June 2007

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

June 2007

TABLE OF CONTENTS

June 2007

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 hight-confidence, survivable link for reception of Emergency Action Messages (EAM) fro the President and Secretary of Defense, the Joint Chiefs of Staff (JCS), and the Commander, United States Strategic Command (CDR USSTRATRCOM) 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 (NEREP0 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) implemention of JCS EHF communications systems which will provided a dramatic increase in throughput capabilitiy. 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) complience, and an objective requirement to provide a functional layered architecture for the EHF/AEHF capability. This will allow the Governmnent to minimize life cycle costs and training costs, and enhance supportabliity. Such a layered approach will facilitate upgrades

through application of common, open, and exposed (or exposable) interfaces with minimum impact over the life of ther 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.

All software development shall be IAW IEEE/EIA 12207.0-1996 (IEEE Standard for Industry Implementation of International Standard ISO/IEC 12207:1995) as appropriately tailored using IEEE/EIA 12207.2-1997 (IEEE Standard for Software Life Cycle Processes – Implementation Consideration). The contents of the deliverables shall be compliant with IEEE/EIA 12207.1-1997 (IEEE Standard for Software Life Cycle Process – Life Cycle Data). If other than IEEE 12207 compliant standards are used, then a matrix must be prepared with the deliverable that shows how the deliverable maps to the IEEE/EIA 12207.1 content requirements.

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; "0N" 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

Acquisition Technology and Logistics, specifically on the Defense Procurement and Acquisition Policy page found at URL http://www.acq.osd.mil/dpap/UID/.

(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 cerification.
- 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.

9. World-Wide Power Considerations.

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).

10. Nuclear Survivability/Vulnerability.

The concept of Nuclear Survivability shall be included in any INFOSEC equipment used or developed for use in military Command, Control, Communications, and Intelligence (C^3I) 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

12. Theory of Design & Operation (TDO) Documentation.

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.

13. Theory of Compliance (TOC) Documentation.

TheTheory 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.

15. Key Management Plan and Key Specification.

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 life cycle 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 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 requirement 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.

16. Fail Safe Design and Analysis (FSDA) Documentation.

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 submital and Security Verification Report after completion of Security Verification testing as a seperate submital 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 submited as one document and must be classified as system high, as it will contain UIC Requirements along with an explination as to how the UIC requierments will be verified and a link to the procedures that will completely verify the UIC requirement. The SV Procedures should contain boundry 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.

18. In-Process Accounting Procedures Documentation.

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.

19. Configuration Control Documentation.

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: