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 DID 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. ..... 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: .....

Signature: .....

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, Configuation 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 requriements for a system or subsystem and the methods to be used to ensure that each requriement 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 teh 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 documetn should be titled System Specification or Subsystem Specification (SSS). Format is per DID DI-IPSC-81431A (Supersedes DI-IPSC-81431), System Subsystem Specification (SSS) and deliverery 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, than 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 DI-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 DI-81439A, Software Test Description (STD), and delivery requirements are described in CDRL UP23.

SECTION 4 - ADDITIONAL REQUIREMENTS

23. Contractor's Target Program Status Report.

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-90001A, 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.

26. Interface & Operator's Guide.

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 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 AwarenessTraining.

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 an 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.

31. Custom Integrated Circuit Design Validation.

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 stimulius 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.

(2) Circuit schematic data provided in either SPICE or CDL net list format. Other formats will be considered, with approval, at the discretion of the Government Program Manager.
(3) Logic equation and/or truth table data provided as a simulation model preferable in Verilog or VHDL format. Logic equations are acceptable provided any and all math symbols are defined. Truth tables are acceptable provided all inputs, outputs and bi-directional are identified. Truth table columns shall be tab delimited. The vendor shall verify that all input and bi-directional input combinatiuons are accounted for and that any symbols used in the truth table are defined.
(4) Composite layout data shall be provided in the GDSII file.

32. Field Programmable Gate Array (FPGA) Documentation

For each FPGA provide documeantion/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. NSTISSIP 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/nonelectronic 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.

June 2007

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 (UVEPROMs):

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 programed 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.

June 2007

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.

June 2007

CONTRACT DATA REQUIREMENTS LIST

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