Rating Maintenance Phase Program Document Version 2

NATIONAL
COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

1 March 1995

NCSC-TG-013-95
Library No. S-242,047

This page intentionally left blank

FOREWORD

This publication, the **Rating Maintenance Phase Program Document Version 2**, is being issued by the National Computer Security Center (NCSC) under the authority of, and in accordance with, DOD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this document is to describe the process and requirements in the Rating Maintenance Phase (RAMP) of the Trusted Product Evaluation Program (TPEP).

Approved:

John C. Davis — 1 March 1995
Director, National Computer Security Center

This page intentionally left blank

RAMP Working Group Members

Timothy J. Bergendahl
Ronald J. Bottomly
Roberta J. Medlock
W. Olin Sibert
Dana Nell Stigdon

Significant contributions to this document were made by all individuals who assisted in rewriting the original Rating Maintenance Phase (RAMP) Requirements, including Diann A. Carpenter, Steve LaFountain, Robin Oliver, Caralyn Wichers, and members of the vendor community. Acknowledgment is also given to the authors of the first version of the **Rating Maintenance Phase Program Document**, NCSC-TG-013, dated 23 June 1989.

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

Chapter 1

Introduction

On 23 June 1989, the first version of the **Rating Maintenance Phase Program Document**, NCSC-TG-013, was published. The 1989 document contained Rating Maintenance Phase (RAMP) Requirements for systems evaluated at the C2 or B1 levels of trust within the Trusted Product Evaluation Program (TPEP), a program of the National Security Agency (NSA). Since then, RAMP has evolved, with new RAMP Requirements announced by NSA in 1991 for systems evaluated at the C2 or B1 levels of trust.[1] In addition, RAMP Requirements for systems evaluated at the B2, B3, or A1 levels of trust were announced by NSA in 1992.[2]

This document, the **Rating Maintenance Phase Program Document Version 2**, describes the requirements for the Rating Maintenance Phase of the TPEP and includes the requirements of all parties involved in RAMP, and provides guidance regarding RAMP deliverables.

1.1 Evaluation Overview

The Department of Defense Computer Security Center was established in January, 1981, to encourage the widespread availability of trusted computer systems for use by facilities processing classified or other sensitive information. In August, 1985, the name of the organization was changed to the National Computer Security Center (NCSC). In order to assist in assessing the degree of trust one could place in a given computer system, the **Department of Defense Trusted Computer System Evaluation Criteria** (TCSEC), DOD 5200.28-STD, dated December, 1985, was published.

The TCSEC establishes specific requirements that a computer system must meet in order to achieve a predefined level of trustworthiness. The TCSEC levels are arranged hierarchically into four major divisions of protection, each with certain security-relevant characteristics. These divisions are in turn subdivided into classes. To determine the division and class at which all requirements are met by a system, the system must be evaluated against the TCSEC or its interpretations, the **National Computer Security Center Trusted Network Interpretation** (TNI), NCSC-TG-005, dated July, 1987, or the **National Computer Security Center Trusted Database Management System Interpretation** (TDI), NCSC-TG-021, dated April, 1991. This evaluation is performed for the NCSC by a evaluation team sponsored by the NSA.

A successful product evaluation results in the production of a Final Evaluation Report (FER) and an Evaluated Products List (EPL) entry. The FER is a summary of the evaluation and includes the EPL rating that indicates the class at which the product satisfies all TCSEC requirements in terms of both features and assurances. The FER and EPL entry are made public.

[1] These requirements are contained within Dockmaster's announce forum transaction 233, dated 12/19/91.
[2] These requirements are contained within Dockmaster's announce forum transaction 268, dated 09/30/92.

1.2 Evaluation Process

A TPEP evaluation involves the following phases:

- The Proposal Review Phase;
- The Advice Phase;
- The Evaluation Phase;
- The Rating Maintenance Phase (RAMP).

Each of these phases is briefly discussed below.

1.2.1 The Proposal Review Phase

Once the vendor has designed and begun implementation of the product, has developed the required documentation on which to base an evaluation, and has signed a non-disclosure agreement, the NSA assigns a team to conduct an Intensive Preliminary Technical Review (IPTR). The IPTR team performs the following functions:

- Ascertains if the product maps to the TCSEC or one of the TCSEC interpretations;
- Reviews target criteria level relating to the product;
- Reviews the configuration of the product;
- Verifies documentation presence and samples documentation completeness;
- Develops a draft evaluation schedule;
- Estimates vendor and product readiness for evaluation;
- Creates an IPTR report.

During the IPTR the team discusses RAMP with the vendor and reviews the vendor's draft Rating Maintenance Plan (RM-Plan).

1.2.2 The Advice Phase

A vendor is considered in the Advice Phase until the necessary evaluation evidence exists to support the evaluation. The NSA assigns resources as available to provide guidance to the vendor while the vendor completes the evaluation evidence, or directs the vendor to seek guidance elsewhere. It is during the Advice Phase that a vendor identifies the Vendor Security Analyst (VSA) personnel and recommends them for training within NSA's VSA Class, provided they have not previously received this training.

1.2.3 The Evaluation Phase

Once a product has passed its IPTR and a legal agreement is in place, an evaluation team is assigned by the NSA. Team training then occurs. Next, the team conducts an in-depth analysis of the product's design; user and test documentation; security testing; assurance documentation; implementation review (for B2 and above); and formal specification review (at A1). During this time, the Initial Product Assessment Report (IPAR) is written and includes a summary focusing on the RAMP Requirements and how they are met.

The team then appears before the IPAR/Test Technical Review Board (TRB) and defends the initial assessment as documented in the IPAR, including all RAMP aspects of the evaluation. In addition, the team summarizes the vendor test plans, presents the team's test plan to the TRB, and answers any questions the TRB members might have about the vendor's testing or the team's proposed testing of the product. The TRB then provides comments to TPEP Management about the product, including any comments they might have about RAMP aspects of the evaluation. As a result of the TRB recommendations and other inputs, TPEP Management makes a decision whether to approve or to disapprove the RM-Plan and whether to move on in the evaluation process.

Once approval to continue the evaluation is given, the evaluation team writes the FER, conducts a RAMP Audit and tests the Trusted Computing Base (TCB). The team then appears before a Final TRB, at which time the team presents the results of the RAMP Audit and team testing to the TRB. Upon a positive recommendation of the Final TRB, and acceptance of the recommendation by TPEP Management, the product is entered on the EPL and the FER is published.

1.2.4 The Rating Maintenance Phase

RAMP begins when the EPL entry is published for the product at the conclusion of the Evaluation Phase. During RAMP, the vendor is doing most of the work to assure that the product under RAMP is capable of maintaining the same rating that was assigned to it via the most recently published EPL entry. RAMP is divided into RAMP Cycles, with a RAMP Cycle being the period of time between two consecutive EPL entries for the product under RAMP. A product under RAMP must always have an NSA-approved RM-Plan in place for RAMP to continue.

1.3 The Reason for RAMP

Once a vendor releases a new version of a product that has received an EPL rating, the new version is not an evaluated product. Because of the frequency of new releases and the limited evaluation resources, continual reevaluation of a vendor product is both impractical and impossible. In order to meet the goal of having commercially available trusted products, an efficient and substitute process for reevaluation is necessary. RAMP was established to provide a mechanism to extend the previous rating to a new version of a previously evaluated computer system product.

RAMP seeks to reduce evaluation time and effort required to maintain a rating by using the personnel involved in the maintenance of the product to manage the change process and perform Security Analysis. Thus, the burden of proof for RAMP efforts lies with those responsible for system maintenance (i.e., the vendor) instead of with an evaluation team.

1.4 RAMP Overview

During RAMP, all changes to the vendor system must be managed by the vendor. For each RAMP Cycle, the vendor must be able to identify all changes to the system and perform Security Analysis of those changes. The procedures the vendor follows to manage changes to the system are described in the RM-Plan. This document is written by the vendor and is approved by the NSA during the original evaluation. The RM-Plan describes how the vendor will meet the RAMP Requirements as well as describing the system to which the plan applies.

During the original evaluation, the vendor also identifies the VSAs[3] who will be responsible for the security of the system. These personnel will attend the NSA VSA Class that serves to describe basic security fundamentals and to explain the procedures of RAMP.

Once the evaluation has been completed, the vendor's Responsible Corporate Officer (RCO) is tasked with ensuring that the procedures outlined in the RM-Plan are being followed. The VSAs are responsible for reviewing the Security Analysis of all changes that have been made to the system, and for determining that the security features and assurances of the system are upheld. VSAs may consult a Technical Point of Contact (TPOC) for assistance with any technical questions regarding the application of the TCSEC requirements.

RAMP Evidence will be recorded for every change, detailing the Security Analysis of the change. This information is used when a RAMP Audit is performed by either the NSA or the vendor, and is used as the basis for a Rating Maintenance Report (RMR). An RMR is a document that is submitted to the NSA for every system release that is to be evaluated. It summarizes all changes that have been made since the last evaluated release of the system, and describes why the security features and assurances of the system are upheld. The RMR is input to the TRB.

The VSA (Security Analysis Team (SA-Team)[4] at B2 and above) must present the contents of the RMR to the TRB before a new EPL rating can be awarded. The TRB serves both as a technical check and as a consistency check with all other evaluations. Upon the recommendation of the TRB, TPEP Management will make a decision whether or not to extend the rating to the new product version.

1.5 Goals and Approach

The goal of RAMP is to keep the EPL populated with currently available trusted products. As previously mentioned, the vendor bears primary responsibility in RAMP for maintaining product trust as the system evolves. The vendor accomplishes this by integrating Security Analysis into the development process.

The NSA recognizes that the expertise for product maintenance lies with the vendor. Therefore, the RAMP Requirements do not seek to dictate development procedures, but rather seek to be as flexible as possible to allow the vendor's current processes to be used with little enhancement.

Rating maintenance is accomplished by using qualified vendor personnel (VSAs) to oversee the vendor's product modification process. These vendor personnel must have strong technical knowledge of computer

[3] Although the plural form of VSA is frequently used within this document, this should not be taken as an indication that there must always be more than one person in the VSA role.

[4] SA-Team is defined within the **Definitions** section of **Chapter 3** of this program document.

security and of their computer product. They will oversee the development/maintenance cycle of the previously rated product, and will demonstrate to the NSA that any modifications to the product preserve the security features and assurances required by the TCSEC for the rating previously awarded to the evaluated product. The work of the VSA is meant to be at the same level of detail as the work performed by TPEP evaluators during the original evaluation.

1.6 Applicability of RAMP

RAMP applies to products that have been evaluated against the TCSEC, the **National Computer Security Center Trusted Network Interpretation** (TNI), NCSC-TG-005, dated July, 1987, or the **National Computer Security Center Trusted Database Management System Interpretation** (TDI), NCSC-TG-021, dated April, 1991. However, the Rating Maintenance Phase always builds upon a product evaluation; it provides no opportunity to avoid an evaluation.

RAMP applies at all levels of the criteria, from C2 through A1. RAMP differs slightly between B1 and below and B2 and above; these differences are highlighted throughout this program document.

1.7 Scope of RAMP

The scope of RAMP activities is limited to those changes that are feasible to evaluate in the context of the RAMP process, which expects re-use of previous evaluation evidence and a corresponding reduction in evaluation effort. There are two factors that limit the applicability of RAMP: changes to the product and changes to the rating. In addition, change in ownership of the product or the vendor company may change a product's eligibility for future RAMP activities.

1.7.1 Product Changes

RAMP applies to the same vendor that originally received the rating. If a vendor sells an evaluated product to a new vendor, the new vendor must submit a proposal for evaluation. The new vendor cannot simply attempt to RAMP any changes made to the system. Once this new vendor has gone through an evaluation, that vendor is eligible to participate in RAMP. This restriction is necessary due to the underlying assumptions of RAMP. RAMP assumes that the vendor has gone through an evaluation and thus, by experience, understands the evaluation process and the types of technical questions that should be asked when performing Security Analysis. Additionally, after performing an evaluation, the NSA is confident that the vendor does indeed understand the system and will be able to maintain it as outlined in the RM-Plan. The NSA has no way of assessing the vendor's understanding and development procedures short of an evaluation.

The types of changes that may be performed under RAMP have not been quantified. An objective measurement of "too much" change has not been established. This will vary depending on the type of system and the level of trust. At the lower levels of trust (B1 and below), the vendor may consult with the TRB during a Final or RAMP TRB meeting regarding future changes to be made.[5] At B2 and above a Future Change Review Board (FCRB) is convened at the beginning of a RAMP Cycle. The FCRB helps to determine if

[5] The vendor would seek guidance from the TRB as to whether the future changes would be appropriate under RAMP.

the proposed changes are appropriate under RAMP. If the changes are deemed appropriate, the FCRB also helps to determine the level of analysis and testing required.

The NSA reserves the right to terminate a RAMP action at any time if the technical changes have been so vast that NSA believes the system warrants a new evaluation.

Systems maintaining ratings under RAMP must also realize that RAMP is not intended to promulgate mistakes or bad decisions. If a mistake was made during the original evaluation and is uncovered during a RAMP Cycle by the vendor or by someone else, the vendor is required to correct the mistake and make sure the system meets the security requirements. Likewise, the vendor must make sure the system meets any new interpretations that have been issued.

1.7.2 Rating Changes

In general, the RAMP process does not allow for changing the EPL rating received in a previous evaluation, for example changing a rating either up or down, adding or deleting "extra credit" features, or changing the set of functions (M, I, A, D) performed by a network component.

However, some changes of this sort may be sufficiently straightforward to evaluate that the RAMP process is applicable. For such changes, TPEP Management will make a case-by-case decision, based on a vendor's proposal, about whether a change is feasible to evaluate under RAMP. For such rating changes, the standard RAMP process described by this document will be followed.

Examples of rating changes that could be evaluated under RAMP might include addition of Device Labels extra credit for a product previously evaluated at B1; addition of a C2-only configuration of a product previously evaluated at B1; deletion of Trusted Path extra credit for a product previously evaluated at B1; creation of an M-component version of a network component previously evaluated as an MDIA-component; or a change in rating from A1 to B3 because formal specifications are no longer maintained.

1.8 Document Organization

This document consists of seven chapters and six appendixes. The first chapter is this **Introduction**. Chapter two provides an overview of the RAMP process; chapter three contains the RAMP Requirements for products under the TPEP; chapters four through six identify and discuss the requirements of all parties involved in RAMP; and chapter seven contains a discussion of the VSA Class. The appendixes provide guidance about writing a RM-Plan; writing a RMR; and RAMP Audits. Sample outlines for the Quarterly Status Report (QSR) and for the TPOC Report are also found within the appendixes, as is a list of acronyms.

Because RAMP continues to evolve, this program document would not be complete without the addition of an electronic chapter. As updates are made to this document they will be posted to the `announce` forum, a bulletin board on the Dockmaster computer system (or its successor) that is publicly available. These announcements, once posted, are to be considered part of this program document. One is not complete without the other. Periodically, this document will be updated to incorporate the posted changes. In this manner, the current state of the Rating Maintenance Phase will be continually documented.

Chapter 2

Overview of the RAMP Process

The Rating Maintenance Phase (RAMP) Requirements are intended to meet two principal goals: maintaining the assurances that derived from the product's original evaluation, and being feasible to meet within the commercial development framework in which the product was created. Furthermore, to be successful, RAMP must be able to achieve these goals at reasonable cost both to the National Security Agency (NSA) and the vendor. This rationale discusses how those goals are met, concentrating in particular on the distinctions between evaluation classes.

2.1 Maintaining Assurances

The principal focus of RAMP is maintaining assurance that the Applicable Requirements are met by the product as the product evolves. This is done by requiring the vendor to follow an analysis and change management process in product development and maintenance, such that the results of the process can be reviewed by NSA. All changes are reviewed for security-relevance by trained Vendor Security Analysts (VSAs); this is central to the success of the change analysis and management.

2.1.1 Role of the Vendor Security Analyst

In effect, the VSA is NSA's representative within the vendor's organization. A VSA has received RAMP training from the NSA, and is expected to understand both the product (or specific aspects of the product, if there are multiple VSAs) and the security requirements—and be able to assess changes with respect to both. The vendor is responsible for maintaining trained VSAs during each RAMP Cycle to ensure that the necessary product expertise is available for the analysis.

In order to be effective in this role, a VSA must have approval authority with respect to changes, and must be able to represent the vendor's organization to the NSA. Thus, a VSA must have a considerable degree of administrative authority as well as technical skills. The VSA's role is essential to the Rating Maintenance Phase, since the VSA has primary responsibility for maintaining the product's assurances. A VSA is responsible for reviewing the Security Analysis of every change to the evaluated system. In essence, the VSAs perform the same work as an evaluation team would, including analysis, approval, reporting, and presentation to the NSA Technical Review Board (TRB).

2.1.2 Role of the Technical Point of Contact

The Technical Point of Contact (TPOC) is an NSA evaluator (or possibly several evaluators, depending on the product). The TPOC's responsibility is to maintain contact between the vendor and NSA; to keep the vendor apprised of relevant evaluation issues; and to ensure that the vendor has a point of contact for technical questions and discussions.

The TPOC's role is to assist the vendor by providing any information necessary to ensure that the vendor's activities are properly directed. This avoids effort wasted in pursuing unsatisfactory approaches because proper and timely guidance was unavailable. Although the vendor is expected to do most of the work in RAMP, continuous involvement by both parties is critical to making the process successful.

The TPOC must be able able to represent the vendor's point-of-view in discussions within the evaluation community. This role can be fulfilled only by an NSA representative because it involves, potentially, access to proprietary information about other product evaluations.

2.1.3 RAMP Audits

Although RAMP is based on trust in the vendor's development process, it would be imprudent to rely on this with no means for validation. Consequently, RAMP Audits are included in this phase. A RAMP Audit is expected to verifiy that the vendor's NSA-approved RAMP process has been followed for the changes implemented during that RAMP Cycle and that the VSA's security analyses are correct.

If there is evidence of process failures (such as significant discrepancies between planned changes and actual implementation, or incomplete or incorrect Security Analysis), aperiodic RAMP Audits may be performed at NSA's discretion.

2.1.4 Changes in Requirements

During RAMP, several things may occur that result in requirements applying differently to the new version of a product than occurred in the original evaluation. First, NSA periodically issues interpretations of the Applicable Requirements and these interpretations may have the effect that some aspect of an already-evaluated product is no longer acceptable. Second, a new product feature (e.g., a new class of objects) may need a new interpretation of Applicable Requirements. Third, a new flaw in some area of the product otherwise unaffected by the changes may be discovered during testing or Security Analysis. Finally, it may be determined in the course of Security Analysis that the original evaluation team, through omission or oversight, incorrectly interpreted some Applicable Requirement.

Rules for handling these situations are deliberately not included in the current RAMP Requirements. In two cases (novel product features and flaws discovered in penetration testing), the Applicable Requirements apply as stated: the new features must conform to the requirements, and appropriate remedial actions must be taken for flaws. In the cases where there is a new interpretation or an error of interpretation, more flexibility is allowed: the results must be incorporated into the product within a reasonable period of time, but it would be inappropriate to hold up a RAMP action whose sole purpose is to fix a critical security flaw in an existing system simply because the system no longer meets a recently-issued interpretation of a particular Applicable Requirement. In these cases, Trusted Product Evaluation Program (TPEP) Management is responsible for reaching an agreement with the vendor that results in a fully-compliant product in a reasonable time without placing an undue burden on the vendor.

2.2 Evaluation Process Activities

During the original evaluation of a product, the product's Rating Maintenance Plan (RM-Plan) must be evaluated and approved by the evaluation team. This approval is reviewed by the Technical Review Board (TRB) during the evaluation, and is reflected in the Evaluated Products List (EPL) entry. The RM-Plan must be described in the Initial Product Assessment Report (IPAR), and presented to the IPAR TRB. Approval of the RM-Plan takes place through the same process (i.e., evaluation) as approval of other evaluation requirements; there is no separate approval step.

Prior to the Final TRB for a product, the evaluation team must conduct a RAMP Audit, and present the results of the audit to the Final TRB. The RAMP Audit must show that the product is being maintained in accordance with the RM-Plan.

The IPAR and Final Evaluation Report (FER) must include a section describing how the product satisfies the RAMP Requirements. This section lists the RAMP Requirements (from Chapter 3 of this document) and describes how each requirement is satisfied.

2.3 Integration with Vendor Process

The intent of the RAMP Requirements is that they be easily integrated with the vendor's existing development process. This is accomplished by stating the requirements at a very high level and allowing them to be interpreted in a cost-effective manner for each vendor. Aside from process details necessitated by the Applicable Requirements themselves, the RAMP Requirements are detailed in the areas of reporting and review with NSA.

These RAMP Requirements ensure that the vendor's effort in analysis, and the level of detail at which the analysis is performed, is commensurate with the effort and scope of the original evaluation. It does not make sense to require greater depth of analysis for product changes than for evaluation, since the goal of RAMP is to be more cost-effective than full-scale evaluation.

2.4 C2-B1 Requirements Versus B2-A1

In order to capitalize on the vendor's expertise with the product, most of the burden for analysis is placed on the vendor's hands, especially at the C2 and B1 evaluation classes. This is done in recognition that the most difficult parts of evaluation involve coming to a mutual understanding, between NSA and the vendor, of what the Applicable Requirements—both features and assurances—mean with respect to a specific product. Once that has been accomplished, it is generally straightforward to maintain that understanding through future development, even in the face of significant changes. Consequently, for C2-B1 products, the change analysis is entirely the responsibility of the vendor, and NSA serves only in an advisory, review, and audit role.

However, products in the B2, B3, and A1 evaluation classes are expected to exhibit far stronger assurances than C2-B1 products, and consequently are employed in environments where security is much more critical than C2-B1 products. Although the vendor can do most of the work in maintaining the rating, the greater assurance and greater sensitivity of information processed by systems of these classes mandates additional effort in evaluation of changes. The additional effort takes three forms: the advance analysis of proposed changes by the Future Change Review Board (FCRB); possible direct support of the analysis effort by NSA personnel; and NSA support for penetration testing.

In some cases, changes to a C2 or B1 product may warrant an FCRB. This would occur where proposed product changes are sufficiently complex to require an in-depth analysis beforehand. Requests for FCRBs for C2 and B1 products will be considered on a case-by-case basis by TPEP Management.

2.4.1 Future Change Review

The role of the FCRB is to assess the likelihood that planned changes will result in unexpected security consequences and to recommend the nature and scope of evaluation effort appropriate to assess those changes. This largely informal proceeding allows the vendor to benefit from the knowledge of experienced evaluators, and also provides NSA opportunity to devote specific resources to assist the vendor in making the changes.

In the previous version of the **Rating Maintenance Phase Program Document**,[1] NCSC-TG-013, dated 23 June 1989, future change review was a much more structured and formal process, and was required. Future change review is no longer required at the B1 and C2 classes because it requires a degree of planning and commitment that is not appropriate in commercial product development (and a corresponding reduction of flexibility for the vendor), and also because standard commercial development practices are considered sufficient to maintain the assurances of those evaluation classes. In addition, this version of the RAMP Requirements eliminates the fixed categories for FCRB recommendations, instead allowing them to be tailored to each situation.

2.4.2 Analysis Support

Depending upon the changes involved, the FCRB may recommend that the SA-Team be augmented with additional NSA evaluators. This recommendation would arise in instances where the FCRB believes the TPOC may require assistance for tasks requiring independence from the developers, yet too arduous for the TPOC to perform alone in a timely fashion. For example, the code study involved in assessing the system's architecture (e.g., for modularity) necessitates that the review be as objective as possible. Because VSAs are typically developers, this need for objectivity may require a greater need for independence between the vendor and NSA.

2.4.3 Penetration Testing

At the B2 class and above, there are strict requirements for penetration testing, which by its very nature is an adversarial process. Furthermore, the penetration testing in the original evaluation is based solely on work performed by the evaluation team, as opposed to the team's review of work performed by the vendor.

Although some very simple changes can be reviewed without any need for penetration testing, most will require such testing to help rule out side-effects. For example, penetration testing may include validation of the vendor's covert channel analysis, which is usually affected by performance enhancements in the underlying hardware—a very common reason for RAMP activity.

[1] Only B1 and C2 products were addressed within this document.

2.5 RAMP Status Changes

In the event of a significant change in a product's RAMP status, NSA will publish an announcement describing the change. Changes warranting such an announcement include a vendor's voluntary withdrawal from the RAMP process; termination of RAMP activities from failure to meet RAMP requirements; change in ownership of the product or vendor; and product changes that result in re-evaluation because they cannot be accommodated by RAMP.

2.6 Products Not Covered by RAMP

RAMP Requirements are not defined for the C1 evaulation class because NSA no longer performs C1 evaluations. The minimal value of such products in protecting sensitive information and the limited customer demand does not justify either evaluations or RAMP. In addition, RAMP Requirements are not defined for subsystem evaluations (performed under the **Computer Security Subsystem Interpretation** (CSSI), NCSC-TG-009, dated 16 September 1988), since the limited assurance provided by such products does not justify their incorporation into the RAMP Program.

This page intentionally left blank

Chapter 3
RAMP Requirements

Before stating the Rating Maintenance Phase (RAMP) Requirements, terms are defined that are used within the requirements. These definitions are to be considered part of the requirements (i.e., whenever one of the defined terms is used, it refers to the definition of that term). Not all of these definitions are applicable to both the C2-B1 requirements and the B2-A1 requirements. Details that differ between the two sets of requirements are spelled out in the requirements themselves.

In these requirements, references are made to the National Security Agency (NSA) as an authority for approvals, appointments, etc. This refers specifically to the Chief of the Trusted Product and Network Security Evaluations Division or a designee.

In these requirements, references are also made to designated personnel: the Vendor Security Analysts (VSAs) and the Technical Points of Contact (TPOCs). Depending on the product, there may be only one of each, or there may be several. In the case that there are several, they are jointly responsible for their activities. Although the plural form is always used, this should not be taken as an indication that there must always be more than one person in the role.

3.1 Definitions

The following definitions apply to the requirements specified within Sections 3.2 and 3.3.

APPLICABLE REQUIREMENTS: The requirements under which the product is to be evaluated, including the **Trusted Computer System Evaluation Criteria** (TCSEC), **Trusted Network Interpretation** (TNI), or **Trusted Database Management System Interpretation** (TDI), and all approved interpretations that apply to the product. An interpretation applies to the product if and only if it refers to a feature or assurance that is present in the product and the interpretation was approved either prior to the most recent Evaluated Products List (EPL) date of the product or more than one calendar year prior to the submission of a Rating Maintenance Report (RMR) for the product version being considered.

CONFIGURATION ITEM (CI): Any item that may be changed under RAMP and is required by the RAMP Requirements for the target evaluation class to be defined as a Configuration Item (CI). The granularity of a CI shall be sufficient to support the Security Analysis of future changes.

CONFIGURATION MANAGEMENT PLAN (CM-PLAN): The vendor document that describes how the TCSEC Configuration Management requirement is met (for levels B2 and above).

FUTURE CHANGE REVIEW BOARD (FCRB): The panel who reviews future evaluated product changes and makes a recommendation to the NSA on the composition of the Security Analysis Team (SA-Team). The FCRB consists of Technical Review Board (TRB) members and other personnel as appointed by the NSA. The FCRB recommends to Trusted Product Evaluation Program (TPEP) Management the nature and extent of the analysis to be performed by the Security Analysis Team (SA-Team), the composition of the SA-Team, the schedule, and the nature of SA-Team's presentation to the RAMP TRB. These recommendations are based on the FCRB's analysis of the scope and complexity of the proposed changes and the degree to which the changes will affect security-relevant aspects of the product.

QUARTERLY STATUS REPORT (QSR): An informal status report to be delivered by the fifth working day of January, April, July, and October describing the vendor's current status and activities with respect to the RAMP program. Failure to deliver two successive QSRs is considered grounds for termination of the product's participation in RAMP.

RAMP AUDIT: A review of the RAMP Evidence, based on a suitable representative sample, to ensure that only approved changes are implemented, that all CIs are updated consistently, and that Security Analysis is performed satisfactorily. In addition to the required RAMP Audits performed by the VSAs, aperiodic RAMP Audits may be performed by a Security Analysis Team (for B2 and above) or the TPOC.

RAMP CYCLE: The period of time between the dates of two consecutive EPL entries for the product.

RAMP EVIDENCE: The record of Security Analysis. It serves to establish accountability for each change and to provide justification for the inclusion of each of those changes.

RAMP PRODUCT: The complete set of CIs comprising the current RAMP action. The original evaluated product is the starting point for the first RAMP Product.

RATING MAINTENANCE PHASE (RAMP): The phase of the Trusted Product Evaluation Program (TPEP) that follows the Evaluation Phase. RAMP consists of a series of rating maintenance actions (RAMP Cycles) that assess the compliance with Applicable Requirements of updated versions of the product and allow those versions to be listed on the EPL. During RAMP, the vendor performs the majority of the work to determine that changes to the product maintain the previously attained rating.

RATING MAINTENANCE PLAN (RM-Plan): The vendor document that describes the mechanisms, procedures, and tools used to meet the RAMP Requirements. The procedures in the RM-Plan are followed throughout the Rating Maintenance Phase. The RM-Plan is proposed by the vendor and approved as part of the evaluation process. The RM-Plan may change during the course of RAMP for a product, particularly in the identification of designated personnel and identification of CIs.

RATING MAINTENANCE REPORT (RMR): Summary of RAMP Evidence that is submitted to the TRB.

RESPONSIBLE CORPORATE OFFICER (RCO): A person empowered financially and legally to commit resources in support of RAMP and support the technical role of the VSAs, including denial of Trusted Computing Base (TCB) changes.

SECURITY ANALYSIS: Security Analysis is an examination of the TCB to determine whether a proposed change, or set of changes, upholds the security features and assurances of the original evaluated product and any subsequent releases of the product that have been previously maintained under RAMP, in compliance with the Applicable Requirements.

SECURITY ANALYSIS TEAM (SA-Team): The individual or individuals (e.g., VSAs, TPOCs, additional evaluators) responsible for performing the Security Analysis and presentation and defense of the RAMP Evidence before the TRB.

TECHNICAL POINT OF CONTACT (TPOC): An evaluator, assigned by the NSA, who serves as the primary technical interface between the vendor and the NSA, and is assigned on the basis of familiarity with the product and its evaluation. A product may have multiple TPOCs, and the set of TPOCs assigned to a product may vary depending on the nature of the RAMP activity being performed.

TECHNICAL REVIEW BOARD (TRB): An advisory panel to the NSA. The TRB provides a source of senior technical review of the technical findings, conclusions, and recommendations of individual evaluation teams. The TRB serves as a check point for the quality, uniformity, and consistency of evaluations.

UPDATED FINAL EVALUATION REPORT: An updated version of the Final Evaluation Report (FER) that describes, at the level of detail of the original FER, the evaluated product together with the changes incorporated during the RAMP Cycle. The updated FER must be maintained in the same form as the original FER produced by the evaluation team, and must include change bars identifying the sections modified by the updates. The updated FER is the joint responsibility of the NSA and the vendor and may not be distributed externally without approval of both parties.

VENDOR BUSINESS POINT OF CONTACT (VBPOC): The person identified to act on behalf of the RCO in support of RAMP.

VENDOR SECURITY ANALYST (VSA): The vendor personnel responsible for execution of all technical tasks in RAMP.

3.2 C2-B1 Requirements

CONFIGURATION ITEM: Configuration items shall be identified by the vendor in an NSA-approved RM-Plan and shall encompass:

1. The components or subsystems, including software source and object code, that comprise the Trusted Computing Base (TCB).
2. Any hardware and/or software features that are used to periodically validate the correct operation of the TCB in satisfaction of the System Integrity requirement.
3. The informal or formal model of the security policy (at the B1 evaluation class).
4. The Security Features User's Guide (SFUG).
5. The Trusted Facility Manual (TFM).
6. The test plan, the test procedures that show how the security mechanisms were tested, and the expected results of the security mechanisms' functional testing, and related test documentation.
7. The design documentation.

8. The RM-Plan.

RAMP EVIDENCE: For each change, RAMP Evidence shall include the following:

1. A description of the change.
2. The issues and conclusions of the Security Analysis.
3. Identification of the CIs affected.
4. The status of the changes to the CIs (e.g., being implemented, or completed).

RATING MAINTENANCE PLAN (RM-Plan): The RM-Plan shall include the following:

1. Identification of the VSA(s) and the RCO, including their corporate position.
2. The division of technical responsibilities among VSAs (if more than one).
3. The original date of approval of the RM-Plan and the dates of all approved changes.
4. The policies and procedures for Security Analysis.
5. The procedures for complying with applicable interpretations.
6. The policy for using emergency procedures for correcting errors and for incorporating these corrections in subsequent scheduled product releases.
7. A convincing argument to show that the described mechanisms, procedures, and tools are sufficient to address all changes to the product, including new features, bug fixes, and changes to satisfy Applicable Requirements.
8. The procedures for a VSA-performed RAMP Audit.
9. The procedures for RM-Plan maintenance.
10. A list of all CIs.
11. The rationale for the chosen granularity of CIs.
12. A description of the format of the RAMP Evidence.
13. All updates necessary to reflect corrective measures taken after a RAMP process failure (e.g., failure to follow, or error in following, the RM-Plan), if one has occurred.

RATING MAINTENANCE REPORT (RMR): Each RMR shall include the following:

1. A summary identifying each change that has been made since the previous evaluated release of the RAMP Product.
2. A description of all security-relevant changes and the Security Analysis of those changes.
3. A description of how the RAMP Product meets the Applicable Requirements.

4. Identification of all tools used for generating CIs.
5. The internal procedures used for restoring the RAMP process if the RAMP Cycle covered by the RMR included a process failure. The description of the internal procedures must include:
   - The nature of the failure;
   - The Security Analysis conducted to establish corrective measures and verify product trust;
   - Establishment of the missing trail of evidence linking the evaluated product to the RAMP Product.
6. Results of the VSA-conducted RAMP Audit.

RESPONSIBLE CORPORATE OFFICER: The Responsible Corporate Officer, or if the RCO has designated a VBPOC to act on behalf of the RCO, the VBPOC, shall:

1. Always be identified while the vendor is participating in RAMP and shall be responsible for the overall management of the vendor's RAMP effort.
2. Identify at least one VSA at all times while rating maintenance actions are underway.
3. Be responsible for submitting a proposed RM-Plan during the initial evaluation and shall obtain approval of the RM-Plan before entering the Formal Evaluation Phase.
4. Ensure that all subsequent changes to the RM-Plan, to reflect all changes made in the vendor's implementation of the ratings maintenance process, are submitted to the NSA for approval.
5. Sign the cover letter of the proposed RM-Plan.
6. Sign the cover letter of the RMR.
7. Ensure that any requested RAMP Audit is conducted promptly following the request.
8. Be responsible for submitting, as directed by the TPOC, copies of the following materials at least four weeks in advance of the scheduled RAMP TRB:
   - The RMR;
   - The NSA-approved RM-Plan;
   - The Updated Final Evaluation Report (FER);
   - The proposed product description for the EPL.

SECURITY ANALYSIS: Security Analysis shall include the following:

1. Examining changes to the RAMP Product for security relevance, including analyzing the effects on the TCB.
2. Reviewing the design of approved changes.
3. Ensuring that the RAMP Product is adequately tested, including ensuring adequate test coverage through modification of the tests as necessary.
4. Ensuring that all documentation needed to show compliance with the Applicable Requirements, including design and user documentation, is updated consistently to reflect all changes to the TCB.

A change shall be considered to affect the TCB if it alters code or documentation within the identified TCB boundary, changes the TCB boundary, augments the TCB, or indirectly affects the function of TCB elements.

A change shall be considered security-relevant if it directly affects any mechanism implementing identified security policies (e.g., discretionary access control (DAC), object reuse, TCB isolation) or if it directly affects the maintenance of security data.

Security Analysis shall encompass cumulative effects involving all CI changes. (For example, two otherwise acceptable changes may conflict in terms of security because one assumes conditions that no longer hold, given the other change.) Security Analysis shall also consider the effects of interrelationships among the security features of the RAMP Product.

VENDOR SECURITY ANALYST (VSA): A Vendor Security Analyst shall:

1. Successfully complete the NSA training program for VSAs (i.e., the VSA Class).
2. Deliver the vendor's Quarterly Status Reports (QSRs) to the vendor forum on the required schedule.
3. Conduct, supervise, or monitor all Security Analysis tasks according to the approved RM-Plan.
4. Review the Security Analysis prior to the submission of the RMR for the rating maintenance action.
5. Conduct an initial RAMP Audit prior to the original evaluation team's testing of the TCB. The results of this initial RAMP Audit must be provided to the evaluation team.
6. Conduct at least one RAMP Audit[1] for each RAMP Cycle. The results of the RAMP Audit must be included in the next quarterly status report following the RAMP Audit.
7. Ensure that before the RMR is submitted, the relevant parts[2] of the entire security functional test suite used in the original evaluation, as updated during the RAMP Cycle, are successfully executed on a representative sample of hardware.
8. Demonstrate to the TRB that Security Analysis has been conducted according to the approved RM-Plan in that RAMP Cycle.

3.3 B2-A1 Requirements

CONFIGURATION ITEM: Configuration Items shall be identified in the CM-Plan and shall encompass:

1. The RM-Plan.
2. The CM-Plan.
3. The hardware/firmware subsystems incorporated in the TCB.

[1] This audit can be conducted in conjunction with the TPOC's audit.

[2] In general, the entire test suite must be executed for each RAMP action because it is infeasible to determine with confidence which tests could not have been affected by the changes. If, however, the changes are limited in scope, or there are parts of the test suite that can be shown to be unaffected, a subset of the tests may be performed. The rationale for any such limitations must be presented to the RAMP TRB Panel.

4. Any hardware and/or software features that are used to periodically validate the correct operation of the TCB in satisfaction of the System Integrity requirement.
5. The Trusted Facility Manual (TFM).
6. The Security Features User's Guide (SFUG).
7. All items specified in the Configuration Management requirement of the Applicable Requirements.

CONFIGURATION MANAGEMENT: The CM-Plan shall include a list of all CIs and the rationale for the chosen granularity of CIs. The CM-Plan shall be followed throughout RAMP.

RAMP EVIDENCE: For each change, RAMP Evidence shall include the following:

1. A description of the change.
2. The issues and conclusions of the Security Analysis.
3. Accountability for change.
4. Identification of the CIs affected.
5. The status of the changes to the CIs (e.g., being implemented, or completed).
6. All other information about the change maintained by the product's configuration management system.

RATING MAINTENANCE PLAN (RM-Plan): The RM-Plan shall include the following:

1. Identification of the VSA(s) and the RCO, including their corporate position.
2. The division of technical responsibilities among VSAs (if more than one).
3. The original date of approval of the RM-Plan and the dates of all approved changes.
4. The policies and procedures for performing Security Analysis.
5. The procedures for complying with applicable interpretations.
6. A convincing argument to show that the described mechanisms, procedures, and tools are sufficient to address all changes to the product, including new features, bug fixes, and changes to satisfy Applicable Requirements.
7. The procedures for a VSA-performed RAMP Audit.
8. The procedures for RM-Plan maintenance.
9. The policy for using emergency procedures for correcting errors and for incorporating these corrections in subsequent scheduled product releases.
10. The format of the RAMP Evidence.
11. All updates necessary to reflect corrective measures taken after a RAMP process failure (e.g., failure to follow, or error in following, the RM-Plan), if one has occurred.

12. The CM-Plan.

RATING MAINTENANCE REPORT (RMR): Each RMR shall include the following:

1. A summary identifying each change that has been made since the previous evaluated release of the RAMP Product.
2. A description of all security-relevant changes and the Security Analysis of those changes.
3. A description of how the RAMP Product meets the Applicable Requirements.
4. Identification of all tools used for generating CIs.
5. The internal procedures used for restoring the RAMP process, if the RAMP Cycle covered by the RMR included a process failure. The description of the internal procedures must include the following:
    - The nature of the failure;
    - The Security Analysis conducted to establish corrective measures and verify product trust;
    - Establishment of the missing trail of evidence linking the evaluated product to the RAMP Product.
6. Results of the VSA-conducted RAMP Audit.
7. Results of the covert channel analysis.
8. Results of the system architecture study.
9. Results of penetration testing.
10. Results of specification to code mapping (A1 evauation class only).

RESPONSIBLE CORPORATE OFFICER: The Responsible Corporate Officer, or if the RCO has designated a VBPOC to act on behalf of the RCO, the VBPOC, shall:

1. Always be identified while the vendor is participating in RAMP and shall be responsible for the overall management of the vendor's RAMP effort.
2. Identify at least one VSA at all times while rating maintenance actions are underway.
3. Be responsible for submitting a proposed RM-Plan during the initial evaluation and shall obtain approval of the RM-Plan before entering the formal evaluation phase.
4. Ensure that all subsequent changes to the RM-Plan, to reflect all changes made in the vendor's implementation of the ratings maintenance process, are submitted to the NSA for approval.
5. Sign the cover letter of the proposed RM-Plan.
6. Sign the cover letter of the RMR.
7. Ensure that any requested RAMP Audit is conducted promptly following the request.
8. Be responsible for submitting, as directed by the TPOC, copies of the following materials at least four weeks in advance of the scheduled RAMP TRB:

- The RMR;
- The NSA-approved RM-Plan;
- The Updated Final Evaluation Report (FER);
- The proposed product description for the EPL.

SECURITY ANALYSIS: Security Analysis shall include the following:

1. Examining proposed changes to the RAMP Product for security relevance, including analyzing the effects on the TCB.
2. Reviewing the design and implementation of approved changes.
3. Ensuring that the RAMP Product is adequately tested including ensuring adequate test coverage through modification of the tests as necessary.
4. Ensuring that all documentation needed to show compliance with the Applicable Requirements, including design and user documentation, is updated consistently to reflect all changes to the TCB.

A change shall be considered to affect the TCB if it alters code or documentation within the identified TCB boundary, changes the TCB boundary, augments the TCB, or indirectly affects the function of TCB elements.

A change shall be considered security-relevant if it directly affects any mechanism implementing identified security policies (e.g., discretionary access control (DAC), object reuse, TCB isolation) or if it directly affects the maintenance of security data.

Security Analysis shall encompass cumulative effects involving all CI changes. (For example, two otherwise acceptable changes may conflict in terms of security because one assumes conditions that no longer hold, given the other change.) Security Analysis shall also consider the effects of interrelationships among the security features of the RAMP Product.

SECURITY ANALYSIS TEAM (SA-TEAM): The SA-Team shall perform the following activities.

1. Conduct, supervise, or monitor all Security Analysis tasks according to the NSA-approved RM-Plan.
2. Review and approve the Security Analysis prior to the submission of the RMR for the rating maintenance action.
3. Perform penetration testing.
4. Perform the system architecture study.
5. Ensure that, before the RMR is submitted, the relevant parts[3] of the entire security functional test suite used in the original evaluation, as updated during the RAMP Cycle, are successfully executed on a representative sample of hardware.

[3] In general, particularly at the B1 class and below, the entire test suite must be executed for each RAMP action because it is infeasible to determine with confidence which tests could not have been affected by the changes. If, however, the changes are very limited in scope, or there are parts of the test suite that can be shown to be unaffected, a subset of the tests may be performed. The rationale for any such limitations must be presented to the RAMP TRB Panel.

6. Review and approve the Updated FER.
7. Review and approve the RMR.
8. Demonstrate to the TRB that Security Analysis has been conducted according to the NSA-approved RM-Plan for each RAMP Cycle.
9. Present to the TRB the processes/methods used for performing penetration testing, covert channel analysis, system architecture study, and specification to code mapping.

VENDOR SECURITY ANALYST: A Vendor Security Analyst shall:

1. Successfully complete the NSA training program for VSAs (i.e., the VSA Class).
2. Deliver the vendor's Quarterly Status Reports (QSRs) to the vendor forum on the required schedule.
3. Present to the FCRB an overview of the changes to be made to the system during the RAMP Cycle and the preliminary Security Analysis of these changes. This presentation shall occur at the start of the RAMP Cycle.
4. Conduct an initial RAMP Audit prior to the original evaluation team's testing of the TCB. The results of this initial RAMP Audit shall be provided to the evaluation team.
5. Conduct at least one RAMP Audit[4] for each RAMP Cycle. The results of the RAMP Audit shall be included in the next quarterly status report following the RAMP Audit.

[4] This audit can be conducted in conjunction with the TPOC's audit.

Chapter 4
TPOC Requirements

A Technical Point of Contact (TPOC) is an evaluator, assigned by the National Security Agency (NSA), who serves as a consultant to a vendor while the vendor is in the Rating Maintenance Phase (RAMP) of NSA's Trusted Product Evaluation Program (TPEP). The TPOC is the interface between the vendor and the NSA, and reports to the NSA Branch Chief who is responsible for RAMP activity associated with the product.

A TPOC for a product is assigned by the NSA during the Evaluation Phase of the TPEP, with the TPOC most likely being a member of the Evaluation Phase team. It is likely that the NSA will assign more than one TPOC for a product, especially if the product is a complex one. During the Evaluation Phase, the TPOC works closely with the Team Leader to assure a smooth transition into RAMP.

During the Evaluation Phase, the team, in the absence of a TPOC, serves as the TPOC. Also, the team must deal with RAMP just as they deal with other issues during the Evaluation Phase.

4.1 TPOC Requirements

TPOC Requirements for products at all levels of trust follow. Only the first requirement differs for C2-B1 products vs B2-A1 products.

1. The first requirement is as follows:
   - For a B1-C2 product, the TPOC shall provide technical guidance concerning satisfying the Applicable Requirements for the product under RAMP;
   - For a B2-A1 product, the TPOC shall provide technical guidance to the vendor concerning the product under RAMP. In the event that a Security Analysis Team (SA-Team) is required by TPEP Management for the RAMP effort, the TPOC shall be the leader of the SA-Team.
2. The TPOC shall represent the vendor point-of-view in technical discussions that involve the evaluation community.
3. The TPOC shall provide quarterly status reports to the vendor evaluation forum by the fifth working day of the month during the months of January, April, July, and October.
4. The TPOC shall examine and assess the RAMP Evidence, including the Rating Maintenance Report (RMR), Rating Maintenance Plan (RM-Plan), updated Final Evaluation Report (FER), and Evaluated Products List (EPL) entry.
5. The TPOC shall examine all change descriptions for Configuration Item (CI) changes that are part of the RAMP action, including those that are not described by the RMR because they are not security-relevant.

6. The TPOC shall assess whether the vendor process requirements, for the Vendor Security Analysts (VSAs) and the Responsible Corporate Officer (RCO), have been satisfied during the RAMP action.

7. The TPOC shall prepare a cover letter describing the TPOC's assessment of the evaluation evidence and changes, and post it to the vendor forum.

8. The TPOC shall conduct at least one RAMP Audit[1] each RAMP Cycle. The results of the audit shall be included in the next Quarterly Status Report (QSR) following the RAMP Audit.

9. The TPOC, in cooperation with TPEP Management, shall schedule RAMP Technical Review Board (TRB) meetings.

10. The TPOC shall ensure that the Updated FER has been completed and shall be responsible for any updates to the Evaluator's Comments section.

11. At least four weeks prior to the scheduled RAMP TRB, the TPOC shall provide to NSA, and post to the vendor forum, a written report that describes the vendor's RAMP activity, the activity of the TPOC during the RAMP Cycle, and the results of the RAMP Audit. This report shall also contain the TPOC's written statement about the quality and accuracy of the Updated FER.[2]

12. The TPOC shall direct the vendor with respect to distribution of the following materials (one copy of the materials to each RAMP TRB member and applicable TPEP Management) in preparation for a scheduled RAMP TRB:

    - The RMR;
    - The approved RM-Plan;
    - The Updated FER;
    - The proposed product description for the EPL;
    - The TPOC's cover letter describing the assessment of evidence.

4.2 TPOC Guidance

The following guidance applies to the TPOC Requirements.

4.2.1 TPOC Technical Guidance to the Vendor.

The TPOC should not be considered as a replacement for the Evaluation Phase team, although the vendor for the product under RAMP can expect to receive some technical guidance from the TPOC. In the event the TPOC needs assistance in performing his/her duties, the TPOC should seek additional NSA resources via the NSA Branch Chief responsible for RAMP of the product.

[1] This audit can be conducted in conjunction with the VSA's audit.
[2] A suggested outline for this report is contained within Appendix E of this program document.

4.2.2 TPOC Representation of the Vendor's Position.

It is possible that during RAMP the TPOC might not agree with the vendor's point-of-view for a particular technical issue. It is essential, however, that the TPOC identify and represent the vendor's point-of-view while acting in the role of TPOC. As an example, the TPOC might enter a transaction on Dockmaster's `interp` forum that identifies her/him as a TPOC for Vendor X's product that is under RAMP, and goes on to represent the vendor's point-of-view relating to an issue. The TPOC would then be free, while acting outside of the role as TPOC, to respond to the transaction just described in a way that does not favor the vendor's point-of-view.

4.2.3 TPOC Recommendation About Revised RM-Plan Approval.

There must always be an NSA-approved Rating Maintenance Plan (RM-Plan) in effect for RAMP to proceed for a TPEP product. When a vendor desires to revise an approved RM-Plan, the TPOC must review the revised RM-Plan and write a summary that focuses on the revision and that includes a recommendation for approval or non-approval of the revised RM-Plan. The summary must also highlight any unusual or risky areas of which TPEP Management should be aware.

The TPOC then provides a copy of the Revised RM-Plan and the summary to the NSA Branch Chief responsible for the RAMP activity and to each RAMP Technical Review Board (TRB) member. Approval of the revised RM-Plan takes place through the same process (i.e., RAMP TRB) as approval of other changes to configuration items.

4.2.4 The TPOC and RAMP TRB Materials.

The TRB materials, specifically the Rating Maintenance Report (RMR), the approved RM-Plan, the Updated FER, and the proposed EPL entry for the product under RAMP, must be made available to the TPOC at least four weeks before the date of a scheduled RAMP TRB. The TPOC facilitates, in accordance with current distribution practices, the distribution of these materials to RAMP TRB members and to TPEP Management.

This page intentionally left blank

Chapter 5

The Technical Review Board

The primary goal of the Trusted Product Evaluation Program (TPEP) is to evaluate and place commercial-off-the-shelf trusted products on to the Evaluated Products List (EPL). The Technical Review Board (TRB) is responsible for assisting in ensuring the technical quality, uniformity, and consistency of TPEP evaluations. During the Rating Maintenance Phase (RAMP) each TRB member has the following responsibilities:

- To ensure that all Applicable Requirements of the evaluation criteria are interpreted correctly by each Vendor Security Analyst (VSA);
- To ensure that the evaluation criteria are applied consistently across all evaluations;
- To ensure the uniformity of evaluation procedures across all evaluations by enforcing a consistently high technical quality for all evaluations;
- To ensure that the VSAs' conclusions are supportable from the evidence presented;
- To ensure that the depth and breadth of analysis are consistent with the proposed rating of the trusted product;
- To provide recommendations to the TPEP Management relative to the quality of the VSAs' understanding of the product, the quality of the presentation of evidence reflected in the report and oral presentation, and the findings of the VSAs and any course of action proposed by them.

The TRB Panel reviews the vendor's NSA-approved Rating Maintenance Plan (RM-Plan), Rating Maintenance Report (RMR), Updated Final Evaluation Report (FER), and draft RAMP EPL entry, in order to determine if the product's rating has been maintained. No RAMP TRB will take place for a product until the FER (or Updated FER) of the previous evaluated version has been completed. Also, a RAMP TRB for a product will not take place until all the required actions from the previous TRB for that product are completed. Required actions are those that have been documented in the TRB Final Decision published by the Deputy Chief of C71.

5.1 TRB Review Process

The RAMP TRB review process is as follows:

1. The VSA is responsible for developing a final draft of the results of an evaluation and a proposed course of action for each major milestone.
2. The Branch Chief, in coordination with the Technical Point of Contact (TPOC), schedules a TRB meeting with the TRB Coordinator. No TRB meeting should be scheduled until the Branch Chief feels confident that the product meets all the requirements of the candidate class.

3. All reports submitted to the TRB should contain line numbers and be available in PostScript format. They should also include all relevant decisions and interpretations affecting the product.
4. Four weeks prior to the TRB meeting, the Vendor Security Analyst (VSA) submits the required documentation to the TPOC. The TPOC, within one week, then distributes the documentation to all applicable TRB members and to TPEP Management.
5. TRB members have two weeks to review the documentation and post comments, statements, and questions to the `TRB` forum. These comments are forwarded to the VSA and/or the TPOC by the TRB Coordinator.
6. In the final week before the TRB meeting, the VSAs (SA-Team at B2 and above) can use the posted comments to prepare their presentation to the TRB.
7. The VSAs (SA-Team at B2 and above) present findings to the TRB.
8. The TRB is allowed up to one week to post the final recommendations to the `TRB` forum. The recommendation is made available to the TPOC and/or the VSA.
9. After the TRB has posted the final recommendation, TPEP Management has up to one week to post the final decision. During this time, the VSAs (SA-Team at B2 and above) and TPEP technical advisors have an opportunity to express their concern to TPEP Management about the TRB recommendation.
10. A final decision can be to accept, reject, or conditionally accept the product. If the product is accepted a new RAMP Cycle for the product begins. If the product is rejected, the VSAs (SA-Team at B2 and above) must repeat all (or some) steps in the process and must defend the product before another RAMP TRB. When the product is conditionally accepted, it means that there are some actions that must be addressed by the VSAs (SA-Team at B2 and above) before the product can enter a new RAMP Cycle.

5.2 Scheduling

The TRB Coordinator can schedule TRB sessions up to nine months in advance. The TRB schedule is published every 30 days on the `TRB` forum and `Team_Leader` forum to reflect newly scheduled products. Initial Product Assessment Report (IPAR)/Test TRBs are scheduled for two days while Test, Final, and RAMP TRBs are scheduled for one day. The TRB session will begin mid-month on a Tuesday and end on a Thursday unless circumstances warrant otherwise.

5.2.1 Scheduling a TRB Date

TPOCs desiring to schedule a TRB should inform their Branch Chief. Once the TPOC and Branch Chief agree on a timeframe, the TRB Coordinator should be contacted to schedule a date.

5.2.2 Cancelling a TRB Date

TPOCs, and/or a Branch Chief wishing to cancel and/or reschedule a TRB date should immediately contact the TRB Coordinator. The TRB Coordinator will work to reschedule the TRB date if that is what is requested.

5.2.3 TRB Panel Scheduling

Each TRB session will have at least four primary members scheduled to appear at the TRB and one alternate member, who will be obligated to fill a primary member's position in case of schedule conflicts. If not required five weeks before the TRB session, the alternate will be excused from the TRB session. If within five weeks of the TRB session a primary member cannot attend, this member must find a replacement from the TRB membership. A different chair will be appointed for each product scheduled to be presented at the TRB session.

5.3 TRB Membership

TRB members are nominated by TPEP Management and appointed by the Chief of C71. Senior technical personnel are nominated for TRB membership based on their experience and expertise. TRB membership is open to all qualified individuals. TRB members participate in four to eight TRB sessions per year.

5.4 TRB Attendance

TRB sessions are treated as closed meetings. Attendance is mandatory for the TRB Panel and the evaluation team presenting the product. Attendance is optional for others within the evaluation community (e.g., TPEP personnel). Because seating is limited, anyone who desires to observe a TRB must make a seat reservation with the TRB Coordinator at least one week prior to the commencement of a TRB meeting. Failure to make a reservation can result in denial of access. The vendor may send the following individuals to the RAMP TRB reviewing the vendor's product:

- All TPEP-recognized VSAs for that specific product may attend and present that product to members of the TRB;
- The appropriate Responsible Corporate Officer (RCO) for that product may attend the TRB to observe the presentations;
- A maximum of three developers associated with the vendor and that product may attend the TRB to observe the presentations.

This page intentionally left blank

Chapter 6

The Future Change Review Board

It is envisioned that more National Security Agency (NSA) involvement during the Rating Maintenance Phase (RAMP) will be required for higher assurance (B2-A1) products than for lower assurance (C2-B1) products, with the increased involvement being in the form of the possible committment of NSA resources to a Security Analysis Team (SA-Team). A Future Change Review Board (FCRB) meeting is always held for products at the B2 through A1 evaluation classes, and may, on approval of Trusted Product Evaluation Program (TPEP) Management, be held for C2 and B1 products.

Because all the types of changes that vendors may make during RAMP cannot be predicted, nor can the scope of changes that vendors may make be quantified, it is very difficult to identify objective criteria for determining the composition of a SA-Team during RAMP. To assist in making this determination, a FCRB will be convened to make a recommendation to Trusted Product Evaluation Program (TPEP) Management on the composition of the SA-Team. Based on the FCRB's recommendation, TPEP Management will make a resource decision concerning how, or whether, to proceed with the proposed RAMP action.

6.1 Purpose

The FCRB is a panel that reviews proposed changes in evaluated products. After the review, it makes a recommendation to TPEP Management regarding the nature and extent of the analysis to be performed by the SA-Team, the composition of the SA-Team, and the nature of SA-Team's presentation to the RAMP Technical Review Board (TRB). These recommendations are based on the FCRB's analysis of the scope and complexity of the proposed changes, and the degree to which the changes will affect security-relevant aspects of the product.

The SA-Team composition recommendation may include only VSA(s), VSA(s) and TPOC(s), or a combination of VSA(s), TPOC(s), and other NSA evaluators, possibly with expertise in special areas. Recommendations for specific evaluator expertise will be made as the proposed changes warrant; for example, a "port" from a single-processor to multi-processor hardware platform would likely need specific expertise in covert channel analysis. Additional evaluators may also be recommended when the proposed changes require significant work to evaluate.

The SA-Team may be required to present its results to the RAMP TRB panel either electronically (i.e., by providing just the Rating Maintenance Report (RMR)) or in person (as well as providing the report). The former option would be recommended when the changes are straightforward and the security-relevant aspects are entirely clear at the time of the FCRB presentation. The latter would be recommended when the changes are complex or where the full security impacts are not yet clear.

The FCRB recommendation will include schedule, level of effort for analysis, required personnel expertise, and nature of presentation to the RAMP TRB.[1] The level of effort recommended by the FCRB can range

[1] This might involve no RAMP TRB presentation; only an on-line interaction with the RAMP TRB; etc.

from nothing beyond the routine Security Analysis performed by the VSA(s), to a significant evaluation effort involving multiple NSA evaluators in addition to the VSA(s) and TPOC(s).

6.2 FCRB Agenda

FCRB members will receive a summary of changes to be presented at the FCRB and a copy of the previous Final Evaluation Report (FER) or Updated FER (if it is one that has not yet been published and available to all FCRB members) two weeks prior to the scheduled FCRB. This serves as background reading for the FCRB members and allows them to think about the scope of changes contemplated by the vendor. The FCRB is not expected to provide written comments to the vendor or the TPOC.

The day of the FCRB, the TPOC will introduce the VSA to the FCRB. The VSA will then present the types of changes to be made during this RAMP Cycle along with a preliminary Security Analysis of the proposed changes.

6.3 FCRB Membership

FCRB members are nominated by the TPOC, the Chief Evaluator, the Senior Evaluator, and the RAMP Working Group and are appointed by the Chief of C71. They are drawn from the TRB members, senior technical evaluators, and TPEP Management. Ultimately, it is envisioned that the FCRB will consist of the regularly scheduled TRB, plus one person (if necessary) who is very familiar with the system being evaluated.

6.4 FCRB Review Process

The FCRB review process is as follows:

1. The Branch Chief, in coordination with the TPOC, schedules an FCRB meeting with the TRB Coordinator. No FCRB meeting is scheduled until a legal agreement has been signed and the RM-Plan has been approved.

2. Three weeks prior to the FCRB meeting, a VSA submits to the TPOC a written summary of proposed product changes to be presented at the upcoming FCRB.

3. Three weeks prior to the FCRB meeting, the TPOC submits the vendor proposed product changes summary and a copy of the Final Evaluation Report (FER) or Updated FER (if not yet printed and distributed) to NSA's distribution organization. The distribution organization prepares and distributes the documentation to all FCRB members and staff within one week. This information is background reading for the FCRB. The FCRB is not expected to prepare written comments for the vendor.

4. The VSA presents proposed product changes to the FCRB.

5. The FCRB chair within one week posts a final recommendations to the TRB forum. This recommendation is made available to the TPOC and/or the VSA.

6. After the FCRB chair has posted a final recommendation, C71 has up to one week to post the final decision. During this week, the evaluation team and C71 technical advisors have an opportunity to express their concern to TPEP Management about the FCRB recommendation.
7. The final decision determines the composition of the SA-Team and the committment of NSA resources to the effort.

6.5 Scheduling

FCRB meetings are held during normally scheduled TRB sessions. An FCRB, however, is always a distinct activity: it must be requested separately from the RAMP TRB, and is perrformed only after all the RAMP TRB activities have been completed. The presentations for RAMP TRB and FCRB may not be combined.

6.6 FCRB Attendance

FCRB sessions are treated as closed meetings. Attendance is mandatory for the FCRB Panel, the TPOCs and VSAs for the product being discussed, and is optional for all others within the evaluation community. Seating at a FCRB is limited, so anyone who desires to observe a FCRB must make a seat reservation with the TRB Coordinator at least one week prior to the commencement of a FCRB meeting. Failure to make a reservation can result in denial of access. The vendor whose product will be discussed at a FCRB Meeting may send the following individuals to the FCRB:

1. All NSA-recognized VSAs for the product may attend and present that product to the FCRB. If a vendor has several products participating in RAMP, only the VSAs representing the product that is the focus of the FCRB may attend.
2. The appropriate Responsible Corporate Officer (RCO) for the product that is the focus of the FCRB may attend the FCRB to observe the presentations.
3. A maximum of three developers associated with the vendor whose product is the focus of the FCRB may attend the FCRB to observe the presentations.

This page intentionally left blank

Chapter 7

The VSA Class

Within the Rating Maintenance Phase (RAMP) Requirements, a Vendor Security Analyst (VSA) is defined as "...the vendor personnel responsible for execution of all technical tasks in RAMP," and a VSA requirement is that "VSA candidates shall successfully complete the National Security Agency (NSA) training program for VSAs." Although formally known as the "National Security Agency's Vendor Security Analyst Training Class," the phrases "VSA Class" or "RAMP Class" are commonly used to refer to this training class.

Typically, the VSA Class is conducted semiannually, with one class offered in the March/April timeframe and the other in the August/September timeframe. Requests for VSA Class registration are posted on the Dockmaster `vsa` forum. Registration can take place either via Dockmaster or by FAX. The NSA assumes no responsibility for the selection of a VSA by a vendor, and, in particular, the consequences of an inappropriate selection of a VSA by a vendor.

The VSA Class consists of two components: a Non-Resident Component and a Resident Component. The Non-Resident Component is completed at the vendor site, and the Resident Component is completed at a site in the Baltimore, Maryland, area. The VSA Class addresses, but is not limited to, the following major areas:

- General principles of computer security;
- **Trusted Computer System Evaluation Criteria** (TCSEC) requirements, including interpretations;
- Security issues in the system development process;
- All aspects of RAMP.

Upon successful completion of the VSA Class, NSA, through its INFOSEC Outreach Program, identifies each VSA as a **Certified Security Advocate** in the discipline of trusted product rating maintenance.[1] If, at any time, a VSA is *not* associated with a vendor product under NSA's Trusted Product Evaluation Program (TPEP), then the VSA is identified not as a Certified Security Advocate but as a **Security Advocate**. A Security Advocate can reapply to NSA to once again become a Certified Security Advocate provided this individual is sponsored by a vendor having an association with NSA's TPEP, and provided that the individual would be a VSA for that vendor's product.

[1] As of 1 February 1994, all current VSAs are "grandfathered" into the INFOSEC Outreach Program as Certified Security Advocates.

7.1 Registration

The first step in the VSA Class registration process is for the Responsible Corporate Officer (RCO) to forward a completed registration form to the RAMP Coordinator.[2] Ideally, the RCO will provide the NSA with the completed registration form several months prior to the beginning of the Resident Component of the VSA Class. An RCO can identify more than one VSA candidate for participation in a particular VSA Class. In such a case, a separate completed registration form should be submitted for each candidate.

If the NSA accepts a VSA candidate into the VSA Class, the NSA will notify both the RCO and the VSA candidate via United States Mail.

7.2 Non-Resident Component

Approximately six weeks prior to the beginning of the Resident Component, the VSA candidate will receive the following via United States Mail:

- A set of instructions relating to the VSA Class as a whole;
- A collection of TCSEC self-paced study modules and related self-tests;
- A collection of **Trusted Network Interpretation** (TNI) self-paced study modules and related self-tests;
- A collection of **Trusted Database Management System Interpretation** (TDI) self-paced study modules and related self-tests;
- Copies of articles that supplement the course modules;
- A self-administered examination based on the study materials identified above, and instructions describing when and how to return the completed examination to the NSA.

In addition to the materials provided by NSA, above, the following books should be obtained by each VSA candidate, since the self-paced study modules require readings from these books. The Tanenbaum book is also used during the Resident Component of the VSA Class.

- **Operating Systems: Design and Implementation**, Andrew S. Tanenbaum, Prentice Hall, 1987; ISBN 0-13-637406-9 025.
- **Building a Secure Computer System**, Morrie Gasser, Van Nostrand Reinhold, 1988; ISBN 0-442-23022-2.
- **Research Directions in Database Security**, Teresa Lunt, Springer-Verlag, 1992; ISBN 0-387-97736-8.

[2] The RAMP Coordinator will be identified within the posting(s) relating to the VSA Class that will appear on the Dockmaster `vsa` forum.

Prior to taking the self-administered examination, which is returned to the NSA approximately two weeks prior to the beginning of the Resident Component of the VSA Class, a VSA candidate should expect to invest 80-100 hours of study time into the Non-Resident Component. Students will not be admitted to the Resident Component if their examination has not been received by the NSA prior to the beginning of the Resident Component.

7.3 Resident Component

The Resident Component of the VSA Class is a five day formal training period that provides attendees with RAMP-specific information, and that models numerous tasks that a VSA is required to perform during a RAMP Cycle. The RAMP Class culminates with each attendee making a presentation before a mock RAMP Technical Review Board (TRB).

During the Resident Component, which focuses on the RAMP Requirements, students are introduced to Trusted MINIX,[3] a derivative of the MINIX Operating System,[4] and an approach to its security analysis. As the week progresses, class participants break into groups that simulate vendor RAMP teams, and each member of each group selects a Service Improvement Request (SIR) for possible implementation within Trusted MINIX. Each group member performs security analysis, generates an Engineering Change Order (ECO), and writes a section of an Rating Maintenance Report (RMR). The RMR is submitted to and defended before a mock TRB panel.

[3] For purposes of the VSA Class it is assumed that Trusted MINIX has been successfully evaluated at the C2 level of trust.

[4] The MINIX Operating System was invented by Andrew S. Tanenbaum and is described within the book **Operating Systems: Design and Implementation**, Andrew S. Tanenbaum, Prentice Hall, 1987: ISBN 0-13-637406-9 025.

This page intentionally left blank

Appendix A
Sample RM-Plan Outline

A Rating Maintenance Plan (RM-Plan) that is written from the appropriate RM-Plan requirements, and that adequately addresses each applicable requirement, should result in a solid RM-Plan. Consistent with this, it is suggested that an appendix of a vendor's RM-Plan contain the entire set of applicable Rating Maintenance Phase (RAMP) Requirements, and that another appendix contain a mapping that shows how the RM-Plan meets the RAMP Requirements.

It is emphasized that the RM-Plan outline presented below is merely an example, and that it is not required. The suggestions that are offered are based on experience that the National Security Agency (NSA) has had with RM-Plans to date. If the outline is adopted, the vendor can decide whether or not to devote an entire section or appendix to a particular topic, or to reduce the number of sections and/or appendixes by addressing multiple topics within a particular section or appendix.

A.1 Cover Page

The contents of this page should identify the product that will be or is under RAMP. In addition, the name of the author(s) of the document should be shown, as well as the date the document was written. The cover page should also identify the date that the NSA approved the RM-Plan, if it has been approved, and should show the history of any prior RM-Plan approval(s).

A.2 Roman Numeral Page(s)

The "Roman numeral page(s)" of the RM-Plan can be used to contain information that might be expected to be modified during the life of the RM-Plan. This information includes the following:

- The name and company title of the Responsible Corporate Officer (RCO);
- The name and company title of the Vendor Business Point of Contact (VBPOC), if a VBPOC is identified;
- The name and company title of the Vendor Security Analyst (VSA), or of each VSA if there are more than one;
- The date and Evaluated Products List (EPL) entry number for each Dockmaster EPL posting relating to the product;
- The title, date, Report Number, and Library Number of the Final Evaluation Report (FER) and each Updated FER associated with the product.

Since changes to an RM-Plan might involve one or more of the items identified above, placement of these items in a common location should simplify the RM-Plan approval process, especially if the only change(s) to an RM-Plan involves one or more of these items.

A.3 Introduction

It is recommended that the Introduction section of the RM-Plan contain a pointer to the applicable RAMP Requirements, and that all definitions within the applicable RAMP Requirements be adopted as definitions for use within the RM-Plan.

In addition, the Introduction section should contain a one or two page overview of the product, along with a pointer to the most recent FER or Updated FER identified within the "Roman numeral page(s)" of the RM-Plan. Other vendor-specific definitions and conventions could also be identified within the Introduction section.

The Introduction section is also a good place to emphasize the role of the VSA in RAMP, and to address the requirement that the RM-Plan shall describe "the division of technical responsibilities among VSAs (if more than one)."

A.4 Procedure for Complying with Applicable Interpretations

The NSA periodically issues interpretations of the **Trusted Computer System Evaluation Criteria** (TCSEC). These interpretations become part of the TCSEC, and as such, must be addressed. Products in RAMP under the Trusted Product Evaluation Program (TPEP) must comply with applicable TCSEC interpretations. This section of the RM-Plan should describe how the vendor will comply with TCSEC interpretations that might impact a product under RAMP. Issues to be addressed include the following:

- A description of how the vendor will monitor interpretations of the TCSEC;
- A description of how the vendor will determine if an interpretation is applicable to their product under RAMP;
- A description of how the vendor will comply with any applicable interpretation(s) that impact their product under RAMP.

A.5 Configuration Items and Rationale

It is recommended that each Configuration Item (CI) be listed in an appendix of the RM-Plan. In addition, that appendix would be an appropriate place to describe the rationale for CI identification.

There should be an indication about the access the Vendor Security Analyst (VSA) has to each CI, specifically, where each CI is kept and the method of VSA access. CI access is very important, since the VSA must have access to each CI in order to perform Security Analysis.

A.6 Security Analysis

Since Security Analysis is the centerpiece of RAMP, the vendor must be sure that the Security Analysis section of the RM-Plan describes in detail how Security Analysis is performed for the product under RAMP. It is essential that the role the VSA plays in Security Analysis be identified, especially in terms of the applicable RAMP Requirements. Diagrams, tracking forms, examples, etc., should be used within this section to convey to the reader of the RM-Plan how product changes are made and how Security Analysis is performed. A vendor should view the development of the Security Analysis section of the RM-Plan as requiring a major level of effort during the RM-Plan development process.

A.7 Format of the RAMP Evidence

By definition, RAMP Evidence is the record of Security Analysis. It is the summary of RAMP Evidence that is contained within the Rating Maintenance Report (RMR) that is submitted to the RAMP Technical Review Board (TRB). It is thus essential that the vendor carefully consider what the RAMP Evidence will be and that the format of the evidence be identified and explained within this section of the RM-Plan. For example, a vendor database that is used to track changes to an evaluated product might be identified as a source of RAMP Evidence. If so, the RM-Plan should identify this database, describe the fields contained within it, and describe the role the database will play in Security Analysis.

A.8 Procedures for VSA-Performed RAMP Audits

A VSA is required to conduct an initial RAMP Audit prior to the evaluation team's testing of the Trusted Computing Base (TCB). In addition, a VSA is required to conduct a RAMP Audit during each RAMP Cycle. This section of the RM-Plan should describe the approach that the VSA will take while conducting a RAMP Audit. Topics that should be covered in this section include the following:

- Identification of the specific RAMP Evidence that will be audited;
- A description of how the RAMP Evidence will be selected for audit, including the approximate percentage of the RAMP Evidence that will be audited;
- A discussion of the depth of the audit.

A.9 RM-Plan Maintenance

There must always be an NSA-approved RM-Plan in place for RAMP to continue. In addition, the NSA-approved RM-Plan is a configuration item under RAMP. Due to these factors, the vendor must describe how the RM-Plan will be managed during RAMP to assure that an NSA-approved RM-Plan is in effect at all times.

A.10 System Failures During RAMP

It is possible that a system failure requiring an emergency fix may occur during RAMP. The vendor must describe how this type of failure will be addressed should it occur.

A.11 Other Sections

As required by the vendor to provide a complete RM-Plan.

A.12 Appendix A - RAMP Requirements

A listing of the applicable RAMP Requirements as they appear within Chapter 3 of this **Rating Maintenance Phase Program Document Version 2**.

A.13 Appendix B - RAMP Requirements Mapping

A table of pointers that demonstrate how the RAMP Requirements shown in Appendix A are satisfied by the current RM-Plan. Particular attention should be paid to the RM-Plan requirements that are contained within the set of RAMP Requirements shown in Appendix A.[1]

A.14 Appendix C, etc.

As required by the vendor to provide a complete RM-Plan. The following are suggested, however:

- Template(s) used for a change request;
- Sample output from a tracking system database.

[1] Although Appendix A and Appendix B might be combined into one appendix, it is recommended that they remain separate so that the RM-Plan reader has available in Appendix A the RAMP Requirements in their original form and without entries that have been made by the vendor.

Appendix B
Sample RMR Outline

The Rating Maintenance Report (RMR) is the summary of Rating Maintenance Phase (RAMP) Evidence that is submitted by the Responsible Corporate Officer (RCO) to the RAMP Technical Review Board (TRB) during a RAMP Cycle. RMR requirements are contained within the set of applicable RAMP Requirements, and the RMR should be written such that the RMR requirements are fully addressed. The following RMR outline is *suggested* but *not required*; it is intended to provide guidance to the vendor community.

B.1 Cover Letter

This letter should be addressed to the Chief of NSA's Trusted Product Evaluation Program (TPEP), and should include the following:

- Identification of the new product version, the evaluated product, and any intervening product releases;
- Identification of the product rating established in the evaluation and maintained through the previous release;
- Serial number of the Final Evaluation Report (FER), and serial numbers of Updated FER(s);
- An assertion that the new release maintains the product rating;
- A statement that all aspects of the National Security Agency (NSA)-approved Rating Maintenance Plan (RM-Plan) were followed during the current RAMP Cycle, and that the contents of the RMR reflects a true account of the RAMP Evidence generated during the current RAMP Cycle;
- The signature of the RCO.

B.2 Introduction

The intent of the **Introduction** is to provide the reader of the RMR with a high-level description of the changes that have been made to the product since the latest Evaluated Products List (EPL) entry was made. Since the vendor submits the NSA-approved Rating Maintenance Plan (RM-Plan), the Final Evaluation Report (FER) or most recent Updated FER, and the RMR to the RAMP TRB, pointers within the RMR to sections of the most recent FER, and/or the NSA-approved RM-Plan can be provided. This will result in an RMR focusing on the RAMP Evidence that was generated during the current RAMP Cycle.

Topics to be covered in the Introduction section of the RMR include the following:

- Identification of any vendor-unique terms used within the RMR;

- Identification of the Trusted Computing Base (TCB) for the original evaluated product in terms of hardware, software, and firmware;
- A discussion of the rationale for Configuration Item (CI) identification for the product under RAMP;
- A list of the CIs for the product under RAMP;
- A list of updated CIs due to product changes during the current RAMP Cycle;
- The rationale for determining effects on the TCB of product changes.

Finally, since the vendor should run the entire security test suite on the product prior to RMR submission, a statement to this effect, including test results, should appear within the RMR, with the Introduction section being a good place to include this information.

B.3 Criteria Interpretations

This section of the RMR is intended to address any **Trusted Computer System Evaluation Criteria** (TCSEC) interpretations that have impacted the product during the current RAMP Cycle. For each such interpretation, the following should be addressed in this section:

- Each TCSEC interpretation applying to the product for the first time should be identified, and comments on the significance of each of these interpretations to the current product release should be provided;
- Pointers should be provided to discussions in the RMR section on "Product Changes and Evidence of System Trust" wherein product changes were made during the current RAMP Cycle because of specific TCSEC interpretation(s).

B.4 Product Changes and Evidence of System Trust

This section is the centerpiece of the RMR, and should address all security-relevant changes that have been made to the product since the last EPL entry. Since the focus of the RAMP is on security-relevant changes, it is suggested that all changes determined to be non-security-relevant be briefly identified within an appendix of the RMR. The identification should be in the form of a one or two line meaningful title that conveys the nature of the change to the RMR reader, as well as an associated vendor reference; for example, an Engineering Change Order (ECO) number.[1] This reference would allow the vendor to provide the NSA with information about a non-security relevant change in a timely manner, if so requested. Similarly, for security-relevant changes determined to be "minor" in nature, another appendix can be used to briefly identify each. A one or two line meaningful title, and an associated ECO reference should be sufficient.

The "Product Changes and Evidence of System Trust" section of the RMR could open with a brief overview of the contents of the section, including pointers to the two appendixes identified above. The remainder of

[1] A vendor might use different terminology. This terminology would be described within the "vendor-specific terminology" portion of the **Introduction** section of the RMR.

this section can then focus on the "major" security-relevant changes that have been made to the product during the current RAMP Cycle. For each, the following should be addressed:

- A description of the change that includes the following:
  1. A functional description.
  2. A description of user-visible effects.
- The ECO number associated with the change;
- Identification of the CIs that were modified, if any, as a result of the change;
- Classification of the change as being or not being security-relevant;
- Evidence of product trust to include the following:
  1. Explanation of relevant TCSEC interpretations, if any.
  2. Relevant TCB mechanisms and assurances.
  3. Tests and test modifications, if any.
  4. Summary of test results.
  5. Pointers to system and test documentation.
  6. Pointers to specific code-level changes.

B.5 Appendix A - Non-Security-Relevant Changes

This appendix would contain a list of non-security-relevant changes, including a one or two line meaningful title for each, and an associated vendor reference for each.

B.6 Appendix B - "Minor" Security-Relevant Changes

This appendix would contain a list of "minor" security-relevant changes, including a one or two line meaningful title for each, and an associated vendor reference for each.

B.7 Appendix C, etc.

As required by the vendor to provide a complete RMR.

This page intentionally left blank

Appendix C
RAMP Audit

The Rating Maintenance Phase (RAMP) Requirements at all levels of trust provide the following definition of the RAMP Audit.

RAMP AUDIT: A review of the RAMP Evidence, based on a suitable representative sample, to ensure that only approved changes are implemented, that all Configuration Items (CIs) are updated consistently, and that Security Analysis is performed satisfactorily. In addition to the required RAMP Audits performed by the Vendor Security Analysts (VSAs), aperiodic RAMP audits may be performed by a Security Analysis Team (for B2 and above) or the Technical Point of Contact (TPOC).[1]

There are two purposes of a RAMP Audit, namely to verify compliance with the RAMP process, and to check the Security Analysis that has been performed.

C.1 RAMP Audits in General

There are two "types" of NSA-conducted RAMP Audits, the first occurring prior to the team's testing of the Trusted Computing Base (TCB), and the second occurring during each RAMP Cycle. In addition, there are two "types" of VSA-conducted RAMP Audits, the first occurring prior to the team's testing of the TCB, and the second occurring during each RAMP Cycle.

The first "type" of RAMP Audit, that conducted during the evaluation and prior to the Test Technical Review Board (TRB), is intended to assure that the policies and procedures identified within the NSA-approved Rating Maintenance Plan (RM-Plan) are in place.

The second "type" of RAMP Audit, that conducted during each RAMP Cycle, is the one whose focus is on the RAMP AUDIT requirement. It is during this type of RAMP Audit that the RAMP Evidence is examined to ascertain that only approved changes have been implemented, that all CIs have been updated consistently, and that Security Analysis has been performed satisfactorily.

C.2 A "Suitable Representative Sample"

The definition of RAMP Audit states that a "suitable representative sample" of the RAMP Evidence must be reviewed during the audit. This raises the question of "What constitutes a suitable representative sample?" This question is not easy to answer. A starting point, however, might be to focus on the RAMP Evidence as a whole, then to break it out into three areas, as follows:

[1] Although not a RAMP Requirement, a vendor can expect that the National Security Agency (NSA) will allow the vendor at least ten (10) working days to prepare for an aperiodic RAMP Audit.

- Major security-relevant changes (e.g., implementation of new features within the product);
- Minor security-relevant changes (e.g., security-relevant bug fixes);
- Non-security-relevant changes (e.g., non-security-relevant bug fixes).

If, as a rule-of-thumb, approximately 10% of the entire RAMP Evidence is subjected to a RAMP Audit, then the following break-out would be reasonable concerning the 10%:

- Direct 70% of the RAMP Audit effort in the area of major security-relevant changes;
- Direct 20% of the RAMP Audit effort in the area of minor security-relevant changes;
- Direct 10% of the RAMP Audit effort in the area of non-security-relevant changes.

C.3 VSA-Conducted RAMP Audits

VSA-conducted RAMP Audits should focus on assuring that the RAMP Audit requirement is met by the vendor.

C.4 NSA-Conducted RAMP Audits

A starting point for the NSA-conducted RAMP Audits would be a vendor/NSA discussion, perhaps originating from a vendor briefing, about the nature of the changes that have been made to the product since the last NSA-conducted RAMP Audit, with emphasis on how these changes were implemented. As a result of this discussion, the National Security Agency (NSA) representative(s) should feel comfortable that all changes made to the system were consistent, in concept, with the mechanisms described within the NSA-approved RM-Plan for the product.

The next step would be for the NSA representative(s) to request the Vendor Security Analyst (VSA) to demonstrate to the NSA that changes to the product have been made in an acceptable manner, as described within the NSA-approved RM-Plan. There would most likely be a one or two week interval between the discussion described above and the evidence demonstration. During this interval, the NSA would identify to the VSA exactly what evidence demonstration must be provided. Suggestions are as follows:

- A demonstration, using real examples, of VSA access to all CIs identified within the NSA-approved RM-Plan;
- A VSA-conducted demonstration of the Security Analysis that was performed for each of the following types of changes, including a demonstration of all tools used to support the Security Analysis process (e.g., on-line tracking system):
  1. A specific "major" security-relevant change.
  2. A specific "minor" security-relevant change.
  3. A specific non-security-relevant change.

- A demonstration, using real examples, of CI update methodology for each of the following types of CIs:

    1. Hardware CI;
    2. Software CI;
    3. Firmware CI;
    4. Documentation CI;
    5. Security test suite CI.

This page intentionally left blank

Appendix D

Sample QSR Outline

During the Rating Maintenance Phase (RAMP) a Quarterly Status Report (QSR) must be posted on the vendor forum by both the Vendor Security Analyst (VSA) and Technical Point of Contact (TPOC) by the fifth working day of the months of January, April, July, and October. Each QSR should have as its subject line "Quarterly Status Report," and have the following format:

Product Identification: This section should include information such as:

- Vendor name and address;
- Product name and version;
- Identification of Evaluated Products List (EPL) entries for this product;
- Platform;
- Product availability date;
- Other information as determined necessary.

Accomplishments this Quarter: A list of what has transpired since the previous QSR, including brief descriptions where appropriate, should be contained within this section.

Plans for Next Quarter: A list of what is expected to occur before the next QSR should be contained within this section.

Major Milestones: This section includes identifying events such as:

- Implementation completion (e.g., of a new product feature);
- Testing completion;
- RAMP Audit activity;
- RAMP Technical Review Board (TRB) presentation.

Outstanding Technical Issues and Concerns: A list of any technically-based questions or issues which have yet to be answered should be contained within this section.

Outstanding Management Issues: A list of any managerial questions or issues which have yet to be answered should be contained within this section.

Membership List: A list of TPOCs, VSAs, and the technical and managerial leaders of both vendor and Trusted Product Evaluation Program (TPEP), including addresses and telephone numbers, should appear within this section.

This page intentionally left blank

Appendix E
Sample TPOC Report

The Technical Point of Contact (TPOC) Report is the summary of the TPOC's assessment of the activities performed in the course of the Rating Maintenance Phase (RAMP) Cycle. The report identifies the main events that occured during the RAMP Cycle being reported. Emphasis (that is, greater detail) is given to the decriptions of those acivities where the TPOC has a more active role. The activities of the Vendor Security Analysts (VSAs) are described in the Rating Maintenance Report (RMR). The following TPOC Report outline is *suggested* but *not required*; it is intended to provide guidance to the TPOCs.

E.1 Introduction

The introduction should provide a brief overview of the activities since the previous RAMP Technical Review Board (TRB) meeting (or, for an initial RAMP Cycle, since the Final TRB). This overview should include identification of version numbers, timeframes when milestones were reached, management issues, interpretations, and any other information that would be of interest to the TRB. For RAMP Cycles for which a Future Change Review Board (FCRB) meeting was held, the introduction should also include a list of the tasks that the FCRB recommended be done.

E.2 Assessment of FER

The TPOC must provide to the TRB an assessment of the quality and accuracy of the Updated Final Evaluation Report (FER). This assessment should include the identification of major additions, deletions, or changes to the FER. This would be fairly high-level, primarily because the TRB will have a copy of the Updated FER.

E.3 Summary of RAMP Audit

Because the RAMP Audit is the primary activity where the TPOC checks the work of the VSAs, this section is the focus of the TPOC report. This is where the TPOC describes the activities of the RAMP Audit. This includes not only the activities themselves, but also an assessment of the outcome. Any problems that were encountered, along with their resolutions, should be described. The TPOC may also want to include an identification of the participants of the RAMP Audit.

E.4 Testing

A summary of the results of the testing effort should be described. This description includes the TPOCs role during testing, any tests that were added to the vendor's test suites during this RAMP Cycle, and an assertion that all of the tests ran favorably.

For B2 and above classes, a description of the Penetration Testing excercise should also be included. Like the description of RAMP audit, this description should contain more detail, because the TPOCs role is more active than, say, the functional testing effort.

E.5 FCRB-Recommended Activities

This section should provide details on the tasks recommended by the FCRB (listed in the "Introduction" section of the TPOC report). Each item should have its own description at a level of detail equivalent to that of Penetration Testing or the RAMP Audit.

Appendix F

Acronyms

CI Configuration Item

CM Configuration Management

CM-Plan Configuration Management Plan

CSSI **Computer Security Subsystem Interpretation**

DAC Discretionary Access Control

DOD Department of Defense

ECO Engineering Change Order

EPL Evaluated Products List

FCRB Future Change Review Board

FER Final Evaluation Report

IPAR Initial Product Assessment Report

IPTR Intensive Preliminary Technical Review

NCSC National Computer Security Center

NSA National Security Agency

NIST National Institute for Standards and Technology

QSR Quarterly Status Report

RAMP Rating Maintenance Phase

RCO Responsible Corporate Officer

RM-Plan Rating Maintenance Plan

RMR Rating Maintenance Report

SA-Team Security Analysis Team

SFUG Security Features User's Guide

SIR Service Improvement Request

TCB Trusted Computing Base

TCSEC **Trusted Computer System Evaluation Criteria**

TDI **Trusted Database Management System Interpretation**

TFM Trusted Facility Manual

TNI **Trusted Network Interpretation**

TPEP Trusted Product Evaluation Program

TPOC Technical Point of Contact

TRB Technical Review Board

VBPOC Vendor Business Point of Contact

VSA Vendor Security Analyst