Rating Maintenance Phase Program

NCSC-TG-013-89

Library No. S-232,468

Version - 1

FOREWORD

The National Computer Security Center has established an aggressive program to study and implement computer security technology, and to encourage the widespread availability of trusted computer products for use by any organization desiring better protection of their important data. The Trusted Product Evaluation Program, and the open and cooperative business relationship being forged with the computer and telecommunications industries, will result in the fulfillment of our country's computer security requirement. We are resolved to meet the challenge of identifying trusted computer products suitable for use in protecting information.

"Rating Maintenance Phase Program Document" is the latest in the series of technical guidelines published by the National Computer Security Center. The Rating Maintenance Phase (RAMP) of the Trusted Product Evaluation Program provides for the maintenance of computer security ratings across product revisions. This document describes RAMP for current and prospective vendors of trusted systems. The primary objectives are to provide formal statements of program requirements and to provide guidance on addressing them.

As the Director, National Computer Security Center, I invite your recommendations for revising this technical guideline. We plan to review this document as the need arises.

_____

Patrick R. Gallagher, Jr.

23 June 1989

- Director, National Computer Security Center

ACKNOWLEDGMENTS

The National Computer Security Center extends special recognition and acknowledgment to Tommy Hammer, Ph.D., as principal author of this document and to LT Patricia R. Toth (USN) as project manager for the publication of this document.

We wish to thank the following for their contributions in developing the concepts and procedures of rating maintenance characterized by this document: Blaine Burnham, Ph.D., David M. Chizmadia, Donald Crossman, Major Doug Hardie, Howard Israel, Shawn P. O'Brien, Michael J. Oehler, Mary D. Schanken, Dana Nell Stigdon, John W. Taylor, and W. Stan Wisseman.

1. OVERVIEW OF THE RATING MAINTENANCE PHASE

1.1 BACKGROUND AND CHARACTERISTICS OF RAMP

The National Computer Security Center (the Center) evaluates commercially marketed products against the

Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) classes D through A1. Each evaluation by the Center yields a TCSEC class designation, or rating, for the given product. The Center publishes these ratings in the Evaluated Products List (EPL), which is widely cited in computer system procurements. The Center thus works in partnership with private industry to establish product trust.

The purpose of the Rating Maintenance Phase (RAMP) is to provide currently available trusted products. RAMP is essential for this purpose because of the frequency with which many vendors revise their offerings. Vendors often market new releases of a product every few months and keep multiple versions under development at all times. Without RAMP, only the initial evaluated version is a trusted system with a TCSEC rating. RAMP allows the Center to establish a rating and an EPL listing for each product release following an evaluated release.

RAMP is intended to yield an EPL listing for a revised product shortly after its release date. This outcome is possible because RAMP builds cumulatively upon the evidence and assurance established by a product evaluation, and because the vendor bears primary responsibility in RAMP for maintaining product trust as the system evolves. The vendor follows strict procedures that integrate security analysis, configuration management, and evidence accumulation into the development process. The Center then extends the product rating to each successive release by ascertaining that the vendor has executed all rating maintenance responsibilities fully and correctly.

RAMP always builds upon a product evaluation; it provides no opportunity to avoid an evaluation. The program does not diminish the role of evaluations in any sense other than reducing vendor motivation to seek product reevaluations. RAMP provides no opportunity for a product release to obtain a different rating from the one held by the original evaluated version (other than a D rating, which terminates RAMP for the given product).

1.2 RAMP BENEFITS AND COSTS

The following are potential benefits of RAMP for system vendors:

- 1) Vendors participating in RAMP can offer their latest products in response to procurements that favor or require systems rated under the Trusted Product Evaluation Program.

2) RAMP makes it easier for vendors to discontinue support of previously rated products that have become outdated.

3) RAMP can reduce a vendor's long-term need for reevaluations while increasing the vendor's rated product offerings.

4) RAMP can clarify a vendor's representation of a new product version as a trusted system.

5) RAMP creates a learning process for vendors that can yield valuable knowledge for trusted system development and marketing.

- RAMP participation creates four general types of cost for vendors:

- 1) Initial expenses of personnel training and program planning.

2) Net vendor costs of establishing RAMP and undergoing a product evaluation with RAMP.

3) Net costs of complying with RAMP procedural requirements when developing product revisions.

4) Costs of producing the Rating Maintenance Report and conducting related tasks to obtain rating approval.

Costs in the second and third categories largely involve the establishment of a rigorous configuration

management system for product changes. These net costs are highly dependent upon company policies and procedures in the absence of RAMP, and must be judged on a case - by - case basis from the description of the program in the following sections.

1.3 RAMP COVERAGE

RAMP is currently available only for the maintenance of C1, C2, and B1 ratings. At present, a product cannot hold a B2, B3, or A1 rating without an evaluation of the precise version in question. RAMP is currently directed toward operating systems. Layered products are also eligible if their sponsors can meet the same requirements that apply to operating systems. RAMP does not cover subsystems. The Center can accommodate the evolution of subsystem products more appropriately through reevaluations. Networks and network components are not eligible for RAMP at this time, pending resolution of relevant issues for these products.

Vendor participation in RAMP is required for all products under evaluation for a C1, C2, or B1 rating. A vendor must establish an intent to participate in RAMP prior to the vendor assistance phase of an evaluation for the original product, and must then pursue the process continuously so that successive versions of the product are rated at the same level as the preceding version. (Previously evaluated products can remain on the EPL, without RAMP involvement.) The Center reserves the right to determine at any point in an application of RAMP that further rating maintenance is not viable under the program because of the nature of product changes. As described in Section 6, the Center provides advance notice of such determinations whenever possible.

1.4 RAMP APPROACH

Figure 1 shows the aspects of a typical product life cycle that create the need for RAMP. Figure 1 does not cover participation in RAMP (or the first two evaluation steps listed below). The uppermost time line depicts a vendor's development of a new product, and the second time line describes the Center evaluation of this release. The sequence of events for a product evaluation without RAMP is as follows.

1) The vendor submits an evaluation proposal package to the Center for the given product.

2) The Center assesses the company, the marketability of the product, and the feasibility of evaluating the product under the TCSEC.

3) The Center prepares a Preliminary Technical Report (PTR) describing the condition of the product, its development schedule and requirements, and its candidate rating level.

4) The vendor develops the product according to the schedule identified in the PTR. The Center provides assistance in meeting the intended rating level.

5) The vendor declares a code freeze (CF) on the given release of the product. The code freeze is the end of substantive product changes (as opposed to testing and fix activities).

6) The Center prepares an Initial Product Assessment Report (IPAR) for review by the Center's Technical Review Board (TRB). In contrast to the PTR, the IPAR is an intensive analysis yielding an estimation of whether or not the product is able to sustain an evaluation at the targeted level of trust.

7) The Center conducts an evaluation wherein product trust must be demonstrated and defended to the satisfaction of the TRB.

8) The TRB makes a rating recommendation.

9) Upon ratification by the Chief of the Product Evaluation Division, the rating is forwarded for publication on

the EPL.

10) The Center publishes a Final Evaluation Report (FER) at roughly the same time that the product appears on the EPL. The FER is a summary, intended to be publicly releasable, of evidence on product trust.

The central portion of Figure 1 describes the vendor's evolution of the hypothetical product over time. Long-range planning of the product's development typically yields a prioritized list of desirable system modifications for inclusion in releases following the original product. The revision process works progressively down this list, with the number of modifications in each revision determined by technical, financial, and marketing factors.

Figure 1 depicts a fast revision cycle in which the development of each successive product version begins before the code freeze for the previous release. A slower cycle might involve the development of each new version after the previous version is released. As already stated, without RAMP only the specific product version evaluated by the Center is a trusted system with a TCSEC rating and a listing on the EPL. This holds regardless of the nature of system changes, because evaluation and RAMP are the only acceptable mechanisms for verifying the performance and assurance of the security features of the product. All new releases without RAMP continue to be unrated until such time as the product is reevaluated, i.e., some version undergoes evaluation by the Center and thereby receives a rating.

A goal of RAMP is life-cycle product assurance, meaning production of evidence that the security features functionality and assurance established in an evaluation are maintained across every system revision. Figure 1 shows the need for several key aspects of RAMP. First, life-cycle product assurance clearly requires vendor involvement and willingness to integrate security concerns into the system development process. Security analysis and the assembly of product evidence cannot be treated as intermittent or external functions. Second, rating maintenance activities obviously must be established very early in the product life cycle, before the original product is completed and work has begun on subsequent releases. Third, the manner in which the Center achieves rapid turnaround of rating maintenance requests is reliance upon ongoing procedural controls. These controls include program planning requirements, training of vendor personnel to perform security analysis, and Center reviews of the rating maintenance process.

The key elements of RAMP are security analysis and configuration management. Security analysis is the intellectual process of designing, analyzing, and testing product changes to assure that they do not compromise the security characteristics of the product. Configuration management*defined as a process of systematically managing changes across an entire system*is the overall procedural framework for implementing and documenting the directives and conclusions from security analysis. Configuration management provides the fundamental linkage of product evidence between the evaluated product and each new release under RAMP. A rigorous configuration management system should be established prior to the evaluation phase and applied to every product change throughout the duration of rating maintenance. This requirement holds for any product in RAMP. (Product evaluations without RAMP require configuration management only for rating levels B2 and above.)

Figure 2 describes the general structure of RAMP. This diagram provides a brief overview of the topics discussed in the following sections, and is superseded in Section 8 by a more detailed graphic depiction of RAMP activities. The boxes in Figure 2 are task groupings arranged on a time scale from left to right. The arrows denote flows of information and program directives.

Ramp Approach - Continued

Box 1 depicts the Center evaluation of the original product.

(This document commonly refers to the evaluated product that starts a RAMP process as the "original" product, even though it may in fact be a reevaluated version of some earlier product.) The vendor has already established an intent to participate in RAMP in the evaluation proposal package for the given product.

While the product is still under development, one or more vendor representatives undertake a Center training program in computer security and RAMP requirements (box 2 in Figure 2). A person completing this program can serve as a Center-recognized Vendor Security Analyst (VSA) in representing the vendor's product to the Center. The VSA role is a key source of product assurance in RAMP. (See Section 2 for a discussion of Center recognition of VSAs.)

The vendor specifies every aspect of the vendor's RAMP process in a Rating Maintenance Plan (RM-Plan). The RM-Plan establishes all procedures for maintaining product trust, including control of changes to the RM-Plan itself. The RM-Plan can be tailored to the vendor's preexisting business practices, but it must be followed precisely throughout the product life under RAMP. Preparation of the RM-Plan (box 3 in Figure 2) begins as soon as the vendor has gained a sufficient understanding of rating maintenance. The RM-Plan must be approved by the Center before the Center's issuance of an IPAR for the original product. The RM-Plan must be in force before development begins on the version that will supersede the evaluated version.

The activities depicted by boxes 4 through 6 in Figure 2 recur for each product revision. (Box 3 recurs whenever the RM-Plan is changed.) Rating maintenance actions*box 4*are configuration management tasks conducted entirely by the vendor. These actions include: examining proposed system changes for security relevance; analyzing the direct and indirect impacts of changes; giving instructions for the implementation of changes; monitoring the implementation process; testing the revised system; modifying the tests as necessary; and updating all documentation to reflect each change. A VSA conducts, supervises, or monitors each of these tasks.

The vendor's RAMP process is subject to two types of reviews by the Center (box 5). The Center conducts an interim review after the start of rating maintenance for each new product revision. These interim reviews may or may not involve site visits after RAMP has operated for one or more releases. The Center also conducts aperiodic on-site reviews. Both types of program review have the purpose of assuring that security features functionality and assurance are being maintained by adherence to all the procedures established in the RM-Plan. Both reviews serve the mutual interest of the vendor and the Center in identifying problems quickly so that the vendor can initiate corrective actions in a timely manner.

The Center assigns a Technical Point of Contact (TPOC) to advise and coordinate the use of RAMP for the given product. A Center Business Point of Contact (BPOC) handles administrative and programmatic aspects of the process. A Responsible Corporate Officer represents the vendor in administrative matters. The Responsible Corporate Officer is a person empowered to commit the company financially to the program and support the technical role of the VSA. Sections 2 and 5 describe these persons and their interactions in greater detail.

Box 6 in Figure 2 covers the submission and review of evidence for a completed revision. The vendor submits to the Center a Rating Maintenance Report (RMR) containing a summary of product evidence. Following an initial review for completeness and general adequacy, the RMR is forwarded to the Center's Technical Review Board (TRB). The VSA or VSAs associated with the product then defend the RMR and other evidence before the TRB. The remaining steps in a successful application of RAMP include a recommendation by the TRB, a rating approval by the Chief of the Product Evaluation Division, and a product listing on the EPL. The process is designed so that, if all the vendor's preparations are complete and accurate, only a short time should elapse between the end of the initial RMR review and the listing of the product on the EPL.

1.5 LINKAGES BETWEEN RAMP AND EVALUATION

The establishment of RAMP is tied to the evaluation process at four points. First, the vendor must include an intent to participate in RAMP as part of the evaluation proposal package that starts the evaluation process. Second, the Preliminary Technical Report (PTR) prepared by the Center establishes the ability of the vendor to conduct RAMP activities. The PTR examines the vendor's understanding of configuration management;

explains the implications of the TCSEC for the given product; and advises the vendor about the contents of the RM-Plan.

Third, the Center does not complete an Initial Product Assessment Report (IPAR) for a product covered by RAMP until an RM-Plan is approved. A section of the IPAR confirms the adequacy of the RM-Plan and the vendor's ability to comply with all provisions of the plan.

Fourth, the vendor of a product in RAMP prepares a RAMP audit to support the evaluation by the Center. The RAMP audit is discussed in Section 3. The Center conducts three TRB sessions. During the first session, at the end of the Design Analysis Phase, the IPAR is reviewed. The second and third TRB sessions occur during the Evaluation Phase. The second session covers product testing. The third is a final, comprehensive session. The initial RAMP audit must be evaluated and approved at the second TRB session. (The program assessment performed at this time constitutes the first RAMP interim review. See Section 5 for further discussion of interim reviews.) The RAMP audit is treated at that time as an integral part of the functional testing requirement (test suite) for the product. This is one of several respects in which RAMP participation increases the evaluation effort for both the vendor and the Center.

1.6 APPLICABILITY OF RAMP

The following table summarizes RAMP eligibility in terms of product type.

RAMP ELIGIBILITY BY TYPE OF PRODUCT

Eligible Products Ineligible Products

Operating Systems Subsystems

Layered products, if vendor Networks

- demonstrates knowledge of base
- product consistent with RAMP
- requirements*

*See Sections 3 and 7

A vendor must satisfy the RAMP requirements summarized in the Appendix. These requirements are linked to the timing of the product evaluation and are determined as the evaluation proceeds. A vendor failing to satisfy these requirements loses the opportunity to participate in RAMP until such time as the product in question is reevaluated.

1.7 DOCUMENT CONTENTS

The organization of material in the remainder of this document generally follows the numbering of boxes in Figure 2. The one exception is that description of the RM-Plan is deferred until all subjects covered by the plan have been discussed.

Section 2 addresses the training of vendor personnel as VSAs.

(Description of the VSA role continues in Sections 4 through 6.) Rating maintenance actions are the subject of Sections 3 and 4. Section 3 discusses the conceptual aspects of configuration management in RAMP, and Section 4 addresses procedural issues. Section 5 deals with program reviews and the structure of RAMP in terms of communication and accountability. Section 6 covers the presentation of evidence for a product revision and the steps leading to a rating determination. Section 7 describes the contents of the RM-Plan. Section 8 provides an overview of the RAMP process. The Appendix summarizes the vendor's and the

Center's requirements for RAMP.

2. VENDOR PERSONNEL

2.1 INTRODUCTION

RAMP defines two roles for vendor personnel: the Vendor Security Analyst (VSA) and the responsible corporate officer. At least one Center-recognized VSA, and a responsible corporate officer, must be maintained while rating maintenance actions are underway. The use of multiple persons in the VSA role is a practical necessity for some products. Vendors choosing to use multiple VSAs must designate one of these persons as the lead VSA and must maintain clearly defined areas of VSA responsibility.

VSAs are responsible for the execution of all technical tasks in RAMP including the presentation and defense of product evidence. Other persons can participate in RAMP tasks at the discretion of the vendor, but only VSAs can represent the RAMP process technically to the Center. The ability of RAMP to yield timely rating approvals for an evolving product depends heavily upon the credibility and expertise of the responsible VSA or VSAs. These VSA characteristics are acquired and demonstrated through the VSA training program and the operation of the RAMP process.

The responsible corporate officer provides overall management of the vendor's RAMP effort and serves as the point of corporate responsibility for RAMP to the Center. The responsible corporate officer designates persons as VSAs; oversees the nonresident phase of VSA training; establishes VSA responsibilities; communicates with the Center on administrative and programmatic issues; and provides corporate assurance that the RM-Plan and submissions of evidence accurately describe the vendor's RAMP process. Any misrepresentation of the process places the product rating at risk, reflecting upon both the responsible corporate officer and the VSAs involved. The responsible corporate officer must occupy a sufficiently prominent position in the corporate structure to bear this responsibility and to commit the necessary company resources to RAMP.

This subsection addresses the VSA training program, the establishment of VSA credibility, and the program requirements pertaining to multiple VSAs. The next four subsections describe VSA duties and responsibilities in more specific terms. Section 7 then discusses the establishment of the VSA role in the RM-Plan, and Section 8 covers Center and vendor responses to failures in this role.

2.2 SELECTION AND RECOGNITION OF VSAS

While the vendor will probably employ numerous technical personnel in support of product development and maintenance, the Center only recognizes as RAMP representatives those individuals who have completed the VSA training program and are named by the vendor's RM-Plan as VSAs. Only these Center-recognized VSAs and the responsible corporate officer can interact with the Center on behalf of the product.

The remainder of this subsection discusses criteria that should be considered by the responsible corporate officer when selecting personnel who will support the technical development or maintenance of a product (to include both VSAs and other technical personnel). Additional criteria, applying only to VSAs, are discussed in the next subsection, Admission To Training Program.

Recommended Criteria for Vendor Selection of Technical Personnel:

- 1) Knowledge of the product on which the person will work.

2) Knowledge of computer science and computer security.

3) Corporate position and expected longevity of association with the vendor and the given product.

4) Time availability for involvement in RAMP tasks.

5) Contribution to multiple-VSA strategy (if used).

Regarding the first two criteria, the emphasis of RAMP upon VSA capability provides strong motivation for vendors to staff this function with the most knowledgeable persons available. The third and fourth criteria are practical considerations of obvious significance and are particularly relevant to personnel serving as VSAs. Problems can result from relying upon persons at either end of the corporate hierarchy. Low-ranking persons may lack sufficient authority and influence to fill the VSA role effectively, whereas high-ranking persons may not have enough time for day-to-day participation in rating maintenance tasks. Ideally, a VSA should be devoted full-time to the security analysis and rating maintenance of the given product. Continuity of involvement is critical because smooth operation of RAMP depends upon the progressive establishment of VSA credibility with the Center.

The last criterion covers such possibilities as using backup VSAs, establishing mentoring relationships among VSAs, and selecting VSAs to fill specialized roles within the RAMP process.

2.3 ADMISSION TO TRAINING PROGRAM

Vendors should submit VSAs for training by the Center as soon as possible when planning to use RAMP. The Center views timely involvement in the training program as an indicator of vendor commitment to the RAMP process. The responsible corporate officer sends a written request for vendor training with a statement of qualification for each potential trainee. (Ideally, the responsible corporate officer also undergoes training.) The Center strongly urges vendors to submit candidates with the following qualifications:

General:

- 1) Participants in the Center training program should have sufficient background in computer science to analyze all aspects of system design including functional hardware logic and software code.

2) A trainee should be knowledgeable about the specific product for which he or she will serve as VSA. (A person can possibly serve as a Center-recognized VSA for multiple products, but at any given time the Center only deals with a VSA as a representative of a specific product.)

- Specific:

- 3) A trainee should have obtained a degree from a four- or five-year college program with a major in computer science, engineering , or other technical field that emphasizes computer science;
- OR, a trainee should have at least five years of professional experience working with computers in a design or analytical capacity.

- 4) A trainee should have at least one year of experience with the specific product for which she or he will serve as VSA.

2.4 CENTER TRAINING PROGRAM

The VSA training program addresses the following subject areas:

general principles of computer security; requirements and Center interpretations of the TCSEC; security issues in the system development process; and all aspects of RAMP. The calendar time required for a trainee to complete the course depends upon scheduling factors but should not exceed two months given an adequate time commitment. It is not possible in such a period to train persons as security evaluators capable of conducting an unsupervised product evaluation; but the course does impart sufficient capability to establish product trust when working from an evaluated system. The Center assumes no responsibility for

the selection of a VSA and, in particular, the consequences of an inappropriate selection of a VSA by a vendor. The Center training program is provided as an additional measure to help the vendor prepare and select appropriate personnel to serve as VSAs who will, in turn, increase the likelihood that the vendor will be able to maintain a given product's level of trust. The Center's principal concern is, and will remain, the maintenance of a product's rating, not the certification of a VSA. For this reason, the Center will assist in the training of, but will not formally certify, VSAs.

The training program currently consists of a three-week program of study conducted at facilities in the Baltimore/Washington, D.C., area. Beginning in 1990 the Center plans to implement a dual-phase program, which will include a nonresident (correspondence) phase and a resident phase (with the former always occurring first).

The remaining description of the Center training program describes the planned implementation of the dual-phase program. The current Center residence program incorporates all resident testing and assessment of VSAs.

The nonresident portion of the training program does not require a classroom setting and can take place at any location convenient to the vendor and the trainees. The flexibility of this phase with regard to location and scheduling allows the training program to be driven by vendor demand. However, the course requires a significant block of time and cannot simply be scheduled around an employee's normal workload. The responsible corporate officer must take responsibility for assuring that each trainee has adequate time for the program. In addition, the nonresident phase will not begin until the vendor has provided for VSA utilization of the Center's Dockmaster information system (described in Section 5).

The materials utilized in the nonresident phase of the training program include:

- 1) documents prepared by the Center for use in the course;

2) additional required and recommended readings; and

3) tests covering the course documents and required readings.

A vendor representative serves as proctor for the nonresident coursework. The proctor monitors the progress of each trainee and administers tests and written assignments. The responsible corporate officer designates the proctor, monitors the conduct of the course, and provides assurance to the Center that all aspects of the nonresident phase are executed conscientiously. A Center training point of contact is available to answer technical and administrative questions about the program.

Trainee performance in the nonresident phase is evaluated on the basis of tests, written assignments, and open-book group projects. The tests cover the course documents and required readings. These materials are forwarded to the vendor with guidelines for interpreting results, such as the scores that constitute satisfactory performance on each test. The vendor has responsibility for determining that a trainee has mastered the nonresident coursework sufficiently to enter the resident phase.

Trainees then undertake approximately one week of resident classwork at the Center facility in Maryland. The resident phase focuses upon a worked example of a Trusted Computing Base (TCB), designed to provide practical experience in security analysis. The related course materials include a sample RM-Plan and a sample Rating Maintenance Report. Trainees are evaluated in this phase by written assignments and an oral examination that takes the form of a product defense before a mock Technical Review Board (TRB).

The Center will notify the vendor of each trainee's performance in the resident phase and offer a recommendation as to whether or not the given person should be used as a VSA. The assessment provided will note the VSA's performance using both an absolute scale of reference (i.e., raw scores on tests) as well as a relative scale (i.e., the VSA's performance as compared to other VSA candidates who have attended

the training). These scores will be supplemented by a subjective assessment of the candidate VSA's performance. In the case of a weak candidate, the Center may indicate that using the given person as a VSA will jeopardize the vendor's RAMP process. The vendor makes the final decision in this regard. The only absolute requirements for Center recognition of a vendor representative as a VSA are: 1) completion of both phases of the training program, and 2) assignment of VSA responsibilities to the given person in the vendor's RM-Plan (discussed later).

The VSA training program addresses general principles of computer security and system development, and is not product-specific. In the event a VSA becomes a vendor representative for some other product, the training program need not be repeated.

2.5 FURTHER ESTABLISHMENT OF VSA CREDIBILITY

Smooth operation of the RAMP process requires a higher level of VSA credibility and expertise than can be established in classroom training alone. In each RAMP cycle, vendors must demonstrate to the satisfaction of the Technical Review Board (TRB) that security analysis has been conducted thoroughly and correctly according to the RM-Plan. This demonstration involves written evidence, VSA defense of the evidence, and VSA credibility based upon past performance in RAMP. The higher the level of demonstrated VSA capability, the less need for time-consuming examination and information requests, and the less risk of a negative rating determination.

A practicing VSA builds credibility through program reviews and presentations to the TRB. The former includes interim reviews during every RAMP cycle and aperiodic reviews on a less frequent basis. The Center places major emphasis on a VSA's first interim review. (See Section 5.) In the first presentation of evidence by a VSA, the TRB examines the VSA's understanding of the product as well as the management of changes under RAMP. The topics of questioning include: 1) the product and its security features and assurances; 2) the procedures followed in applying RAMP on a day-to-day basis; and, 3) the substance and rationale of decisions regarding product changes. Section 6 provides further discussion of the evidence submission process.

Vendors are made aware of any VSA credibility problems through TRB recommendations and other communications between the Center and the responsible corporate officer. A VSA who knowingly misrepresents any aspect of rating maintenance for a product will no longer be recognized by the Center as a RAMP participant for any product. Furthermore, when a vendor (responsible corporate officer) allows a misrepresentation to occur, the RAMP process is terminated with no rating approval for the product version that was misrepresented. The Center then reviews the previous cycles of rating maintenance to determine whether the rating should be rolled back across earlier releases. (See Section 8.) Lesser infractions consisting of inadvertent VSA errors and oversights can yield serious delays and uncertainties in rating approval. Overall, there is strong vendor self-interest in using VSAs who can establish and maintain a high level of credibility with the TRB.

2.6 MULTIPLE VSAS

Vendors can often benefit from using more than one Center-recognized VSA for a given product. The multiple-VSA approach supports program continuity in the event that a VSA becomes unavailable for duty or proves to be deficient in some respect. For some products, multiple VSAs may be essential in order to assign separate responsibility for different production sites, different parts of a product, or different aspects of rating maintenance. A vendor may also employ some VSAs without assigning them any official responsibilities in the RM-Plan. The vendor can use such persons in backup, apprenticeship, or other supporting roles while limiting the number of product representatives.

The Center encourages the use of multiple VSAs subject to the conditions stated in the following paragraphs. These conditions, and all further references to VSAs in the present document, pertain just to Center-

recognized VSAs who have completed the training program and are assigned RAMP responsibilities in the RM-Plan. Other VSAs can be deployed freely by the vendor in the same fashion as regular employees but cannot interact directly with the Center.

The Center must know at all times which VSAs are representing the product and precisely what their individual responsibilities are. At least one Center-recognized VSA must be representing the product at any time that rating maintenance actions are underway. The RM-Plan should describe the primary area of responsibility for each VSA in such a fashion that all RAMP activities are covered and there is no ambiguity as to who is answerable for any given aspect. Divisions of responsibility by production site or corporate department should be noted along with divisions of responsibility by RAMP task. VSA responsibilities cannot be altered without formally changing the RM-Plan to describe the new assignments. As described in Section 7, the vendor must obtain approval for any change in the RM-Plan from the Center Technical Point of Contact. The RM-Plan approval constitutes the Center's recognition of any VSAs named for the first time as responsible representatives of the RAMP process. Vendors are urged to make any changes in VSA responsibilities at the beginning of a rating maintenance cycle, i.e., within a month after the previous rating approval.

Every recognized VSA must sign the Rating Maintenance Report and be prepared to defend product evidence for the given cycle before the TRB. Ultimate responsibility for the RMR rests with the responsible corporate officer. Other VSA duties can be conducted by one rather than all VSAs. For example, only one VSA need be a member of the Configuration Control Board. (See Section 4.) Vendors should nevertheless be aware that the use of multiple VSAs does not lessen the degree to which each is accountable. An application of RAMP is only as strong as its weakest link in terms of VSA credibility.

A vendor using multiple VSAs must designate one person as the lead VSA. Most technical communication between the vendor and the Center involves the lead VSA. The Center may require at its discretion that all technical communication be routed through the lead VSA during some or all of the RAMP cycle. It is logical but not necessary for the lead VSA to have supervisory powers over other VSAs. The RM-Plan should describe any supervisory or coordinating relationships among VSAs. These issues are discussed further in Sections 5 and 7.

3. SECURITY ANALYSIS AND CONFIGURATION MANAGEMENT

3.1 SECURITY ANALYSIS

Security analysis is the intellectual core of rating maintenance.

Configuration management is the supporting framework that assures an accurate translation of security analysis findings into implemented product changes and evidence of product trust. Security analysis can be viewed as an aspect of configuration management (or configuration control). The present document maintains a distinction between these concepts because for many persons configuration management connotes a set of mechanical procedures rather than a thought process.

Security analysis is closely associated with design tasks that would be needed to effect product changes whether or not a product was a trusted system. RAMP not only introduces security as a design consideration but also requires security to be the dominant consideration. RAMP does not permit any compromise of security for the sake of other product design criteria such as performance, cost, and marketability. There can be negotiation among possible ways of implementing security for a given change, but no tradeoff of security features and assurances against other objectives. The dominance of security is always an integral part of security analysis as referenced here.

Security analysis draws upon the vendor's full understanding of the function and interrelationships of security features in the product. This understanding is applied in diverse ways that do not permit description of

security analysis as a standardized set of procedures. The following paragraphs indicate briefly the activities, issues, and outcomes of security analysis for a typical product.

Security analysis starts by establishing the precise nature of all effects of a product change upon the Trusted Computing Base (TCB). (There may or may not be a separate, preliminary screening for the existence of TCB effects; see Section 4.) As defined by the TCSEC, the TCB is the totality of protection mechanisms *including hardware, firmware, and software*that together enforce a security policy. The present document uses a somewhat different definition covering all system elements that support protection mechanisms. The TCB addressed by security analysis and configuration management in RAMP includes system code, tests, associated software tools, test plan documentation, test results, the trusted facility manual, the security features user's guide, and design documentation. (For hardware, the program relies upon functional testing rather than configuration management.)

A product change affects the TCB if it: alters code or documentation within the identified TCB boundary; augments the contents of the TCB; or indirectly affects the function of TCB elements. The determination of indirect effects on the TCB is a critical aspect of security analysis. The analysis considers any possibility of effects due to interrelationships among the product's security features. The analysis also acknowledges and assesses cumulative effects involving multiple product changes. (For example, two otherwise acceptable changes may conflict in terms of security because one change assumes conditions that no longer hold, given the other change.) Security analysis can potentially identify many different TCB effects resulting from a proposed change to a single configuration item.

Security analysis enters a design mode once all TCB effects are identified and understood. The requirement is then to verify that a proposed change can be implemented without compromising the security features and assurances of the product, or else to remove the change from consideration. The security analysis assures that any change is consistent with approved architectures and does not circumvent defined security policy. The process of addressing these criteria is usually integrated or coordinated with the pursuit of other design objectives, but security is always the paramount concern. Depending upon the nature of the change and the vendor's business practices, this phase of security analysis may or may not extend into code-level product development tasks. (See Section 4.) Security analysis includes checking the adequacy of existing system tests as affected by each proposed change. The analysis modifies existing tests or creates new tests as necessary to maintain the effectiveness of the test suite.

The outputs of security analysis include: instructions for implementing changes; recommendations for rejecting other changes; new tests and test documentation; and descriptions of all identified TCB effects, related analytical findings, and design decisions. The RAMP process subjects the conclusions of security analysis to two stages of review and retains all of the above outputs in the configuration management system. Security analysis is also addressed by the RAMP audit function described at the end of this section.

3.2 OVERVIEW OF CONFIGURATION MANAGEMENT

Configuration management is a discipline applying technical and administrative direction to: 1) identify and document the functional and physical characteristics of each configuration item for a product; 2) manage all changes to these characteristics; and 3) record and report the status of change processing and implementation. Configuration management involves process monitoring, information capture, quality control, bookkeeping, and an organizational framework to support these activities. The "configuration" being managed is the TCB plus all tools and documentation related to the configuration management process.

The overall objectives of configuration management in RAMP are to assure that the findings of security analysis are implemented correctly, and to generate product evidence linking with the evidence established in the evaluation. Configuration management records the "footprint" of the security analysis and controls and documents all subsequent rating maintenance tasks. This involves the central direction of system changes to:

- 1) maintain the integrity of system information and the standards affecting its accuracy, timeliness, and reliability;

2) ensure that documentation and tests remain congruous with the rest of the system;

3) ensure adequate testing of changes prior to incorporation;

4) maintain the integrity of all system interfaces; and

5) support the objective of security analysis.

Many vendors of products rated C1 through B1 already use some form of configuration management before participating in RAMP. The existing procedures can often meet RAMP requirements with few modifications, although fundamental changes are sometimes needed. The RAMP requirements are sufficiently flexible to accommodate substantial variations in vendor business practices. Typically, the greatest deficiencies of existing practices relative to RAMP standards involve security analysis rather than the record-keeping aspects of configuration management.

The four major aspects of configuration management are configuration identification, configuration control, configuration status accounting, and configuration auditing. The present section summarizes these activities in conceptual terms. Section 4 then addresses procedural issues in rating maintenance using a representative business model to discuss specific functions needed for RAMP.

3.3 CONFIGURATION IDENTIFICATION

Configuration management entails decomposing the TCB into identifiable, understandable, manageable, trackable units known as configuration items (CIs). The decomposition process is called configuration identification. To support RAMP, this process must occur before the initial RM-Plan is completed so that the plan can include the CIs for the original product. The configuration of the evaluated system is thereby established as a baseline for assessing future changes.

CIs can vary widely in size, type, and complexity. Although there are no hard-and-fast rules for system decomposition, the granularity of CIs can have great practical importance. Selecting CIs that are too small can impede the audit process by yielding an unmanageable volume of identifying data. Overly large CIs can hinder configuration management by obscuring product changes and interrelationships among changes. A potentially favorable strategy is to designate relatively large CIs for system elements that are not expected to change over the life of the product, and small CIs for elements likely to change. System identification ideally should begin early in the design stage for a product when CIs are most readily established on a logical basis. For example, each CI might be a module of code designed to meet one requirement. Regardless of the strategy for establishing CIs, the granularity of control is defined to be the module level. The process must allow for the possibility that system changes will convert non-CI components into CIs.

Vendors in RAMP decompose at least the following system components into CIs and assign a unique identifier to each.

- 1) Software and firmware components of the baseline (evaluated) TCB.

2) Design and user documentation.

3) Software tests including functional and system integrity tests and associated documentation.

4) Development tools including any configuration management tools.

5) Any tools used for generating current configuration items.

6) Any audit trail reduction tools used in the configuration management context.

7) Any other components of the TCB as broadly defined.

Throughout the application of RAMP to product revisions, each change in a configuration item is uniquely identified. The changes of significance for RAMP are any alterations to the TCB since the product evaluation. The date of a CI change is identifiable along with any changes to the related documentation, tests, or development tools. Each change in software source code is separately identifiable, although changes need not be separately stored.

3.4 CONFIGURATION CONTROL

Configuration control is a means of assuring that system changes are approved before being implemented, that only the proposed and approved changes are implemented, and that the implementation is complete and correct. This involves strict procedures for proposing, monitoring, and approving system changes and their implementation. Configuration control entails central direction of the change process by corporate functions that coordinate analytical tasks, approve system changes, review the implementation of changes, and supervise other tasks such as documentation. These procedural requirements of RAMP are the primary subject of Section 4.

Configuration control involves not only the approval of changes and their implementation but also the updating of all related material to reflect each change. There should be guidelines for creating and maintaining functional test software and documentation throughout the life of the system. The change process should include a phase for test creation and maintenance, with associated updating of documentation. Relevant tests should be performed and evaluated whenever system changes are implemented and/or tests are updated. The vendor must rerun the entire test suite before submitting RAMP evidence to the Center.

A vendor's production arrangements may hinder or complicate the process of controlling system change. Hardware and software may be developed by separate groups within the vendor organization, perhaps located at different sites. Code development and integration may occur in different cities, with testing conducted at both locations. Also, a vendor may propose RAMP for a system (layered product) that incorporates another vendor's products. Vendors faced with these difficulties acknowledge the resulting limitations on security analysis and configuration control in their RM-Plans, and establish alternative procedures of equal effectiveness for upholding product trust.

A vendor applying RAMP to a layered product demonstrates configuration management cognizance over all parts of the product, including parts manufactured by other vendors. This means that the vendor understands the base product and its changes since evaluation and conducts security analysis of these changes, to the same extent as required by RAMP for an in-house product. (See Section 7.) Some form of collaboration among vendors is thus virtually essential for RAMP coverage of a layered product.

A vendor's configuration management system includes policies and procedures for correcting any security bugs identified in the product. Responses to flaws, bugs, and breakdowns of RAMP assurance are discussed in Section 8.

3.5 CONFIGURATION ACCOUNTING

Configuration accounting documents the status of configuration control activities and in general provides the information needed to manage a configuration effectively. It allows managers to trace system changes and establish the history of any developmental problems and associated fixes. Configuration accounting also tracks the status of current changes as they move through the configuration control process. Configuration accounting establishes the granularity of recorded information and thus shapes the accuracy and usefulness

of the audit function.

Configuration accounting should yield answers to questions such as the following. What source code changes were made on a given date? Was a given change security relevant? Why or why not? What were all the changes in a given CI between releases N and N+1? By whom were they made, and why? What other TCB modifications were required by the changes to this CI? Were modifications required in the test set or documentation to accommodate any of these changes? What were all the changes made to support a given change request?

The accounting function is able to locate all possible versions of a configuration item and all of the incremental changes involved, thereby deriving the status of that CI at any point in time. The associated records include commentary about the reason for each change and its implications for the TCB. Configuration accounting provides convenient access to such records for use as evidence in the rating maintenance process. In general, the effectiveness of configuration accounting depends upon the quality of system identification and control efforts.

3.6 CONFIGURATION AUDIT

Configuration audit is the quality assurance component of configuration management. It involves periodic checks by the vendor to determine the consistency and completeness of accounting information and to verify that all configuration management policies are being followed. (The following subsection identifies when configuration audits occur.) A vendor's configuration management program must be able to sustain a complete configuration audit by a Center aperiodic review team.

A configuration auditor should be able to trace a system change from start to finish. The auditor should check that only approved changes have been implemented and that all tests and documentation have been updated concurrently with each implementation to reflect the current status of the system. A configuration audit in RAMP must be conducted by a VSA.

3.7 RAMP AUDIT

The RAMP audit process addresses both security analysis and configuration management procedures. The two components of a RAMP audit are a configuration audit as described above and a detailed review of security analysis records for a selection of product changes. The security analysis component involves drawing a random sample of past Service Improvement Requests (SIRs, as described in Section 4) and assessing all the security analysis activities undertaken to meet each request. The objective is to confirm in each case both the adequacy of the analysis and the completeness of the stored records.

As already indicated, the RAMP audit is part of the functional testing requirement for a product in RAMP, and the results of the initial audit are reviewed by the Center evaluation team during the product evaluation. This review ensures that the vendor's RAMP process follows the procedures outlined in the vendor's RM-Plan. A vendor's audit program is established clearly in the RM-Plan. The plan describes the frequency of audits and the procedures for assessing configuration management and security analysis practices. The results of all subsequent RAMP audits are reviewed by the Center's TPOC. (See Section 7.)

4. PROCEDURAL ASPECTS OF RAMP

4.1 INTRODUCTION

RAMP uses strong procedural controls to assure that rating maintenance actions by vendors do not compromise the product trust established in Center evaluations. On the other hand, overly rigid requirements would be costly and inefficient for some vendors and thus could limit program involvement.

The Center reconciles these concerns in RAMP by allowing considerable vendor discretion in the design of configuration management procedures, but requiring meticulous adherence to plans once developed.

Rating maintenance procedures are described here using a generic business model. The Center developed this generic model by interviewing numerous vendors and identifying common elements in their business practices. Discussing RAMP in this context serves to:

- 1) provide a specific illustration of acceptable procedures;

2) establish common names for certain activities and functions;

3) clarify the elements essential for RAMP; and

4) provide a baseline against which alternative approaches can be evaluated.

- The discussion does not imply that each vendor's product revision process must conform to the generic model. What RAMP requires is that the chosen procedures be no less effective than the generic model in maintaining continuity of assurance and providing evidence of product trust.
- The following text assigns standard names to various procedural elements and functions (summarized in the glossary). This does not imply that a vendor must create new entities corresponding to the names, if equivalents already exist. The Center requests vendors to utilize the standard names in their RM-Plans and other formal communications as an assistance to the Center in dealing with diverse products and business plans. Vendors should feel no need to alter their internal language, since the VSAs interacting with the Center can readily translate the few terms at issue.

4.2 GENERIC MODEL

Figure 3 depicts the generic model of rating maintenance actions in RAMP. The diagram emphasizes configuration control, although configuration identification, accounting, and auditing tasks are no less important. All of the boxes and arrows represent configuration management procedures identified in the Center survey of business practices prior to RAMP. The diagram has been converted to a RAMP description by highlighting two control and approval functions (using dotted lines and decision nodes), and by including commentary on the VSA role.

The generic model can be summarized as follows, ignoring momentarily the elements specific to RAMP. Proposed system changes are drawn from a prioritized list of desirable system modifications as described in Section 1. Requests for changes reach the system design group through some mechanism that we call a Service Improvement Request (SIR). Each proposed change receives a preliminary screening for effects on the TCB. A change that clearly does not affect the TCB directly or indirectly enters a design analysis phase addressing product characteristics other than security. (Code-level design of the change may occur in varying proportions at this stage and at the implementation stage.) The design analysis ends with some form of review. A change that affects the TCB, or may affect the TCB, undergoes security analysis in conjunction with design analysis.

The analysis and review tasks yield an Engineering Change Order (ECO), which directs the implementation of an approved change. The ECO covers modifications of tests and documentation as well as the system software. Code is written for the change and entered into a working copy of the system for testing. Existing and modified tests are applied as appropriate. The change is then subjected to a final review. Any change that fails to gain acceptance in this final review is removed from the system. If rejection has been caused by an implementation problem, the change may recycle back to the ECO stage. Other changes rejected in the design review or final review are sent back to the beginning of the configuration management process or discarded altogether. Implemented changes that gain final approval are incorporated into the product, and all documentation is updated accordingly.

4.3 ORIGIN OF PRODUCT CHANGES

This and the following subsections describe the requirements of RAMP in the context of the generic model. For convenience, the text often references the VSA role as if played by a single person even though multiple VSAs are likely.

The system revision process in RAMP starts with an evaluated product (although the first changes may occur while the evaluation is still in progress, or even before the code freeze for the evaluated product). The full configuration management process should be operative as soon as a system is identified, so that all changes relative to the original product can be managed uniformly.

The vendor selects changes from the prioritized list of desirable system modifications established during the product development. Financial and marketing factors affect the choice of changes, since these factors influence the revision cycle and the feasible number of modifications per cycle. RAMP requires some equivalent of the Service Improvement Request (SIR) to provide a formal record of all proposed changes entering the analysis and implementation process.

4.4 CONFIGURATION CONTROL BOARD

All analytical and design tasks in RAMP should be conducted under the direction of a corporate entity called the Configuration Control Board (CCB). The upper dashed line in Figure 3 encompasses the activities in the generic model that the CCB should supervise. These include: 1) screening of proposed changes for impact on the TCB; 2) security analysis of changes that affect the TCB; 3) associated design analysis and review tasks; 4) approval and disapproval of changes on the basis of product trust; and 5) issuance of instructions for change implementation (ECOs).

Central direction by a CCB does not necessarily mean that a vendor must discard other ways of administering configuration management in order to participate in RAMP. The vendor can base the CCB on an existing design supervision group, perhaps joined by other persons when it sits as the CCB, or the vendor can establish the CCB as a forum of representatives from multiple groups involved in product development.

The membership of the CCB must include at all times a Center-recognized VSA for the given product. Furthermore, the responsible corporate officer must have the power to veto any CCB approval of a product change. This veto power can derive from inclusion of the responsible corporate officer as a CCB member with special voting rights; from some other explicit provision of the CCB rules, or from the authority vested in the responsible corporate officer by his or her corporate position. The responsible corporate officer is not required to participate in CCB deliberations or decision-making on a routine basis. This arrangement gives the VSA two ways of influencing product changes (over and above contributing to analysis and design tasks). The VSA can influence changes by participating as a full member in the CCB function, and also by notifying the responsible corporate officer that a given change approved by the CCB is unacceptable in terms of RAMP assurance. In essence, the VSA represents security concerns to the CCB, and the responsible corporate officer enforces the dominance of these concerns. The Center holds the vendor accountable for change control through the responsible corporate officer.

RAMP requirements for the CCB are summarized as follows:

- 1) The CCB operates at all times in accordance with the vendor's RM-Plan.

2) No product change can be implemented without approval by the CCB.

3) The CCB has authority over all analysis, design, and review tasks from the receipt of SIRs through the issuance of ECOs.

4) The CCB has access to all information used in, and generated by, the activities under its purview.

5) The VSA (or a VSA) is a CCB member with all of the rights, powers, and information access possessed by other members.

6) The responsible corporate officer has the power to veto any CCB approval of a product change. Changes vetoed by the responsible corporate officer are disposed in the same fashion as changes disapproved by the CCB.

- There are no restrictions upon CCB procedures for reaching decisions, but the Center encourages using the CCB as a forum for deliberations that can be recorded as RAMP evidence. The CCB ideally functions as a central source of "security wisdom" as well as program oversight.

4.5 COMPLIANCE WITH THE TCSEC AND CRITERIA INTERPRETATIONS

The preliminary screening of proposed changes for effects on the TCB is an optional feature of the generic model, although some arrangement of this nature is probably necessary for efficiency. A nonoptional feature of the model is that the changes that bypass preliminary screening are routed through the subsequent phases of the change control process (i.e., EACH CHANGE MODEL MUST CONTAIN SOME TYPE OF CONFIGURATION REVIEW). Retention of these changes in the process allows the reviews by the CCB and Configuration Review Board (CRB) to verify the absence of any direct or indirect effects on the TCB.

Section 3 has already described the scope and responsibilities of security analysis. This task must determine that a proposed change upholds the security features and assurances of the product in compliance with the TCSEC and the Criteria interpretations. The outcome for each change is evidence that links with product evidence from the evaluation. Security analysis may require intensive problem-solving efforts in establishing TCB effects, designing changes, and developing appropriate tests. The fundamental requirement of RAMP is dominance of security over other design considerations.

The Center periodically issues Criteria interpretations to clarify the application of the TCSEC. An important issue in RAMP is the time that is allowed to elapse between the issuance of an interpretation and the compliance of a product release (and all subsequent releases) with this interpretation. The reasonable maximum time is related to the length of a product's revision cycle (e.g., three months, six months), but it cannot be linked rigidly to the revision cycle without creating excessive difficulties for fast-cycling products and excessive slack for slow-cycling products. The Center recommendation is that each product release in RAMP should comply with all Criteria interpretations for which at least one of the following conditions is true:

- 1) The interpretation was issued prior to the EPL listing for the previous release of the given product.

2) The interpretation was issued at least one calendar year prior to the submission of a Rating Maintenance Report (RMR) for the release in question.

3) The interpretation is accompanied by an effective date, which precedes the RMR submission date for the release in question.

This policy would give vendors a grace period of one revision cycle within which to comply with an interpretation, unless the revision cycle is longer than one year or unless the interpretation has an effective date that overrides the grace period. The Center cites an effective date if rapid compliance with an interpretation is considered especially critical. Each vendor proposes a policy for complying with Criteria interpretations when submitting an RM-Plan for Center approval. (See Section 7.) The approved policy becomes a plan element that must be followed rigorously throughout the RAMP process.

The need to comply with interpretations issued after the product evaluation can mandate design analysis and even product changes that have nothing to do with service improvements desired by the vendor. It is unlikely but possible that an interpretation will terminate rating maintenance for a product and necessitate a reevaluation. Because the interpretations issued during one revision cycle for a product typically do not apply

until the next cycle, the Center can usually indicate in advance whether or not a given interpretation will affect the continued use of RAMP. The VSA has responsibility, however, for keeping abreast of interpretations and assessing their impacts on the product. Criteria interpretations do not apply retroactively, so that product ratings established through RAMP are not withdrawn because of subsequent interpretations.

4.6 ENGINEERING CHANGE ORDERS

An approved system change is implemented through an ECO or a set of ECOs. An ECO tells the maintenance establishment what must be done to the code, the documentation, and other elements of the system to implement the change. The generic model shown in Figure 3 assumes that an ECO contains instructions in relatively high-level language, but code-level directives are also possible. Vendors can determine the format and content of ECOs subject to the following general requirements. In the generic model:

- 1) The ECO provides an orderly mechanism to propagate change across the system and assure synchronization, connectivity, and continuity of alterations.

2) The preparation of ECOs is under CCB control.

3) No system change of any kind can occur without direction by an ECO.

4) Each ECO retains the identities of the initiating SIR and any other SIRs or ECOs occasioned by the initiating SIR.

5) ECOs are retained as evidence for rating maintenance and should have a form suitable for record-keeping purposes.

RAMP assigns considerable importance to the ECO as part of the trail of product evidence. The vendor should establish the granularity of ECOs so that they provide convenient reporting units throughout rating maintenance. As discussed in Section 6, the RMR describes system changes at the ECO level.

4.7 IMPLEMENTATION, TESTING, AND FINAL REVIEW

The lower portion of Figure 3 describes the general process of implementing and testing a system change. The tests must verify that the implemented change preserves the function of security features and the assurance of correct feature operation. Testing and test development should be conducted independently from the implementation of changes as a check on the latter process. (Separation of functions as practiced by accountants can provide a useful safeguard in other areas of rating maintenance as well, subject to RAMP requirements for overall coordination and control.) The reference to testing in Figure 3 covers both functional security tests and performance tests, but only security tests contribute to RAMP evidence.

The results of implementing and testing each change are assembled for a final review before the change is incorporated into the product. An entity called the Configuration Review Board (CRB) carries out this review. The CRB membership should include a Center-recognized VSA (not necessarily the same VSA belonging to the CCB). The VSA should have all of the information access and influence over CRB decisions possessed by any other CRB member. The CRB can have the same overall membership as the CCB or can be an independent quality assurance group.

The final review by the CRB provides closure on each ECO by verifying that every aspect of the approved change was implemented correctly and that no other alterations were made. There should also be a reassessment of test results and system assurances to confirm that system trust has been upheld. The CRB then decides whether or not to accept a given change as part of the product. Rejected changes are removed from the system and disposed in the manner discussed above. The process ends for an accepted change with final incorporation and documentation tasks.

4.8 COLLECTION OF RAMP EVIDENCE

General suggestions of configuration accounting and auditing have been indicated in the previous section. The configuration management system should include numerous checks to assure that all relevant information is recorded and that documentation is updated fully to reflect each product change. As the custodian of RAMP evidence, the VSA must remain in close touch with all documentation tasks and should be able to influence the execution of these tasks.

A vendor with a functioning configuration management system prior to RAMP may choose to record some RAMP evidence externally in order to avoid overloading the system. For each product change, RAMP evidence will include the following commentary: the SIR from which the change originated; the procedures and arguments used in establishing TCB effects; the issues and conclusions of the security analysis; the ECOs generated for the change; and the completion status of ECOs. The vendor must be able to perform line-by-line code comparisons with pointers back to the ECOs causing specific modifications. The commentary on tests should include descriptions of new and modified tests, with stated reasons for the alterations and pointers to the test results.

4.9 VSA ROLE

The required duties of a VSA are suggested by the items on the right-hand side of Figure 3. The VSA is the focus of security wisdom in RAMP. The VSA (or VSAs) tracks the entire rating maintenance process and understands product changes in sufficient depth to verify the adequacy of security analysis and configuration control procedures. The VSA represents the Center concerns to the CCB and CRB, and assures that these functions are operating effectively to maintain product trust.

The VSA is custodian of all RAMP evidence, meaning that the VSA monitors the accumulation of evidence and has sufficient resources to assure its accuracy, completeness, and accessibility. The VSA has direct responsibility for proposing and managing revisions to the RM-Plan. The VSA performs or supervises the RAMP audit function and the preparation of all materials for submission to the Center. Lastly, the VSA is the vendor contact for all technical communication with the Center.

Section 2 has addressed the subjects of VSA training, VSA recognition by the Center, establishment of VSA credibility, and multiple-VSA approaches. At least one Center-recognized VSA must be representing the product at any time that rating maintenance actions are underway. A vendor using multiple VSAs must designate a lead VSA and must maintain an accurate description of VSA responsibilities in the RM-Plan at all times. Communications between VSAs and the Center are discussed in the next section.

PROGRAM REVIEWS, COORDINATION, AND ADMINISTRATION

5. PROGRAM REVIEWS, COORDINATION, AND ADMINISTRATION

5.1 PROGRAM REVIEWS

Two types of program review occur during the RAMP cycle between submissions of product evidence. An interim review takes place following each vendor RAMP audit. Aperiodic reviews occur irregularly throughout an application of RAMP on an average of less than one review per cycle. An aperiodic review is always conducted by a Center review team at the vendor's site (or multiple sites if applicable). Interim reviews may or may not occur on-site. As noted in Section 1, the first interim review for a product in RAMP occurs following the vendor's RAMP audit performed in preparation for the product testing TRB session.

Both types of review have the general purpose of establishing VSA credibility and confirming process assurance in RAMP. The reviews serve the common interest of vendors and the Center in identifying

problems as early as possible so that the vendor can make corrections with minimum impact upon rating maintenance and product evolution.

Review teams examine the evidence accumulation process and scrutinize records such as SIRs, ECOs, test results, and reports on CCB and CRB proceedings. VSAs are questioned about RAMP procedures and may be required to trace the course of events for specific product changes. The vendor must have the ability to perform a line-by-line code comparison for any two points in time and to sustain a RAMP audit by a Center review team. Program reviews are also an occasion for assessing the adequacy of the vendor's RM-Plan, and may lead to RM-Plan modifications.

5.2 INTERIM REVIEWS

Interim reviews and aperiodic reviews differ somewhat in emphasis.

An interim review has a procedural focus, addressing the credibility of the configuration management process and its adherence to the RM-Plan. An aperiodic review covers much of the same ground but includes an in-depth examination of the vendor's ability to conduct security analysis.

The subjects of investigation include the procedures for generating SIRs and ECOs, the adherence to established security analysis and design analysis policies, the exercise of central control by the CCB, the effectiveness of the CCB and CRB review functions, the adequacy of test development and documentation procedures, and all aspects of the configuration accounting system. The interim review team verifies that all product changes are controlled uniformly, that security concerns have precedence over other development objectives, and that sufficient evidence is accumulating to support process assurance.

Interim reviews focus strongly upon the credibility of each VSA as a representative of the vendor's RAMP process. The first interim review for a VSA is a critical milestone in the establishment of VSA credibility. All VSAs demonstrate to the interim review team a broad knowledge of security-related policies, issues, and practices for the given product, and an ability to apply the TCSEC in concrete situations. The interim review verifies that the VSA (or group of VSAs) is tracking every aspect of the configuration management process and is participating sufficiently in each task to understand the major issues and decisions for every product change.

5.3 APERIODIC REVIEWS

An aperiodic review constitutes an assurance checkpoint in a vendor's RAMP program. Vendors receive no information about the timing of aperiodic reviews other than sufficient advance notice to allow an orderly review process (i.e., a few days). Vendors designate one point of contact per RAMP activity site to be notified in case of an aperiodic review.

An aperiodic review examines in detail the soundness of a vendor's decisions and the adequacy of product evidence to support the assertions of product trust contained in Rating Maintenance Reports and other VSA statements. An objective in some cases is to determine the reasons for problems already identified. The review team may select several recent product changes and trace the entire sequence of events leading to the implementation of each, with particular emphasis upon the thoroughness and accuracy of security analysis. This process examines the vendor's analytical competence and sensitivity to security issues as well as the effectiveness of configuration control and configuration accounting procedures.

The aperiodic review team looks for trust violations consisting of: insufficient understanding and application of computer security principles; failure to give top priority to security concerns; errors in security analysis and product testing; failure to follow the RM-Plan; and failure to report all relevant actions and circumstances as product evidence. If an aperiodic review identifies a security flaw in the product or a breakdown of process assurance, the Center reserves the option of withdrawing EPL status from the affected version of the

product and all subsequent versions. (See Section 8.)

5.4 PROGRAM COMMUNICATION AND COORDINATION

There is a designated Center Technical Point of Contact (TPOC) for each product in RAMP. The TPOC tracks the rating maintenance process from the planning phase onward and coordinates all technical interchange between the vendor and the Center. The TPOC is the vendor's entry into the Center for the resolution of computer security issues and concerns. The TPOC assesses VSA performance and other aspects of the program, particularly during the first RAMP cycle but does not directly supervise vendor activities.

There is also a Center Business Point of Contact (BPOC). The BPOC carries out administrative functions in RAMP such as: making programmatic decisions; planning the use of Center resources; providing a conduit for official documentation; and notifying the vendor of rating determinations.

Section 2 has discussed the general duties and responsibilities of the vendor's responsible corporate officer. The responsible corporate officer administers the RAMP program and is the vendor's point of accountability to the Center. The responsible corporate officer is a person empowered to make financial commitments on behalf of the program; maintain a favorable corporate context for its execution; and limit product changes as necessary for protection of RAMP assurance. The responsible corporate officer assumes full responsibility for the contents of each Rating Maintenance Report.

Figure 4 shows the lines of communication in RAMP between the TPOC, BPOC, responsible corporate officer and VSA(s). All interactions on administrative matters are routed between the BPOC and the responsible corporate officer. All technical communication passes through the TPOC, with two exceptions. These exceptions are on-site reviews and VSA interactions with the TRB when defending an RMR.

The Center requires the vendor to designate a lead VSA in multiple-VSA situations primarily to facilitate orderly communications. The lead VSA should conduct most technical interactions with the Center (possibly excluding on-site reviews and RMR presentations), and should receive copies of any written documents passing between the vendor and the Center. In some cases the TPOC may require that all technical communication be routed through the lead VSA.

The lead VSA will provide quarterly, informal status reports to the TPOC (via the Dockmaster system mentioned below). These reports are intended to keep the Center apprised of the vendor's rating maintenance activities.

The Center discourages excessive vendor reliance upon the TPOC as a program advisor. The TPOC apprises the vendor of important developments in the computer security field and is available for consultation on major issues. This does not relieve the vendor of responsibility for keeping abreast of developments through other means (such as the Dockmaster system mentioned below) and exercising security wisdom independently of the Center. Vendors are discouraged from attempting to pass program responsibility back to the Center by submitting routine decisions to the TPOC. The success of RAMP depends upon a vendor's own security analysis capability and willingness to be held accountable for actions affecting the product.

All vendors participating in RAMP must provide for VSA access to the Center's Dockmaster information system by the time VSA training begins. Dockmaster is a Honeywell MULTICS system used by the evaluation community for electronic mail, electronic meetings, forums, queries, and other functions. A RAMP vendor must be prepared to communicate with the TPOC via Dockmaster and to use the system as a general information source.

6. PRESENTATION AND REVIEW OF EVIDENCE

6.1 INTRODUCTION

A vendor in RAMP preserves security features and assurances of a product through security analysis and configuration management. The documentation of this process in a body of evidence linking to the evaluation yields RAMP assurance of product trust. Because the process is subject to strong procedural controls*the RM-Plan, on-site reviews, and VSA training*the Center can extend the product rating to each new release without performing a full reevaluation or a lengthy assessment of all product evidence. Rating approvals are based upon a moderately detailed summary of evidence and a face-to-face presentation of this material by the vendor to the Center. The Center reserves the right to request additional evidence as necessary.

The vendor prepares the summary of evidence in the form of a Rating Maintenance Report (RMR). The vendor can submit the RMR to the Center at any time after all changes have ended for the product version in question. Delays can be minimized by preparing much of the RMR while the product is being revised, i.e., by summarizing the evidence as it accumulates.

The following are the major steps leading to a rating approval and EPL listing for a revised product. These steps are discussed at greater length following the description of the RMR.

- 1) Vendor submits RMR and other materials to TPOC.

2) TPOC circulates RMR to Center evaluators for review.

3) TPOC forwards RMR and supporting materials to Technical Review Board (TRB).

4) TRB reviews RMR and issues comments to vendor (through TPOC).

5) VSA or VSAs defend RMR before TRB.

6) TRB makes recommendations on rating maintenance to Chief of Center Product Evaluation Division.

7) Chief of Product Evaluation Division approves or disapproves product rating.

8) Revised approved product receives EPL listing.

Steps 1 and 2 may iterate until the TPOC is satisfied with the level of detail of the RMR. Only a short time should elapse between steps 3 and 8 if the vendor has properly satisfied the RAMP requirements (summarized in Appendix A) and has a well-executed RAMP process (defined by the vendor's RM-Plan) with adequate VSA credibility. Thus, efficient preparation of the RMR and supporting materials can lead to an EPL listing at roughly the same time that the new product version is released.

6.2 RATING MAINTENANCE REPORT

The RMR summarizes product evidence at a level of detail intermediate between the information that would be required to conduct an evaluation and the information typically contained in a Final Evaluation Report. The RMR asserts that product trust has been upheld and includes sufficient commentary to allow an understanding of individual product changes. Figure 5 presents a suggested outline for an RMR. The Center does not impose a standard format on these documents but requires coverage of all the listed items.

The major components are a cover letter, a description of the system configuration, a section on Criteria interpretations, a discussion of each product change at the ECO level, and a future change analysis. The cover letter identifies the product and describes its history of rating maintenance. The cover letter must be signed by the responsible corporate officer and all recognized VSAs. It affirms that the responsible corporate officer: 1) has reviewed the RMR; 2) assumes full responsibility for the RMR contents; and 3) acknowledges responsibility for the sincere and conscientious execution of all rating maintenance actions.

The first report section gives a complete overview of the system configuration and its changes since the product evaluation. Much of this material can often be carried forward from earlier documents. General

discussion of RAMP policies and procedures can appear either here or in a separate section. The second section discusses the significance of all Criteria interpretations applying to the given product release. (The vendor's policy with regard to interpretations is discussed in Section 4 and Section 7.)

The items in the third section of the suggested RMR outline are repeated for each product change. RAMP defines an individual change in this context as an Engineering Change Order (ECO) that has been implemented. Figure 5 assumes a classification of ECOs according to product module and configuration item. (The classification may vary if ECOs overlap configuration items.) Discussions can be pooled and cross-referenced in cases where several ECOs have been used to achieve a common purpose, but the RMR should list each ECO individually.

The last lines in the third section of the RMR outline suggest the topics requiring mention in the evidence summary for an ECO affecting the TCB. Very little discussion is necessary for other ECOs*one or two sentences as compared with at least a paragraph for each ECO having TCB impact. (These two categories of ECOs may be segregated in the RMR.) The appropriate depth of discussion for an ECO affecting the TCB depends upon the sensitivity of relevant security mechanisms and assurances and upon the complexity of the security analysis.

The fourth section of the RMR as outlined in Figure 5 is a discussion of probable changes in the product beyond the current version. The Center uses this future change analysis to assess the future applicability of RAMP to the product (as discussed below). The Center requests vendors to describe the major product changes anticipated for the next two release cycles or the next 18 months, whichever period is greater. A failure to provide this information increases the vendor's risk of discovering suddenly that RAMP is no longer feasible and the product is no longer eligible to participate in RAMP. In order to be placed on the EPL, the product must then be reevaluated.

Figure 5. Suggested Rating Maintenance Report Outline

COVER LETTER

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 numbers of the Final Evaluation Report (FER), any revised versions of the FER, and the RMR for the most recently maintained release. Assertion that the new release maintains the product rating. Responsible corporate officer warranty of document contents.

Signatures of the responsible corporate officer and all Center-recognized VSAs.

SECTION 1: SYSTEM CONFIGURATION

Listing of the hardware/software configuration for the

evaluated product

(original TCB by module).

Rationale for system decomposition into configuration items. Updated listing of the configuration, noting changes: List of hardware contained in the secure configuration. List of TCB software modules, noting any modules that have been changed and the file length (lines of code) of each module. Rationale for determining effects on the TCB of product changes, with pointers to specific changes itemized in Section 3.

SECTION 2: CRITERIA INTERPRETATIONS

List of all Criteria interpretations applying to this product release.

Comments on the significance of each interpretation for the product as revised.

Pointers to discussions in Section 3 of product changes

made because of specific Criteria interpretations.

SECTION 3: PRODUCT CHANGES AND EVIDENCE OF SYSTEM TRUST

Name of module or document changed.

ID number(s) of configuration item(s) changed.

Engineering Change Order (ECO) number.

Description of change:

Functional description.

Description of user-visible effects.

Classification of change according to effects on the TCB (yes or no).

Evidence of product trust (if change affects the TCB):

Explanation of relevant Criteria and interpretations.

Relevant TCB mechanisms and assurances. Design issues, alternatives, and solutions. Tests and test modifications if any. Summary of test results. Pointers to system and test documentation. Pointers to specific code-level changes.

SECTION 4: FUTURE CHANGE ANALYSIS

Expected product changes in next revision cycle.

Expected product changes in second revision cycle.

Later evolution of product.]

6.3 OTHER SUBMISSION MATERIALS

The materials submitted concurrently by the vendor to achieve rating maintenance include several items in addition to the RMR. The overall package is as follows.

- · RATING MAINTENANCE REPORT (RMR)
- ·
- · RM-PLAN(S) WITH CHANGE BARS
- ·
- · FINAL EVALUATION REPORT (FER) WITH CHANGE BARS
- ·
- · FINAL EVALUATION REPORT WITH INTEGRATED CHANGES
- ·

- · PROPOSED PRODUCT DESCRIPTION FOR EPL
- ·

As discussed elsewhere, RM-Plans often change during a rating maintenance cycle because of procedural refinements and changes in VSA responsibilities. The Center is always aware of changes and always possesses a current version of the RM-Plan, because changes cannot be effected without Center approval. The vendor's submission package at the end of a rating maintenance cycle includes an additional copy of the RM-Plan with change bars showing every alteration relative to the plan that was in force at the end of the previous cycle (i.e., when the previous RMR was submitted). This document must show the date on which each RM-Plan change was approved by the Center. Its purpose is to assist review of the vendor's program by the TRB. (A general principle of the rating approval process is that the vendor should not assume a TRB "memory.") The vendor may also choose to include a separate document consisting of a proposed RM-Plan for the next revision cycle. Submitting proposed RM-Plan changes at this time facilitates Center approval and serves the Center objective of confining most plan alterations to the beginning of a cycle.

The submission package includes a copy of the Final Evaluation Report (FER) for the initial evaluated product, with change bars converting the FER to a description of the current release. The vendor also provides a copy of the FER with these changes integrated into the text. The latter document is called a RAMP FER to distinguish it from the direct output of a Center evaluation.

The remaining document submitted with the RMR is a brief description of the revised product for use by the Center in publishing an EPL listing if the new version maintains the product rating. This and the RAMP FER are the only program documents intended for public release.

6.4 REVIEW AND DEFENSE OF RMR

The TPOC receives the RMR and associated materials from the vendor and forwards these documents to Center evaluators for review. A primary objective is to prepare the VSAs for examination by the TRB. The reviewers point out areas of the RMR that are deficient or likely to receive special TRB attention. The VSAs respond by revising the RMR and/or assembling supplementary evidence for the product defense. The TPOC then submits the RMR and related materials to the TRB. After examining the RMR, the TRB may transmit written comments to the VSAs (through the TPOC), which establish a partial agenda for the VSAs' oral presentation and defense.

All Center-recognized VSAs should be prepared to meet face-to-face with the TRB and discuss the aspects of RAMP for which they have been responsible. The TRB will expect the VSAs to present a thorough technical overview of changes to the product TCB and the security analysis of those changes, thus demonstrating continuity of function and retention of assurance. When new VSAs are involved, the face-to-face examination is strongly concerned with establishing VSA credibility. The TRB questions each new VSA in depth about the nature of the product as well as about rating maintenance procedures and individual changes.

The TRB will focus upon changes which raise complex security questions, or which are not fully understandable from the RMR description, or which provide a good context for detailed examination of procedures. The responsible VSA first describes the change and answers questions on the basis of memory and supplementary information brought to the session. If these responses are inadequate, the TRB requests additional evidence.

The TRB subsequently issues a recommendation to the Chief of the Product Evaluation Division stating that product trust has or has not been maintained by the current product version at the level established by evaluation. If the product does not sustain its rating, the vendor may or may not be given the option of reconstructing the RAMP process in some fashion and returning for another TRB review. The given RAMP cycle ends with a rating determination by the Chief of the Product Evaluation Division and, if the determination is favorable, a listing of the new release in the EPL.

6.5 FUTURE APPLICABILITY OF RAMP

RAMP applicability is limited. If product revisions fundamentally alter security mechanisms and assurances, the result from a security standpoint is a new product requiring evaluation to qualify as a trusted system. At the start of RAMP, the Center verifies the potential applicability of the program to the initial revisions of the product before approving the vendor's RM-Plan. The RMR review at the end of each cycle is the occasion for later forecasts of RAMP applicability. These forecasts of future RAMP applicability are an integral part of the trusted products partnership established between the Center and the vendor.

The Center uses the information in the vendor's future change analysis to estimate (if possible) the point at which RAMP will no longer be viable and the product cannot be placed on the EPL without a reevaluation. This point can result from cumulative changes as well as from especially significant changes in any one revision cycle. The Center criteria for RAMP applicability cannot be summarized conveniently here. The extremes are that most changes in system architecture are not coverable by RAMP, whereas product changes that do not affect the identified TCB directly or indirectly can always be covered.

The Center has designed RAMP with the intention of giving vendors at least one cycle's advance notice of the need for a product reevaluation. (Hence the request for information in the future change analysis describing at least two cycles.) The degree of certainty expressible by a RAMP forecast is governed, in large measure, by the level of detail, completeness, and the schedule provided in the future change analysis by the vendor. Notifying the vendor that RAMP can proceed for another revision cycle does not commit the Center to approve rating maintenance for that cycle when completed, and a forecast of RAMP applicability for a later cycle may be changed as that cycle approaches. The Center reserves the right to deny a rating and/or discontinue a RAMP process at any time.

When forecasting RAMP applicability for a product, the Center addresses any expected difficulty in complying with recent or prospective Criteria interpretations that do not apply to the current product version.

As discussed in Section 4, Criteria interpretations can affect the use of RAMP irrespective of the nature of product changes.

7. RATING MAINTENANCE PLAN

7.1 INTRODUCTION

Strict adherence to a comprehensive RM-Plan is one of the most important program controls in RAMP. The RM-Plan is the vendor's document, tailored to the product in question and to the company's business practices and personnel. The plan and any proposed changes must be approved by the Center and must describe accurately throughout product maintenance what the vendor is doing to the product and what evidence is being recorded.

A vendor starting a new RAMP process should commence preparation of an RM-Plan during or immediately after VSA training. No rating maintenance actions on the product can occur until an approved RM-Plan is in place, which means that delays in program planning can slow the startup of product revisions. Vendors should develop a new RM-Plan by building upon rather than rejecting previous practices. The Center encourages this approach in order to minimize the chances of conflict and inefficiency in RAMP. Also, the vendor should not attempt to resolve every issue and establish an ideal plan before submitting a draft to the Center for review. A period of consultation between the vendor and the Center is usually necessary to arrive at a mutually acceptable RM-Plan. In plan development as in later phases of RAMP, the Center is eager to help vendors who approach the process constructively.

A vendor initiates the RM-Plan approval process by submitting a new or revised plan to the TPOC. The TPOC coordinates the Center review and issues an approval when the plan is judged to comply with RAMP

requirements. The TPOC will document approvals of new or revised RM-Plans and changes to existing plans via the Center's Dockmaster system.

A vendor may wish to change an existing RM-Plan in order to improve the rating maintenance process or alter VSA responsibilities. There are no fixed limitations on changing an RM-Plan, but the Center urges vendors to minimize the total number of changes and to confine change requests to the beginning of each rating maintenance cycle. A change request includes a copy of relevant sections of the RM-Plan with all proposed changes shown by change bars, plus a copy of the entire plan with the changes integrated into the text. The latter becomes the operative RM-Plan when approval is granted.

All RM-Plan changes must receive Center approval regardless of their nature. On receiving a change request, the TPOC determines the scope of the Center review based upon the magnitude and implications of the proposed change(s). The TPOC can grant immediate approval of a change that is very minor or unavoidable (such as a reassignment of program responsibilities due to loss of a VSA). In all cases, however, the old RM-Plan remains in force until the change is approved and documented on the Center's Dockmaster system.

RM-Plans are intended to be current but not release-specific.

This distinction becomes relevant when successive product releases overlap in terms of development, i.e., when work starts on version N+1 before the code freeze for version N. In such cases, a single RM-Plan describes the vendor's RAMP process for all work on the product. The RM-Plan may reference specific product versions when describing VSA responsibilities, thus creating a need to update the plan periodically; but this is similar to cases in which VSA assignments are based upon specific product changes or other transient factors. The single-plan format applies unless there is a branching of the product, i.e., a situation in which version N includes changes that are not contained in version N+1, as well as vice versa. If the Center allows RAMP coverage of both branches, the vendor must maintain a separate RM-Plan for each.

7.2 OVERVIEW OF RM-PLAN CONTENTS

The RM-Plan tells how the vendor will accomplish all the tasks and achieve all the results described previously in sections 3, 4, and 6. The RM-Plan cannot state exhaustively how security analysis will be conducted and cannot guarantee that errors will never occur. However, the plan describes the vendor's procedures and safeguards in sufficient detail to constitute an essential part of RAMP assurance.

While the format of individual RM-Plans may vary, a vendor's RM-Plan must address the following topics. Each of these topics is discussed in the subsections that follow.

- A. The product and its configuration.

B. Security analysis.

C. Configuration control.

D. Collection and verification of evidence (configuration accounting and RAMP auditing).

E. Compliance with Criteria interpretations.

F. Presentation and defense of security analysis and product evidence.

G. VSA responsibilities and program administration.

H. Vendor response to failures.

I. Numbering and retirement of product versions.

J. Management of the RM-Plan.

7.3 THE PRODUCT AND ITS CONFIGURATION

An RM-Plan must begin with a description of the rated product and all its components. This description should address all elements of the TCB in specific terms. It should also cover business aspects of the product such as control over the distribution of documentation.

The RM-Plan describes how configuration identification has been performed. The plan should discuss the vendor's approach and objectives in decomposing the system, and should describe system elements in sufficient detail to show compliance with the configuration identification requirements listed in Section 3.

There should be commentary on any special implications of the system identification for configuration control. The plan specifies the naming conventions used for configuration items (CIs) and for changes to CIs. Policies regarding the creation of new CIs for revised products should also be discussed.

A startup RM-Plan includes a development process timetable, indicating when submissions of evidence are anticipated, and a future change analysis discussing the expected evolution of the product. As in the RMR for a completed RAMP cycle, the future change analysis should cover at least the first two cycles or 18 months of RAMP, whichever is longer. The Center assesses the expected changes and expresses a judgment by way of the RM-Plan approval that the product rating can probably be maintained through the initial revisions.

7.4 SECURITY ANALYSIS

The RM-Plan states the vendor's policies and procedures for security analysis in as much detail as possible. It describes security analysis and related design activity on a task-by-task basis, from identifying TCB effects through developing new tests and reporting on the acceptability of changes. The plan should demonstrate clearly that the vendor understands and adheres to the concept of security dominance in product development. This part of the RM-Plan may or may not be integrated with discussion of the vendor's configuration control system, which covers the overall structure of change control and the participation of corporate groups in this process.

The RM-Plan must describe the steps taken by the vendor in assessing the effects of product changes on the TCB. This description covers methods of establishing indirect TCB effects as well as effects due to interrelationships among security features. The plan should reference any generic procedures used such as regression testing. There should be clearly stated arrangements for identifying any cumulative effects due to multiple product changes and/or collateral modifications entailed by changes. These arrangements are especially critical when security analysis and system design tasks are spread among several operating groups.

The RM-Plan then describes the principles and procedures followed by the vendor in establishing acceptable designs for product changes and determining when changes cannot be implemented for security reasons. If no single description of this process is adequate, the plan can reference various categories of product changes and show how the process operates for each. There should be explicit discussion of the relationships between security analysis and the pursuit of other design objectives.

A section of the RM-Plan must address the development and application of system tests as an element of security analysis. This discussion covers: the vendor's general testing policies; the determination of test adequacy as affected by product changes; the guidelines followed when modifying or creating tests; and the vendor's procedures for updating the test plan on the basis of security analysis findings.

The RM-Plan summarizes the vendor's criteria and methods for concluding that a change is or is not acceptable under the TCSEC and describes how these conclusions are documented and forwarded for

Configuration Control Board (CCB) review. The plan must demonstrate that the security analysis yields adequate RAMP evidence in the form of recorded analytical findings and support for all decisions affecting the product.

7.5 CONFIGURATION CONTROL

As established in Section 3, configuration management is the framework for reviewing, implementing, and documenting the conclusions of security analysis. The portion of the RM-Plan on configuration control presents the vendor's business plan for accomplishing these objectives.

A vendor developing a startup RM-Plan may find it convenient to work incrementally from existing practices. First, the vendor's existing configuration management system is modeled and evaluated against the conceptual requirements of RAMP discussed here in Section 3. The vendor revises the model by identifying needed elements and finding the most harmonious ways of including these elements within the present business context. The vendor then evaluates the revised model against the procedural requirements and VSA responsibilities outlined in Section 4. Functional equivalents of the SIR, ECO, CCB, and CRB are identified. If there is no full equivalent for one of these entities*e.g., no central authority that can be designated as the CCB*the vendor overcomes the deficiency by building upon present functions with as little disruption as possible. Similarly, the vendor seeks to identify persons who can serve effectively as VSAs in their present corporate positions (and who are qualified and available for VSA training). Only if such persons are unavailable does the vendor consider restructuring groups and reassigning personnel to achieve adequate VSA involvement.

The RM-Plan must present a unified discussion of configuration control centering upon the vendor's business model as revised. The discussion should trace the course of events for a product change from its entry into the RAMP process as a SIR through its final approval and incorporation.

The plan should explain the preliminary screening of changes for TCB effects, if conducted as a separate task, and describe the vendor's safeguards against incorrect categorization of changes. The plan shows how product changes that lack TCB effects are routed through the various design and implementation steps and change reviews. The RM-Plan then presents the detailed discussion of security analysis for changes affecting the TCB, if this discussion has not already been provided. The vendor indicates which operating groups conduct the security analysis and to what extent the VSA or VSAs participate in each aspect. (Coverage of the VSA role by the RM-Plan is discussed further below.)

The RM-Plan should describe in specific terms how the CCB will coordinate the security and design analyses and will review system changes. The discussion addresses the composition of the CCB, the lines of authority among its members, the nature of its deliberations, and the manner in which the CCB assures security dominance in the product development process. Other topics are the power of the CCB to influence security analysis, the quality control steps involved in CCB review, the ability of the CCB to request additional information, and the disposition of product changes that fail to receive CCB approval. The RM-Plan should describe VSA membership and participation in the CCB, and the ability of the responsible corporate officer to veto a CCB approval when requested by the VSA.

The RM-Plan should discuss the manner in which ECOs are generated and what they contain. The relevant data include: who prepares ECOs; the granularity of ECOs; the conditions under which multiple ECOs are used to effect a given change; the level of detail at which ECOs direct implementation tasks; the instructions in ECOs for testing implemented changes; any quality control procedures for ECOs; and the manner in which the CCB controls the production of ECOs. The RM-Plan should also indicate the role of ECOs in the vendor's record-keeping system.

The RM-Plan describes the vendor's procedures for assuring that all approved changes are implemented correctly and that only these changes are made. The plan should discuss the structure of the implementation

and testing groups, indicating the degree to which the testing function is conducted independently. The description of testing procedures should mention interactions with the design group (outside the ECO process) on the subjects of test adequacy, test development, and test results. The plan should also summarize briefly the management of the system code, e.g., the use of working copies to implement and test changes.

The RM-Plan must specify the nature and operation of the Configuration Review Board (CRB) as described above for the CCB. The plan then discusses the final review process in terms of: the information delivered to the CRB on each implemented change; the quality control procedures utilized by the CRB to assure that the implementation is correct; the means of verifying that no system modifications have occurred other than the approved change; and the CRB policies for granting final approval or disapproval. Any exceptions to the review process should be noted. The RM-Plan describes the removal of disapproved changes from the product and the policies for returning such changes to an earlier stage of assessment.

The RM-Plan must acknowledge any special limits upon configuration control. For example, if the vendor's product development activities take place at more than one site, the RM-Plan states what aspects of RAMP occur at each site and how central coordination is achieved.

RM-Plans for layered products must describe specifically how the vendor will deal with the involvement of more than one company in producing the product. There is no compromise in the required level of RAMP assurance to accommodate layered products. The vendor demonstrates full configuration management cognizance, meaning that the vendor has evidence on the base product and its evolution comparable to the evidence required by RAMP for an in-house product. The vendor's RM-Plan describes in detail how this evidence is obtained, covering the nature of security analysis and the existence of any cooperative arrangements among producers.

7.6 COLLECTION OF RAMP EVIDENCE

The RAMP process essentially yields three categories of product evidence: 1) the findings of security analysis, with support for all conclusions from that analysis; 2) the records from configuration control of the design phase, from SIR receipt through CCB review and ECO issuance; and 3) the configuration control records for the implementation phase, covering test results, test documentation, and verification of changes by the CRB. Ideally, there should be a unified configuration accounting system that embraces all of this information. Vendors entering RAMP may find, however, that the first category of evidence overloads existing configuration accounting systems because of the extensive commentary on security analysis findings and decisions. An acceptable solution is to establish supplementary information files with clear linkages to the configuration management data via pointers and cross-references.

The RM-Plan must include an overall description of the vendor's record-keeping system, covering basic facts such as where the master version of the code is stored and how it is protected from unauthorized modification or use. The discussion lists the major database elements and notes any associated divisions of activity. (For example, the recording of information for system changes might be distinguished from the management of system documentation, tests, tools, test documentation, etc.) The plan describes how the vendor can determine the status of proposed and approved changes and can locate any supporting information.

The RM-Plan then revisits the entire configuration control process and states the documentation requirements associated with each step (unless documentation has already been covered in the section on configuration control). There should be one or more reporting tasks associated with almost every element of a rating maintenance model such as shown earlier in Figure 3. In each case, the RM-Plan must describe: what information is recorded; where it is recorded; who is authorized to store and retrieve information; and what steps are taken to assure that information is accurate and comprehensive. The plan also discusses the uses of this information in the configuration control process for review and approval purposes.

The Center recognizes that there may be a time granularity below which the system code, documentation, tests, and test documentation cannot be maintained on a synchronous basis because of lags in the updating process. The RM-Plan should estimate the duration of configuration accounting lags and describe any necessary steps to avoid problems from this source.

The RM-Plan must address the RAMP audit function and the VSA role in this function. The plan must establish configuration audit procedures for verifying compliance with every configuration control and configuration accounting requirement, and for checking the adequacy of all associated evidence. The plan should describe the security analysis portion of the RAMP audit in terms of: the procedures for sampling SIRs; the number of SIRs investigated; and the standards for assessing the adequacy of security analysis and related documentation. The RM-Plan should also state the vendor's intended schedule of RAMP audits. The Center does not impose a uniform requirement in this regard because of the widely varying circumstances encountered, with the exception that at least one RAMP audit must occur per RAMP cycle.

7.7 COMPLIANCE WITH CRITERIA INTERPRETATIONS

The RM-Plan must explain in detail the vendor's policy for complying with Criteria interpretations as they occur. The Center's recommended guidelines for such a policy have been discussed in Section 4. The objective is to provide the maximum compliance with interpretations consistent with a vendor's unique ways of doing business. Center approval of the RM-Plan is contingent upon attaining this objective. The policy statement in the RM-Plan should refer to the product revision cycle (i.e., the maximum number of cycles that can elapse before compliance occurs) and should also include calendar time as a factor if the revision schedule is variable.

7.8 PRESENTATION OF EVIDENCE

Section 6 has described the contents of the Rating Maintenance Report (RMR) and other documents submitted by the vendor to the Center at the end of each RAMP cycle. The RM-Plan should discuss briefly how these documents are prepared and how they will be used to defend the product, the security analysis, and the configuration management process before the TRB.

The new material in any given RMR consists primarily of the evidence summaries for product changes. (See Figure 5 in Section 6.) The RM-Plan should describe the contents of these summaries for product changes that do and do not affect the TCB. The summarization process should be discussed with reference to the extent of VSA involvement, the configuration accounting files used, and the vendor's ability to prepare evidence summaries while other product changes are still under way. The RM-Plan should estimate the time delay between the end of product changes and the submission of an RMR to the Center for review.

Regarding the defense of evidence, the RM-Plan should indicate which VSA or VSAs will represent the product at the next evidence submission and what provisions will exist for supplying evidence not contained in the RMR. Rough estimates should be given for the number of hours or days needed to comply with various types of information requests by the TRB.

7.9 VSA AND RESPONSIBLE CORPORATE OFFICER RESPONSIBILITIES

The RM-Plan must establish the VSA and responsible corporate officer roles in very specific terms. The required topics include: the qualifications and corporate position of the responsible corporate officer and the VSA or VSAs; the ability of the responsible corporate officer to support RAMP and the VSA function; the division of technical responsibilities among multiple VSAs, if used; and the extent of VSA involvement in every individual RAMP activity. The plan normally presents the task-by-task description of VSA duties as an integral part of the material on configuration control and collection of evidence.

The RM-Plan names the person or persons occupying the VSA role and summarizes briefly the qualifications

and experience of each. Any person representing the product as a VSA must have completed the Center training program. (As noted earlier, the approval of an RM-Plan confers Center recognition upon the VSAs referenced in the plan as product representatives.) The description of each VSA's corporate position should cover both line management and matrix management responsibilities. Any intended use of contractors or part-time employees as VSAs should be noted and explained.

There should be a general statement of the vendor's strategy for assuring that the VSA or VSAs can: track all aspects of the revision process; confirm the findings of security analysis; influence product changes; assure the accuracy and completeness of evidence; and represent the product effectively to the Center. If multiple VSAs are utilized, the RM-Plan explains the reasons for this approach and describe the primary areas of VSA responsibility in such a fashion that the Center can associate one and only one VSA with each element of the RAMP process.

The task-by-task description of VSA duties must cover for each activity in RAMP: 1) the share of work conducted personally by a VSA;

2) the extent of VSA supervisory authority over the given task; 3) the ability of a VSA to influence how work is done and what outputs are produced; 4) the arrangements whereby a VSA can evaluate the adequacy of procedures and accuracy of data; and 5) the terms of VSA access to all information used in and generated by the task.

The RM-Plan should emphasize VSA involvement in the CCB function, the CRB function, the configuration audit, and the presentation and defense of evidence. The plan should name the VSA who serves as a CCB member and show how this function allows the VSA to control product changes through direct input to CCB decisions and through the veto power of the responsible corporate officer. VSA involvement with the CRB is discussed similarly. The plan describes VSA responsibilities for producing the RMR and representing the product to the TRB. It names the VSA or VSAs who serve as configuration auditor(s) or audit supervisors. The RM-Plan must confirm that VSAs have access to Dockmaster and are responsible for tracking Criteria interpretation activity.

The RM-Plan must describe how the responsible corporate officer will support the RAMP process and serve as the point of vendor accountability to the Center. This description covers: the power of the responsible corporate officer to make decisions and corporate commitments on behalf of RAMP; the extent of responsible corporate officer supervisory authority over the VSA(s) and over the operating groups involved in RAMP tasks; the influence of the responsible corporate officer over product changes; the role of the responsible corporate officer as the vendor's contact with the BPOC; and the ability of the responsible corporate officer to influence the corporate response to failures in the product or the RAMP process. As described in Section 6, the responsible corporate officer must be in a position to assume full responsibility for the content of RMR submissions.

The RM-Plan must name the lead VSA, if there are multiple VSAs, and describe all lines of authority among the responsible corporate officer, the lead VSA, and other VSAs. There should be an overview of RAMP program administration showing how RAMP fits into the corporate management structure. The RM-Plan should include a corporate organization chart and a personnel directory listing the department and job title of all persons who might contact the Center on the subject of RAMP. The organization chart should be abbreviated horizontally by showing only the portion of the corporate hierarchy that contains the responsible corporate officer, the VSAs, all CCB and CRB members, and all operating groups with major involvement in RAMP.

7.10 EXCEPTION HANDLING

The RM-Plan must describe any and all exception handling procedures that may be used in the development of the product. Exception handling refers here to actions outside the normal cycle of releases, not exceptions

to RAMP practices. Under no circumstances are interruptions in configuration management allowable.

Specifically, the RM-Plan must address the vendor's response to product and process failures. The failures that can occur for a product in RAMP fall into three categories, as follows.

Bug: Improper execution of an acceptable design.

Flaw: Incorporation of an inadequate design decision.

Breakdown of process: Deficiency in the security analysis and/or configuration management procedures that confer RAMP assurance.

These failures can have widely varying impacts upon the responsible vendor, the user community, and the product rating. Bugs and flaws are of greatest immediate concern to users. However, breakdowns of process tend to have the greatest long-term impacts on product ratings and continued RAMP applicability. Errors can usually be located and corrected if the process remains pure, but RAMP assurance may not be recoverable if the process fails. Section 8 discusses the response of the Center to these types of failures.

The primary focus of exception handling is the management of system bugs. The Center recognizes that at the C1 through B1 rating levels (which are features-oriented rather than assurance-oriented), a product may contain implementation errors that are undetected by evaluation and that may be exploitable under some circumstances. It is not acceptable to pass responsibility for vulnerability management on to system users. Vendors should therefore plan ahead for the possibility of bugs and should develop procedures for correcting bugs with minimum delay and risk to users.

The following are suggested steps to deal with a potentially exploitable bug once identified. The vendor:

- 1) immediately deploys a repair and recovery team to analyze and solve the problem

2) contains information regarding the bug in order to minimize risk to operational systems

3) provides immediate notice to the TPOC so that the Center can take any necessary steps to assure the protection of system users

4) undertakes the replacement or repair of all operational systems that contain the bug

5) reports progress to the Center on a weekly basis

6) packages the repair or replacement in such a fashion that the exploitable bug is not easily determinable from the repair distribution.

The RM-Plan must explain how these and related tasks will be accomplished in case of product failure, and must state corporate policies for using exception-fix procedures and for correcting bugs in subsequent scheduled product releases.

The RM-Plan must also describe the vendor's internal procedures for restoring the RAMP process if there is a process failure (and if the Center determines that the process can potentially be restored). These procedures include: establishing the precise nature of the error or breakdown and the reasons for its occurrence; tracing the full ramifications of the problem for all affected product versions; conducting security analysis to establish corrective measures and verify product trust; and reestablishing the unbroken trail of evidence linking to the evaluated product.

7.11 NUMBERING AND RETIREMENT OF PRODUCT VERSIONS

A product release that includes any correction for a bug or flaw becomes a different product from the

standpoint of the Center and the user community. The vendor must develop a product identification system that reflects this fact. A favorable approach is an alphanumeric system in which the numeric portion (typically involving decimals) denotes the product version as released and the letter suffix denotes corrections. For example, version 1.0 might be the original product subjected to evaluation; versions 1.1, 1.2, and so on might be successive releases in RAMP; and versions 1.0a and 1.1a might be the first two versions after a correction has been added. This system yields a two-dimensional product flow as illustrated in Figure 6.

In this example, a system bug is discovered after the second version (1.1) has been released. The development of a correction for this bug yields two new products, 1.0a and 1.1a. Then another bug is identified after version 1.2 has been released. This bug is corrected in

- 1.1 and 1.2, yielding products 1.1b and 1.2b, but is not corrected in 1.0 because the original product version has been retired (as defined below). The two diagonal arrows in the diagram indicate that each bug correction is incorporated in the next scheduled release. Every RM-Plan should establish a product identification system that has this degree of flexibility and comprehensiveness.

The RM-Plan should also indicate that the vendor will inform the Center whenever a rated product version is retired. Retirement is defined in this context as the point at which a vendor no longer offers a product version for sale and no longer provides bug fixes and related services for that version. The Center needs to be informed of retirement decisions so that the affected products can be shifted to a separate section of the EPL.

7.12 MANAGEMENT OF RM-PLAN

Previous discussion has suggested why RM-Plans may change

occasionally and how changes are effected. Due to the possibility of change, the RM-Plan must describe how the plan itself is managed. This discussion should indicate how the vendor establishes a need to change the RM-Plan; how the vendor formulates and proposes specific changes; and how the vendor assures compliance with RM-Plan changes when in place.

8. RAMP TERMINATION, SANCTIONS, AND RISKS

8.1 OVERVIEW OF RAMP PROCESS

Figure 7 depicts graphically various processes from the initial evaluation and VSA training to the establishment and application of RAMP for a product. (Figure 7 is an expansion of Figure 2). The starting points for establishing RAMP are the original product and the training of vendor representatives as VSAs. The vendor develops an RM-Plan and obtains approval for the plan before the Center starts the phase of product evaluation. Figure 7 emphasizes that the RAMP process builds upon an evaluated product and upon the evidence yielded by evaluation.

The RM-Plan establishes a configuration management framework for the analysis, design, implementation, and approval of product changes. The VSAs participate in these rating maintenance actions and assure that security concerns dominate all decisions affecting the product. The outputs of rating maintenance consist of approved product changes and evidence supporting the changes. The VSAs summarize this evidence in an RMR, which is submitted to the TPOC and reviewed by the Center community. The TRB then receives and reviews the RMR, examines the VSAs on the evidence, and recommends that the product rating be extended (or not extended) to the new release. The cycle ends with approval or disapproval of the rating by the Chief of the Product Evaluation Division and listing of the new approved release on the EPL. The TPOC is the interface between the vendor and the Center in all technical communications except the interim and aperiodic reviews and the TRB examination. (The diagram omits the responsible corporate officer and BPOC

roles.)

There is no fixed limit on the number of revision cycles that can be covered by an application of RAMP. The termination of a RAMP process can be either voluntary or involuntary from the vendor's standpoint. A vendor might choose to terminate RAMP because the product is being discontinued; because no further revisions are planned; or because rating maintenance is not considered essential for further releases.

Applications of RAMP tend to have a natural life span ending with the vendor's introduction of a replacement product that requires evaluation and a new RAMP process. Voluntary exits from RAMP are usually pre-arranged to occur at the end of a rating maintenance cycle.

The intermediate cases are situations in which a vendor desires to continue RAMP but needs to implement product changes that RAMP cannot cover. Given a commitment to the changes, the vendor must decide whether to terminate RAMP permanently or undergo reevaluation to start another RAMP process. The requirement for such a choice might be established by the VSAs when analyzing changes during a revision cycle; by the vendor when planning future changes; or by the Center when reviewing the vendor's future change analysis in an RMR. Advance notice of the decision point obviously benefits the vendor by minimizing wasted effort and allowing timely placement of the product in the queue for a reevaluation (if future rating maintenance is intended). Consequently, the vendor should supply as much information as possible to the Center in each future change analysis. The Center attempts to provide an interval of at least one revision cycle within which the vendor can seek reevaluation while rating maintenance is still under way. However, the Center cannot guarantee that this outcome will occur, or that any given rating maintenance cycle will be successful.

8.2 OVERVIEW OF RAMP PROCESS

Involuntary termination of RAMP is associated with failure in the product or process. Failures can be identified through program reviews, TRB examinations, or other mechanisms. The Center response to an identified failure depends upon the nature of the problem and how it occurred.

The Center terminates permanently the use of RAMP for a product if the vendor has knowingly misrepresented any aspect of the product or its RAMP process. The VSA or VSAs responsible for the misrepresentation will no longer be recognized by the Center as representatives of any product. The Center permanently lifts the rating of the product release for which the misrepresentation occurred and the ratings of any later versions dependent upon that release for rating maintenance. Furthermore, the Center activates the aperiodic review process to investigate the possibility of misrepresentations or other errors in earlier releases. The product rating is then rolled back at least to the earliest known breakdown of RAMP assurance.

When an inadvertent failure is identified, the Center may or may not allow the vendor to rebuild RAMP assurance and continue the rating maintenance process. If a failure is identified during a TRB review, the vendor may or may not be allowed to fix the failure and resubmit the product depending on the nature of the failure. A vendor usually is permitted and able to fix a bug (implementation error) while rating maintenance is under way. The Center treats a system flaw (design error) similarly to a bug unless its correction requires an architectural change that RAMP cannot accommodate. The Center does not approve any new ratings until all identified bugs and flaws have been eliminated, but normally does not suspend past ratings so long as the RAMP process is unimpeached and the vendor makes every reasonable effort to protect the user community. A breakdown of process, such as a loss of product evidence, tends to have the most serious consequences for rating maintenance even if no deliberate malfeasance is involved. The Center usually lifts the ratings for all affected releases at least temporarily, and determines on the basis of individual circumstances whether and how the vendor can reconstruct the RAMP process.

8.3 RISKS OF RAMP PARTICIPATION

There are no sanctions in RAMP that apply retroactively to products evaluated by the Center. Choosing to participate in RAMP cannot place an existing product rating in jeopardy. Thus, a vendor's decision to initiate a RAMP process can only create the following risk. There is a chance that the net costs incurred to participate in RAMP will not yield the desired ratings for product revisions, and hence may be viewed as financial losses.

Section 1 has suggested the ways in which RAMP participation can create net monetary costs for a vendor. A major determinant is the extent to which a vendor's business practices need to be altered to meet RAMP requirements for security analysis and configuration management. When evaluating whether these costs and adjustments are supportable, a vendor should be aware of the following considerations.

- 1) The chance that an application of RAMP will be unsuccessful can be greatly reduced by approaching the program constructively and conscientiously. This means allocating the time of highly capable and experienced personnel to the RAMP process; applying scrupulously the RAMP principles of security dominance and configuration management; and keeping the Center as well-informed as possible about upcoming product changes.

2) The net costs of creating and pursuing a RAMP process can be viewed as an investment with potential returns extending well beyond the given product. The capabilities developed in one RAMP experience are valuable not only for other applications of the program but also for the creation of new trusted products from start to finish.

Regarding the second point, the value of in-house security wisdom is increasing very rapidly for computer vendors. Various factors are making access to the expanding market for trusted systems more and more dependent upon the availability of this resource. RAMP is the appropriate context and focus for developing security analysis capability.

APPENDIX

SUMMARY OF RAMP REQUIREMENTS

This appendix summarizes the vendor's and the Center's requirements for RAMP. These requirements are linked to the timing of the product evaluation and are listed in approximate order of occurrence, under the phase of the evaluation process in which they occur. A vendor failing to satisfy these requirements loses the opportunity to participate in RAMP until such time as the product in question is reevaluated. The Center reserves the right to deny a rating and/or discontinue the Rating Maintenance Phase at any time.

PREEVALUATION PHASE

- 1. Vendor establishes an intent to participate in RAMP in the evaluation package/proposal for a given product.

VENDOR ASSISTANCE PHASE/DESIGN ANALYSIS PHASE

- 1. The vendor must identify and maintain a responsible corporate officer. The responsible corporate officer represents the vendor in administrative matters, serves as the point of vendor accountability to the Center, is able to make decisions and corporate commitments on behalf of RAMP, and supports the technical role of the VSA.

2. The vendor must complete training of one or more Vendor Security Analysts (VSAs) before implementation of the vendor's Rating Maintenance Plan but not later than completion of the IPAR. The vendor must provide for VSA access to the Center's Dockmaster computer system at the time VSA training begins. Whenever a vendor uses more than one VSA, a lead VSA will be identified by the vendor.

3. The Center will provide RAMP training for VSAs.

4. The vendor must develop, have approved, and implement a

Rating Maintenance Plan (RM-Plan). The RM-Plan must be approved by the Center prior to its implementation but not later than completion of the IPAR. The approved RM-Plan must be implemented before development begins on the version that will supersede the evaluated version.

- 5. The Center will review the vendor's RM-Plan for purposes of approving the RM-Plan.

EVALUATION PHASE

1. The vendor must maintain a responsible corporate officer.

2. The vendor must maintain one or more Center-trained Vendor

Security Analysts (VSAs) once the vendor's RM-Plan has been implemented. The vendor must provide for VSA access to the Center's Dockmaster computer system. Whenever a vendor utilizes more than one VSA, a lead VSA will be identified by the vendor.

3. The Center will provide RAMP training for VSAs.

4. The vendor must complete implementation of the

Center-approved Rating Maintenance Plan (RM-Plan) and must follow the business practices outlined in the RM-Plan. The RM-Plan must be implemented before development begins on the version that will supersede the evaluated version. Any changes to the RM-Plan must be approved by the Center and must be made according to the provisions within the approved RM-Plan.

5. The vendor must conduct, for his own purposes, an initial

RAMP audit to assure that security feature functionality and assurances are being maintained by adherence to all the procedures established in the vendor's approved RM-Plan.

6. The Center evaluation team will review the results of the vendor's initial RAMP audit to ensure the vendor's RAMP process follows the procedures outlined in the vendor's RM-Plan.

7. The Center assigns a Technical Point of Contact and a Business Point of Contact before completion of the evaluation phase. The TPOC advises and coordinates the use of RAMP for the given product. The BPOC handles administrative and programmatic aspects of the process.

RATING MAINTENANCE PHASE

- 1. The vendor must maintain a responsible corporate officer.

2. The vendor must maintain one or more Center-trained Vendor Security Analysts (VSAs) once the vendor's RM-Plan has been implemented. The vendor must provide for VSA access to the Center's Dockmaster computer system. Whenever a vendor uses more than one VSA, a lead VSA will be identified by the vendor.

- 3. The Center will provide RAMP training for VSAs.

4. The Center maintains a Technical Point of Contact and a Business Point of Contact.

5. The vendor must provide product instruction for the Center Technical Point of Contact, as needed

throughout the Rating Maintenance Phase. This is to include product documentation, vendor provided classes, and hands-on system access time.

6. The vendor will provide quarterly informal status reports to the Technical Point of Contact via the Center's Dockmaster system throughout the Rating Maintenance Phase.

7. The vendor must conduct, for each RAMP cycle, at least one RAMP audit to assure that security feature functionality and assurances are being maintained by adherence to all the procedures established in the vendor's approved RM-Plan.

- 8. The Center Technical Point of Contact will review the results of the vendor's RAMP audit to ensure the vendor's RAMP process follows the procedures outlines in the vendor's RM-Plan.

9. The vendor will submit concurrently to the Center the following documents for each version of an evaluated product for which the vendor desires to have the rating maintained via RAMP:

- a) Rating Maintenance Report (RMR)

b) Rating Maintenance Plan (RM-Plan) with change bars

c) Final Evaluation Report with change bars

d) Final Evaluation Report with integrated changes

e) Proposed product description for EPL

The documents intended for public release are the final evaluation report with integrated changes and the proposed product description for EPL.

- 10. The Center will review the vendor's documents for purposes of extending the rating to the specific release and for placement on the Evaluated Products List.

11. The vendor's RAMP process is subject to two types of reviews (Interim Reviews and Aperiodic Reviews) by the Center. Both types of program review have the purpose of assuring that security feature functionality and assurances are being maintained by adherence to all the procedures established in the vendor's approved RM-Plan.

GLOSSARY

BPOC - Business Point of Contact (Center).

CCB - Configuration Control Board.

Center - National Computer Security Center.

CF - Code Freeze.

CI - Configuration Item.

COMPUSEC - Computer Security.

CRB - Configuration Review Board.

Criteria - Same as TCSEC.

Dockmaster - A Center computer system serving

the evaluation community.

ECO - Engineering Change Order.

EPL - Evaluated Products List.

Evaluated Product - A product version that has undergone evaluation by the Center. (By convention, excludes products assigned D ratings. An evaluated product is always a rated product, but the reverse is not always true for products in RAMP.)

FER - Final Evaluation Report.

Interpretations - Published Center Interpretations of the TCSEC.

IPAR - Initial Product Assessment Report.

PTR - Preliminary Technical Report.

RAMP - Rating Maintenance Phase.

Rated Product - A product version with a TCSEC rating and a listing on the EPL, obtained either through evaluation or RAMP. (By convention, excludes products with D ratings.)

RM-Plan - Rating Maintenance Plan.

RMR - Rating Maintenance Report.

SIR - Service Improvement Request.

TCB - Trusted Computing Base.

TCSEC - Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD); the Criteria against which products are evaluated to establish security ratings.

TPOC - Technical Point of Contact (Center).

TRB - Technical Review Board (Center).

VSA - Vendor Security Analyst.

BIBLIOGRAPHY

Department of Defense Trusted Computer System Evaluation Criteria, December 1985 (DOD 5200.28-STD).

Brown, Leonard, R. "Specification for a Canonical Configuration Accounting Tool," Proceedings of the 10th National Computer Security Conference, 21 September 1987, p. 84.