b) Telecommunications Security Requirements Document........ 2
   c) Contract Data Requirements List.............................. 2
   d) Unified INFOSEC Criteria (UIC).............................. 2

## SECTION 2 - GENERAL REQUIREMENTS
4. Software Products................................................. 3
   a) Software Virus Certification................................... 3
   b) Malicious Code Prevention Certification..................... 3
   c) Software Product Deliverables................................. 3
5. INFOSEC-Boundary.................................................. 3
6. Marking.................................................................... 4
   a) Marking of Modules, Printed Wiring Assemblies (PWAs), or Hybrids 4
   b) Marking of the End-Item........................................... 4
   c) Marking of Documentation Submitted............................ 5
   d) Marking of Resubmitted Documentation.......................... 5
   e) Bar Code Marking................................................. 5
7. Warranty Coverage.................................................... 6
8. Maintenance/Training................................................ 6
9. World-Wide Power Considerations.................................. 7
10. Nuclear Survivability/Vulnerability................................. 7
11. Acquisition of INFOSEC Equipment, Software, Components, and Parts Outside of the United States........... 7

## SECTION 3 - SECURITY & TECHNICAL REQUIREMENTS
13. Theory of Compliance (TOC) Documentation........................ 9
14. Covert Channel Analysis............................................ 9
15. Key Management Plan and Key Specification...................... 9
   a) Key Management Plan (KMP)..................................... 9
   b) Key Specification.................................................. 15
16. Fail Safe Design and Analysis (FSDA) Documentation............. 15
17. Security Verification (SV) Plan & Reports........................ 16
18. In-Process Accounting Procedures Documentation................. 16
19. Configuration Control Documentation................................ 16
20. Engineering Drawings, Software and Configuration Item (CI) Database........................................ 17
21. Physical Configuration Audit (CA) Plan and Report.............. 18
22. Software.................................................................. 19
   a) System Subsystem Specification (SSS)............................ 19
   b) Software Requirements Specification (SRS).................... 19
   c) Software Test Plan (STP).......................................... 20
   d) Software Test Report (STR)....................................... 20
   e) Software Products Specification (SPS).......................... 20
   f) Software Version Description (SVD)............................ 20
   g) Software Development Plan (SDP)............................... 20
   h) Software Design Description (SDD)............................. 21
   i) Software Test Description (STD)................................. 21

## SECTION 4 - ADDITIONAL REQUIREMENTS
23. Contractor's Target Program Status Report........................ 22
24. TEMPEST Documentation............................................ 22
<table>
<thead>
<tr>
<th>Section Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) TEMPEST Control Plan</td>
<td>22</td>
</tr>
<tr>
<td>b) TEMPEST Test Plan</td>
<td>23</td>
</tr>
<tr>
<td>c) TEMPEST Test Report</td>
<td>23</td>
</tr>
<tr>
<td>25. Anti-Tamper Protection Requirements</td>
<td>23</td>
</tr>
<tr>
<td>27. INFOSEC Security Awareness Training</td>
<td>25</td>
</tr>
<tr>
<td>28. Maintenance Manuals</td>
<td>26</td>
</tr>
<tr>
<td>29. Security Production Assurance (SPA)</td>
<td>26</td>
</tr>
<tr>
<td>30. INFOSEC-Boundary Verification Test (IVT)</td>
<td>27</td>
</tr>
<tr>
<td>31. Custom Integrated Circuit Design Validation</td>
<td>29</td>
</tr>
<tr>
<td>a) Integrated Circuit Graphics Database</td>
<td>29</td>
</tr>
<tr>
<td>b) Computer Aided Chip Development Data</td>
<td>29</td>
</tr>
<tr>
<td>c) Computer Aided Cell Development Data</td>
<td>29</td>
</tr>
<tr>
<td>32. Field Programmable Gate Array (FPGA) Documentation</td>
<td>30</td>
</tr>
<tr>
<td>SECTION 5 - CONTRACTOR GUIDELINES FOR ACQUIRING KEYING MATERIAL</td>
<td>31</td>
</tr>
<tr>
<td>33. Guidelines For Obtaining Key</td>
<td>31</td>
</tr>
<tr>
<td>APPENDIX A</td>
<td>36</td>
</tr>
</tbody>
</table>
NATIONAL SECURITY AGENCY
TELECOMMUNICATIONS SECURITY REQUIREMENTS DOCUMENT (TSRD)
for the
MINUTEMAN MINIMUM ESSENTIAL EMERGENCY COMMUNICATIONS
NETWORK (MEECN) PROGRAM UPGRADE (MMP-U) INITIATIVE

SECTION 1 - INTRODUCTION

1. **Purpose.**
This document provides detailed descriptions of the requirements necessary for approval for use of
the product/system named above, under the terms and conditions of the User Partnership Program
(UPP). These requirements have been separated into two sections. Section 3 contains the essential
security related requirements that are applicable for every UPP program. Section 4 contains
additional security related requirements for a product system that is designed and developed to meet
Information Assurance Directorate (IAD) specific cryptographic requirements.

2. **General Description of Product/System.**
The mission of the MMP terminals is to provide a high-confidence, survivable link for reception of
Emergency Action Messages (EAM) from the President and Secretary of Defense, the Joint Chiefs of
Staff (JCS), and the Commander, United States Strategic Command (CDR USSTRATCOM) to
the Intercontinental Ballistic Missile (ICBM) Launch Control Centers (LCCs) as well as a
survivable force report-back capability supporting the Nuclear Execution and Reporting Plan
(NEREP) process and STRATCOM generated Force Direction and Force Management messages.
Survivable communications are key elements of our deterrence strategy because potential
adversaries must be convinced that launch orders will actually be received by the LCCs and our
communications, both received and transmit, will not be easily disrupted.

The MMP Upgrade program will replace the existing Extremely High Frequency (EHF) Low Data
Rate (LDR) function of the existing MMP terminals with LDR and Extended Data Rate (XDR)
functions capable of operating on any JCS EHF MILSATCOM system. The Advanced Extremely
High Frequency Data Rate (AEHF) satellite constellation is the second increment of the planned
Department of Defense (DoD) implementation of JCS EHF communications systems which will
provided a dramatic increase in throughput capability. The upgrade MMP will be fielded to provide
operational terminals, training, test, and maintenance beginning in 2010, to ensure MMP users take
advantage of AEHF throughput enhancements.

The MMP Upgrade program intends to increase flexibility of the upgraded MMP products, by
providing an architecture that can be modified or extended to incorporate technology and capability
upgrades. To this end the MMP Upgrade terminal has a requirement for Software Communications
Architecture (SCA) compliance, and an objective requirement to provide a functional layered
architecture for the EHF/AEHF capability. This will allow the Government to minimize life cycle
costs and training costs, and enhance supportability. Such a layered approach will facilitate upgrades
through application of common, open, and exposed (or exposable) interfaces with minimum impact over the life of the terminal.

3. **Applicable Documents.**

The product/system shall be produced by the User's contractor in accordance with (IAW) the requirements of the NSA/User Partnership Agreement (UPA), including this Telecommunications Security Requirements Document, its corresponding Contract Data Requirements List (CDRL), and the Unified Information Security (INFOSEC) Criteria (UIC).

   a) **User Partnership Agreement.**

   The UPA apprises the User and its contractor of the specific security and product/system related requirements which must be met before the NSA will certify the product/system for operational use.

   b) **Telecommunications Security Requirements Document.**

   The TSRD describes the requirements applicable to the INFOSEC- Boundary components and all associated hardware, software and firmware under development. This includes:

   1. Introduction
   2. General Requirements
   3. Security & Technical Requirements
   4. Additional Requirements
   5. Contractor Guidelines For Acquiring Keying Material

   c) **Contract Data Requirements List.**

   The CDRL identifies specific types and quantities of technical data necessary for the NSA to evaluate and subsequently certify the product/system, and subsequently manage changes incorporated into the hardware/software throughout the program life cycle. The description of each CDRL includes the point in time during the development and production schedule that the NSA needs the data.

   d) **Unified INFOSEC Criteria (UIC).**

   The UIC describes the security requirements of the product/system.
SECTION 2 - GENERAL REQUIREMENTS

4. Software Products
   a) Software Virus Certification
      The contractor certifies that, to the best of its knowledge and belief, software provided under this TSRD and the software development environment, does not contain any viruses and has undergone virus scan using the latest approved scanner of known viruses which could damage, destroy, or alter software, firmware, or hardware, or which could reveal any data or other information accessed through or processed by the software. Further, the contractor shall immediately inform the NSA upon reasonable suspicion that any software provided hereunder may cause the harm described above.

   b) Malicious Code Prevention Certification.
      The contractor certifies that, to the best of its knowledge and belief, software provided under this TSRD does not contain any malicious code, program, or other internal component (e.g., computer virus) which could damage, destroy, or alter software, firmware, or hardware, or which could reveal any data or other information accessed through or processed by the software. The contractor certifies that controls and processes are in place such that the software development environment and programmers are deterred from inserting such. The contractor Software Development Plan shall delineate the components, controls, and processes to prevent such cases. Further, the contractor shall immediately inform the NSA upon reasonable suspicion that any software provided hereunder may cause the harm described above.

   c) Software Product Deliverables.

5. INFOSEC-Boundary
   The INFOSEC-Boundary encompasses those portions of the product/system (e.g., chips, hybrids, PWAs, modules, subassemblies, components, fill port(s), control/zeroize functions, signal and power line filters and buffers, related software, etc.) which perform or implement the security-related functions specified in this TSRD. The INFOSEC-Boundary, to include both hardware and software, shall be captured, and the configuration item (CI) drawings baselined, by the performance of a Physical Configuration Audit (PCA) IAW the PCA Plan specified in this TSRD. The contractor is responsible for identifying those CIs comprising the INFOSEC-Boundary, for controlling changes to those CIs and the INFOSEC-Boundary, and for identifying and marking these CIs.
6. Marking
(See NSTISSI 4001). All custom parts, subassemblies, and assemblies within the INFOSEC-Boundary must be conspicuously marked and identified by the contractor with NSA-furnished zero-N (0N) part numbers. (These are part numbers that have a “0N” prefix.) The NSA will provide a series of “0N” part numbers to the contractor. The contractors five-digit Commercial and Government Entity (CAGE), as shown in the CAGE H4-Series Handbook, may be included on INFOSEC-Boundary hardware. In that case, the NSA’s identification numbers must be included as suffixes to the contractors CAGE-code. However, if limited marking space is available, the NSA marking must take precedence over any other markings.

a) Marking of Modules, Printed Wiring Assemblies (PWAs), or Hybrids
In all cases wherein NSA markings are required, the contractors markings are also permitted. However, if space is limited allowing only one set of markings, the NSA’s marking requirements must take precedence. The NSA will provide a block of “0N” numbers for the contractor to assign to modules, PWAs, and hybrids, as appropriate.

(1) All modules, PWAs, or hybrids within the INFOSEC-Boundary must be conspicuously marked with identifiers pursuant to the sections below, the trademark of the contractor, and, space permitting, the part number selected by the contractor.
(2) The identifiers for a CCI module shall be as follows: a Trigraph (as appropriate for modules), “0N” number and the designator “Controlled Cryptographic Item” or “CCI”. The module’s markings shall be readily visible to allow identification at the level of intended use.

(3) The identifiers for a CCI PWA shall be as follows: a Trigraph (such as E-ABC), “0N” number and the designator “Controlled Cryptographic Item”, or “CCI”.
(4) The identifiers for a CCI hybrid shall be as follows: a Trigraph (such as U-ABC), “0N” number and the designator “Controlled Cryptographic Item”, or “CCI”.
(5) The CCI module’s, PWA’s, or hybrid’s designators shall be permanently affixed to a location on the module, PWA, or hybrid, respectively.

b) Marking of the End-Item.
(1) All NSA-certified product/system(s) containing modules, PWAs, or hybrids shall conspicuously bear the designator “Controlled Cryptographic Item” (in plain view), an identifier pursuant to the sections below, a serial number assigned by the NSA, the trademark of the contractor, and the model number selected by the contractor. In addition, all endorsed cryptographic items sold to U.S. Government entities must contain a Universal Identifier (UID) label/plate (see e. (2) below).

(2) The identifier for a product/system containing NSA-certified cryptographic algorithm shall be the product/system's name or short title of the product/system's name followed by a space and then “(EC)” (Endorsed for Classified Traffic) in parenthesis (i.e., MX300S (EC)). Where a product/system consists of two or more sections not contained in a single enclosure, each section must have separate identifiers. If an implementation of the NSA algorithm is a retrofit to a previous product/system containing the DES module, then the CCI designator, the (EC) identifier, and the serial number assigned by the NSA
shall be affixed to the product/system. The new label/plate shall be included in the upgrade kit with installation instructions.

(3) All required markings/plates shall be permanently affixed to the product/system.

(4) The Controlled Cryptographic Item (CCI) designator, the "(EC)" identifier, and the serial number assigned by the NSA shall be in a size of type large enough to be readily legible, consistent with the dimensions of the product/system and their nameplates.

c) **Marking of Documentation Submitted.**

All documentation submitted for evaluation must be clearly and completely identified. Include the CDRL sequence number, contractors name, address, and point of contact; contract/UPA number; name of project and/or product/system; classification of project; date of submittal; revision level of documentation; "ON" number(s), if assigned; name and designator of NSA program manager; and other data deemed appropriate by the contractor. Additional identification requirements, if any, are stated elsewhere in this requirements document, as appropriate.

d) **Marking of Resubmitted Documentation.**

Plans and reports that are resubmitted for evaluation shall include a Revision Status page indicating the revision level of each page contained in the re-submission. Additionally, the individual changes on each page shall be highlighted. (e.g., use change-bar symbols, underlining, asterisks, bold or emphasized print, or similar marking). *Do not highlight changes on engineering drawings.*

e) **Bar Code Marking.**

Unless otherwise specified in the UPA, nameplates, printed wiring assemblies, and shipping containers are subject to the following bar code marking requirements using Standard DoD Bar Coding Symbology (SDS) IAW MIL-STD-1189 and NSA-2:

1. **Nameplates.** Bar code symbology printed on nameplates shall contain, as a minimum, the short title, the sequential serial number assigned by the Government, and National Stock Number (NSN).

2. **UID plates.** Plates or permanent labels containing a UID bar code IAW the DoD Policy that was articulated in Office of the Secretary of Defense Memorandum of August 16, 2002, SUBJECT: Universal Identifier Code, as well as any and all subsequent DoD issuances implementing and clarifying the original policy, shall be affixed permanently to the outside of the device. These plates/labels shall be affixed in a manner consistent with the marking requirements of the aforementioned DoD policies; the most current version of MIL-STD-130 available (MIL-STD-130L at the time of this writing); NSA-2J; and any subsequent DoD and/or NSA policies issued or updated after publication of this TSRD. Plates/labels shall be affixed in a position visible when the device is in normal use, and shall have a life at least equal to the life of the device/part itself. The data to be encoded in the UID, as well as its format, shall be as specified in the various DoD policy documents, as well as any NSA policy documents that may be issued after publication of this TSRD.

Information concerning this DoD policy, as well as copies of all the applicable DoD policies, are found on the web site of the Office of the Undersecretary of Defense for

(3) **CCI Printed Wiring Assemblies.** The bar code message shall contain only the short title (nomenclature) and NSN.

(4) **Shipping Containers.** Bar code symbols shall be placed on the exterior of shipping containers of end items and shall include: sequential serial number assigned by the Government, the NSN, if applicable, and the contract/UPA number. If more than one end item will be packed in a shipping container, the unit of issue and the quantity shall also be included. Where the symbol width must be reduced, the "stacking procedure" is preferred. The clear-text message shall be printed adjacent to the bar code. Depot level repair part shipping containers shall also be bar coded; except that the word "spares" shall be used in lieu of serial numbers.

7. **Warranty Coverage.**
Manufacturers shall provide information on guarantees and other warranty coverage for their product/systems to their customers. Basic warranty coverage shall either be for 5-years minimum, or may consist of a shorter initial warranty that can be extended by the customer to 5-years minimum through the purchase of an extended warranty. The NSA requires the contractor to provide warranty coverage for the INFOSEC-Boundary components to the same extent provided for the product/system as a whole. It is also expected that the warranty coverage offered by other contractors to the contractor shall be extended to the contractors authorized Users. Additionally, if repair authority is given to the User, an impact statement as to the effect on warranty must be provided.

*Warranties should only be required if these are COTS products or the procuring activity has requested warranties for the non/INFOSEC-Boundary components of the equipment/system.*

8. **Maintenance/Training.**
Maintenance concept and training plan to support the product/system shall be addressed by the contractor. These issues include, but are not limited to,

- Support plans and training plans – these shall be submitted to the NSA/PMO for approval prior to certification.
- Users operating manual – a copy of the manual must be submitted and approved by the NSA/PMO prior to certification and then an approved copy included with each piece of equipment.
- All technical documents (maintenance information, user manuals, etc.) shall conform to the international specification ASD/AIA/S1000D (commonly referred to as "Spec S1000D"). Information on S1000D, as well as a downloadable copy of the specification, can be found on this group's web site at http://www.s1000d.org/ Such documents should be available in both hard- and soft-copy formats (the latter in .pdf, html, and .xml at a minimum).
- Manufacturers are encouraged to make available for sale to users any necessary documentation, manuals, and training that would permit users to perform some level of maintenance and repair that extends beyond basic troubleshooting (e.g. more than battery
changing, determining if power is on, etc.). Such maintenance and repair troubleshooting is ideally accomplished utilizing only standard, commercially available, automated test equipment. If any specialized tools or proprietary test equipment are required for maintaining or repairing user-serviceable functions then the manufacturer is also encouraged to make those available for sale to users, or to provide the necessary contact information to allow the direct purchase of these items by the user. It is assumed that all such maintenance and repairs, when authorized by the manufacturer and subsequently performed by trained and qualified technicians in a manner consistent with the manufacturer's documentation and instructions, would not void any basic or extended warranty.

Electronic equipment when connected to world-wide power sources can encounter a considerable range of AC voltages, frequencies, stability, safety, and interconnection configurations. It is important, therefore, that care be taken during CCEP power supply design to ensure that the aforementioned areas are given proper consideration, and that the equipment remains usable and functioning in the presence of such variations (within the ranges or limits specified by the PM).

The concept of Nuclear Survivability shall be included in any INFOSEC equipment used or developed for use in military Command, Control, Communications, and Intelligence (C2I) systems and/or military weapons systems. The contractor is CAUTIONED to properly coordinate with the User to implement this protection, as required by the User, into equipments produced under UPP programs.

11. Acquisition of INFOSEC Equipment, Software, Components, and Parts Outside of the United States.
INFOSEC equipment is uniquely sensitive, requiring specific procedures to ensure security. The cryptographic principles, technology, and critical design features employed in INFOSEC equipment must be carefully protected. Therefore, the acquisition of INFOSEC equipment, components, or parts outside of the United States is prohibited without written approval from NSA. This prohibition includes design, manufacture, production, assembly, inspection or test in a location not in the United States, of equipment, assemblies, subassemblies, accessories, or parts, which are not covered by a Government specification or standard. Standard off-the-shelf parts do not require approval. If, at a later date, the production, assembly, inspection, or testing of the equipment, software, components, or parts is moved outside the United States, then the device immediately loses NSA certification.

Exceptions to the above policy will be handled by NSA on a case-by-case basis. When an exception is granted, it is understood that the contractor may be required to perform a security evaluation on a random sampling of parts to include an external visual, internal visual and die comparison against a reference photo in order to maintain certification. The NSA will determine the percentage of parts that must be sampled and passed to maintain certification. An x-ray analysis may be required in some cases. Additionally, the contractor agrees to maintain anonymity to the Government. Information identifying the Government as the intended recipient or the intended use of the components or parts shall not be sent offshore. This includes drawings, purchase orders, or part markings which reference NSA or that are unique to NSA.
In addition, the utilization of Commercial-Off-The-Shelf (COTS) software as an integral part of the INFOSEC or security boundary poses additional cryptographic and security issues. The use of uncleared individuals and/or foreign nationals as software developers must be limited in the development of security related software in compliance with the following excerpt from the Director of Central Intelligence Directive 6/3, which states:

"Protected Hardware, Software and Firmware – Uncleared personnel developing hardware, firmware, software or data files shall not, to the maximum extent possible, have any knowledge that the software, hardware, firmware or data files will be used in a classified area. Before hardware, firmware, software or data files that are developed or modified by uncleared personnel can be used in a classified processing period, appropriately cleared, technically knowledgeable personnel shall review them to ensure that no security vulnerabilities or malicious code exist. Software, hardware and firmware used for maintenance or diagnostics shall be maintained within the secure computing facility and even though unclassified, shall be separately controlled.” Note that the NSA considers the reference to “uncleared personnel” in the above paragraph to include “foreign nationals” in any and all instances. In addition, the “appropriately-cleared, technically-knowledgable personnel” referred to that perform the review shall not include foreign nationals, even if cleared. Exceptions to this policy MUST be approved by NSA.
SECTION 3 - SECURITY & TECHNICAL REQUIREMENTS

The TDO is divided into four chapters. The first chapter describes the top level requirements of the system, the system’s operational environment, and the top level security of the system. The second chapter breaks the system down into functional blocks. The third chapter describes the physical configuration of the system and where each function described in chapter 2 is performed. The fourth chapter identifies the design features of the system which satisfy each security requirement and goal. The TDO addresses by section and by requirement, but in a general nature, all of the Requirements Specifications and goals in the NSA-provided UIC that the developer’s product/system will meet. It also includes a more detailed discussion and justification of those requirements and goals in the UIC that the system will not meet. This section should not contain a restatement of the requirements and goals in the UIC, but instead it should reference them by UIC section title and number within the respective section. Format is per Data Item Description (DID) DI-MISC-81608, Theory of Design & Operation (TDO), and delivery requirements are described in CDRL UP03.

The Theory of Compliance 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) This section should not contain a restatement of the requirements and goals in the UIC, but instead it should reference them by UIC section title and number within the respective section. The Software Requirements Specification, by mapping to the UIC, shows down to the unit/component level (file level) where the security requirements are implemented. Format is per DID DI-MISC-81609, Theory of Compliance (TOC), and delivery requirements are described in CDRL UP04.

14. Covert Channel Analysis
The Covert Channel Analysis Report documents the results of a covert channel analysis on a trusted computing base (TCB). Format is per DID DI-MISC-81345, Covert Channel Analysis Report, and delivery requirements are described in CDRL UP33.

The contractor is required to prepare and submit to the NSA for approval, a Key Management Plan and a Key Specification IAW the following paragraphs. The final Key Management Plan and Key Specification must be approved by the NSA prior to product/system approval for use.

a) Key Management Plan (KMP).
The KMP is the document that describes the management of all key management products and services used by a cryptographic application (cryptographic engine, End Cryptographic Unit (ECU), or system as defined below) throughout its lifetime. The KMP documents the capabilities that the cryptographic application requires from the current and planned Key Management Infrastructure (KMI). This ensures that any lifecycle key management services are supportable by and available from the KMI in a timely manner. Refer to IAD
Regulation No. 25-6, Key Management Planning, for the policy regarding KMPs. Format is per DID DI-MISC-90019B, Key Management Plan, and delivery requirements are described in CDRL UP13. A cryptographic application refers to either a cryptographic engine, ECU, or system. These are defined as:

- **Cryptographic engine**: a device that performs cryptographic functionality; it may be implemented in either a chip or module
- **ECU**: the lowest level hardware unit containing cryptographic functionality that must be serviced by the KMI; it is the host assembly that embeds a cryptographic engine
- **System**: two or more cryptographic applications integrated into an architecture to provide a specific set of security services

The KMP described in this document uses an incremental three-step process. This will allow early insight into the development of a cryptographic application and its key management requirements to assess compatibility with the current and planned KMI. The three-step process includes the KMP1, **Cryptographic Application Description and Security Services** document (delivered during the preliminary design phase), the KMP2, **Key Management Products And Services Requirements** document (delivered during the preliminary design phase), and the KMP3, **Total Key Management Plan** (delivered during the critical design phase). However, depending on the type of cryptographic application whether the KMP is being written for an ECU, a cryptographic engine or at the system level and where it is in the development cycle, tailoring of the process can be arranged between the NSA KMP Advocate and PMO.

The KMP that is developed for an ECU must be written IAW Paragraph 13a(1). The NSA KMP Advocate assigned to support the development of the ECU-level KMP and the PMO will determine if tailoring the KMP process is appropriate, depending on where the ECU is in the development cycle.

When developing a KMP for a cryptographic engine, the unique key management products and services needed from the KMI to support the operation of cryptographic engine need to be defined. *(EXCEPTION: A cryptographic engine that is developed specifically to be embedded into a single ECU with no other planned applications can be addressed by the ECU or System KMP.)* The NSA KMP advocate assigned to support the development of a cryptographic engine KMP and the PMO will determine the required content. The checklist provided in Attachment A will be used to document information about the cryptographic engine development to assist in determining if tailoring of the KMP process is appropriate.

The system KMP builds upon the engine- or ECU-level KMPs and is written to address specific operational key management products and services requirements. If an engine or ECU used by a system is not certified, an engine- or ECU-level KMP must be written. *(EXCEPTION: An engine or ECU that is developed specifically to be integrated into a single system with no other planned applications can be addressed by the system KMP.)* The system KMP would look at the requirements and impacts for the delivery of key management products and services to a system, with particular attention given to any intermediate storage and handling requirements before loading into the engines and/or ECUs. The NSA KMP Advocate assigned to support the development of the system KMP and the PMO will determine if tailoring the KMP process is appropriate. During these
discussions between the KMP Advocate and the PMO, it may be determined that KMP section content as described in Section 13a(1), may be modified and the extent of these modifications to support the development of the system KMP.

(1) Content
The level of detail required for each section of the KMP can be tailored, depending upon whether the KMP is being written for a cryptographic engine, ECU, or at the system level. The KMP will contain a title page that includes the program name, program manager's name and telephone number, the NSA PMO, and OPR-assigned KMP number. A revision page, list of reference documents, table of contents, and definition of abbreviations and acronyms page will also be included. The information contained in a KMP will have appropriate classification markings, IAW service or agency-specific policies. Terminology used in a KMP will be IAW the National INFOSEC Glossary (NSTISSI 4009). The KMP will not contain proprietary information. The following are the required sections that must be addressed in each KMP submission:

- KMP1, the **Cryptographic Application Description and Security Services** document provides a description of the cryptographic application functionality, background, and secure communication requirements. The following sections are required for KMP1:
  - Cryptographic Application Description and Background
  - Communications Environment (include allied interoperability requirements)

- KMP2, the **Key Management Products and Services Requirements** document, includes the key management products and services requirements, and the revised KMP1 submission reflecting formal comments and recommendations received during the KMP1 review process. The following section is required for KMP2:
  - Key Management Products and Services Requirements (include use of benign techniques or documented waiver)

- KMP3, the **Total Key Management Plan**, folds in KMP1 and KMP2 and the associated comments and recommendations received during the KMP2 review process. The following sections are required for KMP3:
  - Key Management Products and Services Ordering
  - Key Management Products and Services Generation
  - Key Management Products and Services Distribution
  - Key Management Products and Services Storage
  - Access Control
  - Accounting
  - Compromise Management and Recovery
  - Key Recovery

**NOTE:** If the cryptographic application is supported by EKMS, a statement to that effect shall be included in the appropriate KMP section below.
(a) **Cryptographic Application Description and Background** - This section provides a brief description of the cryptographic application, including the purpose of the cryptographic application, and whether it is a new cryptographic application, a modification of an existing cryptographic application, or an existing cryptographic application that has never had a KMP approved. Background information describing who initiated the cryptographic application, why, and future upgrade capabilities, if applicable, must be provided. The level of information that the cryptographic application is protecting (Type 0, Type 1, Type 2) must also be discussed. A brief description of the security services (confidentiality, integrity, non-repudiation, access control, identification and authentication, and availability) the cryptographic application provides must be included. Information concerning long-term and potential interim key management support (operational, test, contingency, maintenance key management products and services) for the cryptographic application must also be provided.

(b) **Communications Environment** - This section provides a brief description of the communications environment, distinguishing between secured and unsecured communications, in which the cryptographic application is expected to operate. Some examples of communications environments include:

- Data network (internet, NIPRNET, SIPRNET)
- Wired communication (telephone)
- Wireless communication (satellite, radio frequency)

If the cryptographic application plans to communicate with allies, an overall strategy for achieving allied interoperability must be included. If allied interoperability is not required, an explanation must be provided. A figure that illustrates the communications environment and supporting text must be included in this section.

(c) **Key Management Products and Services Requirements** - This section, along with the revised KMP1, comprises the KMP2 submission. The key management products and services requirements describe the types, quantities, cryptoperiod (lifetime), algorithms, and additional information that define the cryptographic application's requirements for key management products and services. A description of the cryptographic application's use of benign techniques must also be included. If the cryptographic application is not using benign techniques, a waiver must be submitted with an acceptable justification IAW the IAD Policy #17, and referenced in the KMP.

Cryptographic applications using public key certificates (often called "X.509 certificates") shall describe the class of certificates, and whether certificates and tokens already issued to subscribers will be used for the cryptographic application, or whether the cryptographic application will require additional certificates and tokens. If additional certificates and tokens are required, the KMP shall describe a rough order of magnitude of the quantity of required certificates. If "standard" certificates and tokens already issued (or planned
to be issued) by the KMI are adequate for the cryptographic application described in the KMP, then the KMP shall so state. Otherwise, any new or additional certificate or tokens features (e.g., new certificate extensions or formats) shall be described in the KMP.

The cryptographic application's key management products and services requirements information must be included in table format. The following information must be included in the table:

- Key management products and services types (keys, certificates, tokens for each type: 0, 1, 2, operational, test, contingency, maintenance)
- Key management products and services quantity (per ECU to be keyed)
- Projected quantity of ECUs
- Key management products and services algorithm
- Key management products and services format (reference existing Key Specification if known)
- Cryptoperiods
- Key management products and services classification levels
- PKI certificate classes (class 3, 4, 5)
- Tokens
- Need dates (for operational, test, contingency, and maintenance)
- Projected duration of need
- Anticipated Controlling Authority

(d) **Key Management Products and Services Ordering** - This section describes the ordering of key management products and services via KMI. Details must be included that are sufficient to permit determination of long-term support by the KMI.

(e) **Key Management Products and Services Generation** - This section describes the generation of key management products and services used by the cryptographic application for which the KMP is written. If the cryptographic application does not provide generation capabilities, identify the source that provides key management products and services used by the cryptographic application.

(f) **Key Management Products and Services Distribution** - This section describes the distribution and translation of key management products and services within the cryptographic application. The distribution plan will include when and where the key management products and services are encrypted or unencrypted, the physical form (electronic, PROM, floppy, disk, paper, etc.) and how they are identified during the distribution process.

(g) **Key Management Products and Services Storage** - This section addresses how the cryptographic application for which the KMP is being written stores key management products and services, and how they are identified during their
storage life (EKMS 308 key tag, Distinguished Name). Storage capacity capabilities for key management products and services must be included.

(h) Access Control - This section addresses how access to the cryptographic application will be authorized, controlled, and validated to request, generate, handle, distribute, store, and/or use key management products and services. The use of passwords, personal identification numbers (PINs), and their expiration dates must be included. For PKI cryptographic applications, role-based privileging and the use of tokens must be described.

(i) Accounting - This section describes accounting of key management products and services used by the cryptographic application for which the KMP is written. The use of event logs to support the tracking of key management products and services generation, distribution, storage, use and/or destruction must be detailed. The use of appropriate privileging to support the control of key management products and services used by the cryptographic application must also be described, in addition to the directory capabilities used to support PKI cryptographic applications, if applicable. The KMP shall identify where human and automated tracking actions are performed and where two-person integrity is required, if applicable.

(j) Compromise Management and Recovery - This section addresses how secure communications can be restored in the event of the compromise of key management products and services used by the cryptographic application for which the KMP is written. The recovery process description must include the methods of rekey or replacement. For PKI cryptographic applications, the implementation of Certificate Revocation Lists (CRLs), Compromised Key Lists (CKLs), and Indirect Certificate Revocation Lists (ICRLs) must be detailed. A description of how certificates will be reissued and renewed within the cryptographic application must also be included.

(k) Key Recovery - For cryptographic applications that provide a key recovery capability this section must be included. Key recovery addresses how previously unavailable confidentiality key can be recovered. The key recovery process description must include a discussion of the generation, storage, and access for the long term storage key. The process of transitioning from the current to future long-term storage key must also be included.

(l) Appendix A (optional) - Use of standard key management products and services provided by the KMI is highly encouraged. However, a cryptographic application may identify requirements that are currently not supported by KMI. This appendix, if applicable, addresses where improvements to the KMI are required in order to achieve the needed cryptographic application functionality. This will assist in identifying requirements for current and/or planned capability increments of the KMI. Even if a cryptographic application can be fully supported by the current or planned KMI, improvements to the KMI shall also be identified if they
improve the functionality of the cryptographic application, reduce User workload, or improve/reduce KMI functionality. Requirements identified in this appendix will be analyzed for potential upgrades to the KMI, based on available cost, schedule, and performance constraints.

(m) Attachment 1: Key Management Plan Checklist for Cryptographic Engine Developments - The following key management-related information for cryptographic engine developments is needed to determine and resolve potential impacts to the Key Management Infrastructure in a time frame that meets User requirements. Please provide yes/no responses to the following questions as well as additional information for each “yes” response.

- Are unique key management products and services required by the cryptographic engine for proper operation? Are the unique key management products and services approved by NSA?
- Are there any cryptographic capabilities to be supported by the KMI that are not fully programmable in the cryptographic engine?
- Does the cryptographic engine implement a standard IAD software download capability for importing updated cryptographic functions?
- Does the cryptographic engine use any non-key material KMI products or services (such as CKL/CRLs, PAC/dePAC, seed key conversion, etc.)?
- Does the cryptographic engine implement or have the capability to implement benign techniques?
- Does the cryptographic engine design preclude use of any Cryptographic Algorithm Configuration Management Board (CACMB) approved cryptographic algorithm?
- Does the cryptographic engine design preclude allied releasability?

b) Key Specification.
The key specification describing the keying scheme and key requirements of the configuration item(s) shall be addressed using SECTION 5, “Contractor Guidelines for Acquiring Keying Material”. Format and delivery requirements are described in CDRL UP29.

The Contractor shall prepare and submit FSDA documentation to the NSA for approval.

A detailed description of the FSDA process is included in C Technical Report Number 02-00, 27 January 2000, “Fail-Safe Design & Analysis: Revised”. The FSDA process consists of nine steps associated with two broad categories of development activity. Steps one through five of the FSDA process normally occur during the requirements definition phase of a program and are performed by the Government. Steps six through nine include tasks which occur during the requirements verification phase of development and are completed by the contractor.

FSDA is based on a system engineering methodology intended to be performed as a concurrent part of the design and development process. The contractor shall begin the functional to physical level system decomposition as defined in Step 6 of C Technical Report Number 02-00 during the initial conceptual phase of development. The fault trees as described in Step 7, physical pin-to-pin analysis as described in Step 8, and summary of the FSDA analysis as described in Step 9 shall be completed
in conjunction with the physical design effort within the guidelines of C Technical Report Number 02-00. Data delivery shall consist of two submissions. An Initial (draft) version of Steps 6-9 shall be submitted during the Preliminary Design Review (PDR). The Final version of Steps 6-9 shall be submitted immediately following the Critical Design Review (CDR) and must be approved prior to the start of Security Verification Test (SVT). Format is per DID DI-MISC-90090A, Fail Safe Design and Analysis, and delivery requirements are described in CDRL UP02.

17. Security Verification (SV) Plan & Reports.
The contractor shall prepare and submit a SV Plan with detailed procedures as one CDRL submittal and Security Verification Report after completion of Security Verification testing as a separate submittal to the NSA for approval. The SV Plan and Procedures and the SV test Report(s) shall be submitted under separate cover. The SV Plan and Procedures CDRL shall be submitted as one document and must be classified as system high, as it will contain UIC Requirements along with an explanation as to how the UIC requirements will be verified and a link to the procedures that will completely verify the UIC requirement. The SV Procedures should contain boundary testing. For a description of the SV Plan & Reports, refer to the UIC. In addition, Cryptographic Verification is a subset of Security Verification. Formats are per DIDS DI-QCIC-90021B, Cryptographic Verification Plan, and DI-QCIC-90022B Cryptographic Verification Report; delivery requirements are described in CDRL UP05.

The Contractor shall prepare written In-Process Accounting Procedures in compliance with the INFOSEC Supplement to the Industrial Security Manual (DoD 5220.22-S). Format is per DID DI-QCIC-90059, In-Process Accounting Procedures Plan and delivery requirements are described in CDRL UP12. As an alternative, the contractor may submit a copy of its “boilerplate” In-Process Accounting Procedures if those procedures have been reviewed and approved by an IAD program office within the last year. A copy of the approval must be provided with the submitted procedures. Any In-Process Accounting Procedures unique to the program must be submitted to the NSA Program Office for review and approval in addition to the boilerplate document.

After the configuration items (CI) and the CI database have been baselined (see physical configuration audit plan and report), all proposed changes and variances within, or which affect, the INFOSEC-Boundary shall be submitted to the NSA Program Manager for processing and approval. NSA approval of changes and variances must be obtained prior to the shipment of any product/system affected by the change or variance. The contractor shall ensure that proposed changes and variances do not degrade the security integrity, specified performance, interchangeability, or reliability of the product/system. All changes and variances shall be submitted electronically utilizing a separate notice for each “0N” number. A single notice may be utilized to depict changes to a drawing and associated parts list reflecting the same “0N” number. Format is per DID DI-CMAN-90072, Engineering Database and Configuration Management Information, and delivery requirements are described in CDRL UP09.

Changes, variances and modifications to INFOSEC-Boundary CIs shall be prepared and delivered to the NSA IAW the following requirements: