Trusted Product Evaluation Program Procedures

Contents

1.0 Overview of the Trusted Product Evaluation Program (TPEP)

1.1 Background

In January 1981, the Department of Defense assigned responsibility for Computer Security to the Director of the National Security Agency (NSA). The DoD Computer Security Center was formed as a result of this action that same year, and was later renamed the National Computer Security Center (NCSC). The Center's Charter, promulgated in DoD Directive 5215.1, specifically tasks the Center to establish and maintain...

"... technical standards and criteria for the security evaluation of trusted computer systems that can be incorporated readily into the Department of Defense component life-cycle management process..."

The NCSC issued the first DoD Trusted Computer System Evaluation Criteria (TCSEC), commonly referred to as the "Orange Book," in August 1983. It was reissued in December 1985 as a Department of Defense Standard. The TCSEC Standard is specifically intended to serve the following purposes:

o To provide a standard to manufacturers regarding what security features to build into their new and planned commercial products that will provide widely available systems that satisfy trust requirements (with particular emphasis on preventing unintended disclosure of data) for sensitive applications.

o To provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

o To provide a basis for specifying security requirements in acquisition specifications.

To provide DoD components with a security evaluation metric, the TCSEC associates defined levels of trust with a rating identified by a digraph. Each identified level of trust builds upon the previous level to increase the security features of a product and assurance to the user that the product will function as designed. While the TCSEC is the basic guideline for TPEP evaluations, it is augmented by other process requirements which will be discussed in these procedures such as Technical Assessment (TA), Intensive Preliminary Technical Review (IPTR), RAMP, and documentation.

For TPEP, the TCSEC is applied to evaluate the computer product while excluding the application environment. The goal of this type of analysis is to provide system engineers with system components that have known trust and security features. Assessment of the product's appropriateness for a specific environment is in the realm of the certifier/accreditor community and will not be addressed here.

The Information Systems Security Organization (ISSO), which is the NCSC's parent organization at NSA, evaluates security features and assurances of trusted products against the TCSEC and its interpretations through the TPEP. Under the TPEP, vendors approach the ISSO with their commercial-off-the-shelf (COTS) trusted computer security product requesting an evaluation targeting a specified level of trust rating. The results of the TPEP evaluations are published semi-annually in the Evaluated Products List (EPL) as Chapter 4 of the Information Systems Security Products and Services Catalogue. The EPL provides an unbiased and authoritative evaluation of a product's suitability for use in processing classified and sensitive information. The product rating contained in the EPL is the highest class for which that product met or exceeded each of the individual requirements contained in the TCSEC.

1.2 TPEP Goals

The ultimate goal of the Trusted Product Evaluation Program is to encourage the widespread availability of trusted computer products to data owners and users who wish to protect their sensitive and/or classified information. Additional goals are:

o To ensure the availability of useful trusted products that meet the end user's operational needs.

o To provide trusted products to be used when constructing an implemented trusted system.

o To provide specific guidance on the utility of trusted products.

o To provide specific guidance on the interoperability of the security features and the level of assurance associated with specific features for individual evaluated products.

o To foster an open and cooperative business relationship with the computer and telecommunications industries which will result in the fulfillment of INFOSEC requirements for the National and Defense Information Infrastructures.

1.3 TPEP Process Overview

The TPEP focuses on the security features and assurances of commercially produced trusted products which include operating systems, networks and/or network components, and application products such as database management systems. The evaluation process consists of Pre-Evaluation, Evaluation, and the Rating Maintenance Program (RAMP). This section provides a brief overview of the TPEP process. A more detailed description of each step in the process is contained in later sections.

1.3.1 Pre-Evaluation

The following must be performed leading up to the start of an evaluation of a trusted product. These activities ensure that the product and its associated evidence are ready for the evaluation process to begin.

1.3.1.1 Receipt of Proposal

NSA reviews the vendor's product proposal to ascertain if the product is likely to meet the TCSEC requirements, has good market potential, and if the product design is at an appropriate level of maturity.

1.3.1.2 Technical Assessment

For those products which are candidates for evaluation, a vendor must demonstrate that the product design and the associated evaluation evidence are complete. A Technical Assessment is often the first examination of the product and evidence. The outcome of a Technical Assessment is a recommendation to receive commercial or NSA advice, schedule an Intensive Preliminary Technical Review or to terminate the evaluation effort because of technical shortcomings of the product. Technical assessments can also be used as tools throughout advice to gauge progress toward evaluation.

1.3.1.3 Advice

To assist the vendor with their preparation for evaluation, NSA may recommend the vendor seek outside advice or NSA advice, depending on the product's complexity, level of trust and available NSA evaluator resources. NSA resources are assigned to provide advice for a specified period of time. Advice should culminate in a successful Intensive Preliminary Technical Review. At the end of the specified period of time, progress toward the IPTR is noted, market potential is again reviewed and a decision is made to hold the IPTR, continue advice, or discontinue advice.

1.3.1.4 Intensive Preliminary Technical Review (IPTR)

The purpose of an IPTR is to accurately assess completeness of both the product and the evaluation evidence and to ensure the vendor's readiness to undergo evaluation. A larger team of NSA evaluators assess the product and evidence and recommend whether or not the product should enter evaluation.

1.3.2 Evaluation

The vendor provides the evaluation team with system level, developer-oriented training for the vendor's product. Training is followed by a comprehensive review, by the evaluation team, of the system design. The team performs security analysis of the product design including both hardware and software components of the system. The team reviews the completed design, user, test and Rating Maintenance (RM) documentation. The team uses the information gathered during design analysis to write an Initial Product Assessment Report (IPAR) which is presented to a Technical Review Board (TRB). The team also briefs the TRB on the vendor's plans and the team's plans for testing the product. After the evaluation team performs security testing on the product at a site provided by the vendor, the results are included in the IPAR, which is transformed into the Final Evaluation Report (FER). The evaluation team presents the results of testing at the Final TRB, and the TRB makes its recommendations to NSA management, which makes the final decision as to entry on the Evaluated Products List.

1.3.3 Rating Maintenance Program

The Rating Maintenance Program (RAMP) provides a mechanism for a vendor to maintain the TCSEC rating of a product throughout its life cycle. During RAMP, the vendor works with the NSA Technical Point of Contact

(TPOC) to discuss proposed changes to an evaluated product. The Vendor Security Analyst (VSA) performs a security analysis of the product changes as they occur. For C2 or B1 products where the change analysis is entirely the responsibility of the vendor, the vendor presents all security relevant changes to a Technical Review Board (TRB) which makes a recommendation to NSA management regarding approval of the effort to date, and/or recommended actions for the team. If changes are approved, the original rating is applied to the current version of the product, and an entry in the EPL is made to document the maintenance of the rating. The Final Evaluation Report is updated by the vendor. RAMP is mandatory for all products involved in the TPEP.

2.0 Eligibility Requirements

[Top of Document]

2.1 Market Review

After receipt of the vendor's product proposal, the potential market for the product as described by the vendor will be reviewed for validation with market literature or sources. To allow NSA to assess the U.S. Government requirements for any product, the vendor must provide sufficient detail to identify its utility in the marketplace. For details on the minimum market information that NSA requires in the proposal, see section 3.3.1.

NSA will review the proposed product to determine if it has a satisfactory market share as compared to other similar products in the commercial sector (e.g., XYZ Company's proposed relational database product makes up 35 percent of the total U.S. installed base of this type of product).

In addition to looking at installed bases, NSA will review currently available market trend information to determine if the product could satisfy a need for trust technology which is not currently available.

2.2 Financial Review

In addition to vendor-provided financial reports, NSA will check the vendor's financial stability to complete the TPEP evaluation and make the evaluated product commercially available. One source for validating this information is the listing of financial indicators published by Dunn and Bradstreet. The vendor must be incorporated in and operating under the laws of the United States of America, and the vendor must show evidence of a corporate commitment to allocate resources to produce a trusted product.

2.3 Acceptance of Products for Evaluation

The decision to accept or reject products for TPEP evaluation and to prioritize them for evaluation will be based upon information provided in the product proposal. The following items must be addressed:

o The vendor must demonstrate that the product satisfies the requirements of the Trusted Computer System Evaluation Criteria (TCSEC) or its interpretations (e.g., the Trusted Database Management System Interpretation - NCSC-TG-021, dated April 1991, the Trusted Network Interpretation - NCSC-TG-005, dated 31 July 1987, etc.).

o The vendor must demonstrate sufficient technical expertise and resources to undertake the evaluation.

o The vendor must demonstrate the company's preparedness to begin the evaluation process within one month after execution of the Evaluation Agreement (EA).

o The vendor must demonstrate the company's intention to satisfy the requirements of the Rating Maintenance Phase (RAMP).

The proposal must demonstrate the market potential of the product. Some examples of market potential are that the product:

o Provides a trust solution to satisfy an expressed need of a member of the DoD or Intelligence Community for commercially available systems.

o Will help expand the coverage of the Evaluated Products List (EPL) by providing trust for a specified hardware/operating system for which none exists or for which no solution exists at the targeted level of trust.

o Has a satisfactory market share as compared to other products of this type in the commercial sector (e.g., XYZ Company's proposed relational database product makes up 35% of the total U.S. installed base of this type of product).

o Provides a critical technology to the DoD and/or Intelligence Community.

3.0 Pre-Evaluation

3.1 Initial Contact

NSA's initial point of contact for the Trusted Product Evaluation Program (TPEP) is the ISSO Business Affairs Office. Interested companies are invited to call or write to:

Trusted Product Evaluation Program
National Security Agency
9800 Savage Road Suite 6740
Fort George G. Meade, Maryland 20755-6740
(410) 859-6091 **EFFECTIVE 21 DECEMBER 1998 (410) 854-6091**

Vendors should request information on the TPEP process and inform NSA of their potential product, its proposed level of trust, a brief description of the company and its primary market objectives, and proof that the company is located in and owned and operated under the laws of the United States (date and place of U.S. incorporation, if

applicable, will be acceptable). Upon receipt of this information, V21 will prepare and mail a TPEP introductory package to include:

A TPEP Introductory Letter: This letter is a brief description of the TPEP Process and the vendor's requirements for submission of a vendor's product proposal. The letter extends to the vendor an invitation to attend a pre-proposal technical meeting with appropriate NSA representatives who will be able to discuss the TPEP process in depth. V21 will conduct the introduction to the meeting and discuss the business aspects of the proposed effort. A representative from NSA's technical evaluation staff will then discuss the evaluation process. Any other questions the vendor may have can be addressed at that time. A pre-proposal meeting is at the option of the vendor.

The TPEP Procedures: This contains detailed instructions about the TPEP process including specific contents of the product proposal, directions for the Technical Assessment (TA) and/or Initial Product Technical Review (IPTR) preparation, and the requirements for Evaluation and Rating Maintenance. There are also sections that discuss vendor eligibility, TPEP termination standards and process, and NSA's policy on protecting vendor Proprietary Information.

The Department of Defense Trusted Computer System Evaluation Criteria (TCSEC): The TCSEC provides the evaluation criteria and is mandatory for use by all DoD Components in carrying out technical security evaluation activities applicable to the processing and storage of classified and other sensitive DoD information.

The Rainbow Series Documents: The Rainbow Series documents are technical guidelines designed to provide insight into the TCSEC requirements and guidance for meeting each requirement. These guidelines are published in pamphlet form and each bound in a distinctively colored cover.

The Information Systems Security Products and Services Catalogue: This catalogue is a listing of U.S. Government-evaluated Information Systems Security products and services, which may be used to protect information at several levels of sensitivity. Chapter 4 contains the Evaluated Products List (EPL), which provides system developers, managers, and users an authoritative evaluation of a product's relative suitability for use in processing sensitive information.

Documents on the Form and Content of the Design and Test Documentation: These documents identify the design and test information required to satisfactorily complete a C2 or B1 evaluation. They provide a systematic approach for the vendor to identify design and test documentation requirements and to enable vendors to plan for the creation of required test and design documentation. Both guidance documents provide an opportunity for a vendor to reuse existing documentation. A brief description of these design and test documents follows:

o Architecture Summary Document (ASD) - The ASD gives an overview of the hardware and software of the product and then describes the architecture by analyzing the product by logical subsystem. A description of each logical subsystem is given with references to the other documents in this series and to the detailed design documentation. The ASD functions as a roadmap for architecture information.

o Interface Summary Document (ISD) - The ISD begins with a narrative overview that describes the interface classes of a product and then provides interface summary tables. The tables are organized by logical subsystem, all the security relevant interfaces of the product are listed, both summary information on the type of interface and pointers to detailed information on the interfaces are provided.

o Extended Philosophy of Protection (POP) - The POP covers the subjects and objects of the product, the security policy, the mechanisms that support the policy and the approach to assurance. The POP is called extended because it must detail, requirement by requirement, how the product meets the TCSEC.

o Test Matrix Document (TMD) - The TMD is essentially an index to the vendor's testing documents. It provides an overview of the testing documentation, a high- level matrix and multiple low-level matrices. The high-level matrix maps pairs to sections of a test procedures document. The high-level matrix is the first step in test coverage analysis. The lower level matrices map pairs to more specific test procedure references.

A Sample TPEP Evaluation Agreement (EA): The Evaluation Agreement is the legal agreement that must be executed prior to evaluation of a TPEP product. Upon proper execution, the EA sets forth the legal responsibilities of the vendor and NSA in conducting a TPEP evaluation.

A TPEP Questionnaire: This questionnaire helps the vendor to prepare the technical part of a product proposal. Different portions of the questionnaire apply to different types of products and different levels of trust.The product questionnaire must be returned to NSA as part of the product proposal.

3.2 Vendor Proposal

After receiving the TPEP Introductory Package from NSA, if the vendor chooses to pursue evaluation, he should forward a product proposal providing the following information:

Product Overview
A completed Trusted Product Evaluation Questionnaire
A brief corporate history, and
A corporate organizational chart identifying:

(1) A Responsible Corporate Officer (RCO). The RCO should be able to commit the company to legal agreements defining evaluation responsibilities.
(2) A Business Point of Contact (BPOC) who is the person best able to answer questions from potential customers as well as NSA market utility questions on the current and forecast federal demand for the product proposed for evaluation. The BPOC should also be prepared to provide technical points of contact for questions from NSA about the product's technical capabilities and design.

The proposal must demonstrate the product's direct and obvious benefit to the Information Systems Security posture of the nation, and should address the applicable requirements outlined in the TCSEC or its interpretations. This determination will be based on the information contained in the product proposal and TPEP questionnaire, measured against national computer security needs and priorities as discussed in Section 2. The vendor should submit the product proposal and completed TPEP questionnaire to NSA/V21.

3.3 Product Proposal Review

A product proposal is reviewed for two purposes. The first is to determine the potential market benefits of accepting the product for evaluation (i.e., are there customer requirements for such a product?). It should be noted that the information provided in the proposal is not the sole basis for this decision. The TPEP actively solicits customer input on requirements and maintains this information for use when determining the market impact of a product proposal. The second purpose of a proposal review is to determine, at a very preliminary level, if the product appears to provide feasible security mechanisms such that the requirements of the TCSEC or of the TCSEC as interpreted by the TNI or TDI can be satisfied.

3.3.1 Market Information

The market information portion of the proposal package must include the following and may include additional information believed to support the proposal:

o Compare and contrast the proposed product and similar products that are now available showing the advantages of the proposed product.

o List the intended market, including a current customer base. State what requirements customers have established, in terms of functionality and level of trust.

o State what portion of the market the product is intended to address and how you derived the specific market projections. If the product to be developed is a retrofit or a new version for existing equipment, include the

potential volume of sales for those existing equipment already fielded.

o List known or projected U.S. Government requirements that the product will satisfy, stating the approximate number of products needed by each Government agency or service. List the same for civilian agency or commercial requirements that the product will satisfy.

o Include in the market identification both current and forecasted demand, indicating both the current installed base of the proposed product (or planned host system) and the forecasted growth of this base through new sales or migration from earlier systems. Distinguish among U.S. Department of Defense, U.S. Intelligence Agencies, other Federal Agencies, and non-government purchases.

3.3.2 Technical Information

Using the product questionnaire as guidance, the vendor must discuss and define the proposed product's configuration, the Trusted Computing Base (TCB), the underlying security policy, and subjects and objects as these items pertain to the specific product. The product proposal must contain a complete technical overview of the product with regard to how it meets the requirements of the targeted level of trust. Vendors should note specialized sections of the product questionnaire that must be answered for products such as network systems and components, databases, etc.

If a proposed product incorporates trust technology from another vendor, the vendor submitting for the evaluation must be prepared to explain the interaction of both products in the proposal, during the IPTR, and during the evaluation. The NSA evaluation team will work directly with the vendor who proposes a product for evaluation. That vendor bears the sole responsibility for providing all necessary evaluation evidence to support the evaluation team's analysis. The NSA will not solicit input from a second party vendor. The submitting vendor should include in the proposal evidence of a legal agreement with any second party vendor providing access to and use of the product and associated documentation as well as test suites and test procedures.

3.3.3 Proposal Review Decision

If, in the opinion of NSA, the proposed product is expected to meet the TCSEC requirements and has the appropriate technical and market characteristics, NSA will accept the product as a candidate for evaluation and will assist the vendor in preparing for evaluation. During the proposal review, NSA may request that the vendor supply additional information regarding either the market or technical content of the proposal.

If the proposed product clearly lacks technical merit or market utility, NSA will reject the proposal and provide the vendor with the rejection rationale.

3.4 Technical Assessment (TA)

A Technical Assessment (TA) is an effort by a small team of evaluators to provide a quick assessment of the state of the product and its associated evidence. A TA is a short term activity, limited in scope, based on the product complexity, estimated vendor preparedness, and targeted level of trust. This assessment provides the vendor with guidance on what remains to be done before an Intensive Preliminary Technical Review (IPTR) can be scheduled. If advice is recommended, the TA is the technical foundation for advice givers to use as they become acquainted with the product's functionality and security posture. The TA will also recommend to NSA management the level of advice that is required and how long it should continue.

Technical Assessments, although often used to give the initial assessment of a vendor's readiness for evaluation, are also tools for advice givers to use while preparing for evaluation. For example, a TA can be used to gather information on a specific issue or section of the product.

A TA may consist of vendor presentations, informal question and answer sessions or any other appropriate form for the exchange of information. Subjects of a TA will include the security policy, Trusted Computing Base

(TCB) identification, subject and object identification, the implementation of security mechanisms, and progress on user, design, and test documentation. At the conclusion of a TA, the team will generate a report documenting the meeting. This report will be used in the assessment of vendor readiness for evaluation and required advice. The report will be reviewed by NSA management and provided to the vendor within three weeks. The TA team will recommend that one of the following actions be taken by NSA:

o The vendor should seek commercial advice and NSA should not spend resources until the vendor believes the product is ready for evaluation. At that time another TA will be scheduled. If NSA is confident that the vendor is well prepared for evaluation, an Intensive Preliminary Technical Review (IPTR) will be scheduled.

o NSA should provide advice givers until the product is ready for evaluation. Once advice givers believe the product is ready for evaluation, an IPTR will be scheduled.

o NSA should not consider this product for evaluation because of technical shortcomings.

o In an exceptional case where advice is not required, the TA team can recommend that an IPTR be scheduled.

3.5 NSA Decision

The results of the proposal review and the first TA will be used by NSA management to verify that the product is a good technical candidate for evaluation. If the decision is NO, the vendor is provided a rationale for this decision and the product is rejected. The vendor may re-submit a product for evaluation at a future time when the rationale for rejection is no longer valid (i.e., the product design has been changed to allow evaluation against an existing set of requirements, a new set of requirements is established, etc.) If the decision is YES, then a second decision must also be made, whether or not NSA resources will be used to advise and assist the vendor in preparing for evaluation.

NSA management will review the recommendations of the TA team, and determine whether NSA or commercial resources will be utilized, the level of NSA resources to apply, for how long to apply the resources, and when to review the product again to gauge progress both technically and to reassess the continued marketability of the product. These decisions will be documented and send to the vendor.

Technical Assessments that are not the initial review of the product will contain other recommendations relative to the product's progress to evaluation. For example, a Technical Assessment may have been done to determine what was left to complete for an IPTR and may recommend that additional resources be added and/or an IPTR be scheduled within a certain timeframe. NSA management will review these recommendations, document any decisions made, and send these to the vendor.

3.6 Advice

NSA may provide advice to the vendor in order to assist them with the preparation for evaluation. NSA will only provide resources for advice if NSA and the vendor believe such advice is mutually beneficial. The nature of this advice and the role of NSA personnel providing advice will be determined based on one or more technical assessments of the vendor's product and readiness for evaluation. NSA will provide clarification of documentation requirements and security requirements as well as guidance in preparation for RAMP. NSA will assign the appropriate number of evaluators (typically two) to provide advice. At the start of advice, the vendor will be sent a letter containing the names of the advice givers, expected timeframe for advice, pertinent sections of the prior TA, and an anticipated IPTR date. NSA resources are assigned according to the level of trust, type of technology, the potential market, and the priority of the product for the Department of Defense and Intelligence Community. Generally, products targeted at higher levels of trust receive priority over products at lower levels of trust, and products developed using a new and innovative technology receive a higher priority than products of outdated technology.

The advice schedule is dependent on the type of product, level of trust and the result of the preceding TA. The TA will be provided to the vendor and advice givers and should be used to guide what advice is needed.

3.6.1 NSA Advice vs. Commercial Advice

NSA evaluators will give trust technology design and documentation advice for the following types of products:

o Products that are a unique or new technology (i.e., a unique network device); or

o Products that are of high priority for the Department of Defense and Intelligence Community (i.e., a primary platform for a major DoD program)

o Products that have a substantial market impact

NSA will only commit to providing identified resources for a specific period of time. If that time passes and the product is not ready for an IPTR to be scheduled, NSA will only continue to provide advice after NSA management reviews resource availability and the resource requirements of other potential products seeking NSA advice. Whenever the period of time for which NSA has agreed to provide advice passes (usually a scheduled IPTR date), NSA may recommend the vendor seek commercial advice and cease to provide advice. In all cases, the continuance or discontinuance of advice will be documented and sent to the vendor.

3.6.2 Content of NSA Advice

The advice givers will provide instruction about the level of detail and content in design and test documentation. More specific advice will be provided in response to vendor queries on a case by case basis. NSA advice will be provided for issues relevant to the following activities:

o Assistance in Understanding the TPEP Process

o Interpreting TCSEC requirements

o Product design

o Modelling (model creation and interpretation)

o Design and test documentation requirements

o RAMP requirements

o Implementation questions relative to product design

o User documentation coverage requirements

Once an evaluation of the product actually begins, problems that must be fixed are not restricted to problems identified while the vendor received advice from NSA.

3.6.3 Communication During NSA Provided Advice

Communication between vendor and NSA advice givers will be primarily by telephone. NSA evaluator travel will be minimal. A Dockmaster computer account will also provide an important means of communication. All advice that is given and all minutes from meetings with the vendor during the period of time when advice is given, will be documented and posted on Dockmaster.

3.6.4 Commercial Advice

Vendors will usually be asked to seek commercially available trust technology design and documentation advice:

o for products that are targeted at the lower levels of trust (i.e., B1 and C2)

o for products for which there is only a marginal market, or for which a market is dependent on the outcome of an RFP

o if NSA evaluation resources are not available

For the case in which guidance is provided by a commercial organization, NSA will not participate in the negotiation of an expected completion date for that guidance/advice, this schedule will be between the vendor and the commercial organization.

NSA will have a vendor liaison assigned to the vendor receiving commercial advice. This vendor liaison will track the vendor's progress and be knowledgable of the targeted advice schedule.

Communication between the vendor and an outside advice giver is entirely the responsibility of the two parties involved. Current interpretations of the criteria for evaluation will be publicly available electronically on Dockmaster and consultants should be aware of and use this information in their consulting role.

The vendor has the sole responsibility to choose and contract for commercially available guidance. NSA does not endorse or recommend any vendors for guidance about trust technology issues.

Vendors should require that the outside advice givers document all communication, including meetings between the vendor and advice giver for their own records. Some of this information may be useful in the subsequent IPTR and/or Evaluation. It is the vendor's responsibility to notify their vendor liaison at NSA when they will be ready for an IPTR.

3.7 Intensive Preliminary Technical Review (IPTR)

Before a TPEP evaluation begins, NSA will meet with the vendor's technical experts to conduct an Intensive Preliminary Technical Review (IPTR). This review will ensure that the acceptance of the product for TPEP evaluation is based on a sound technical understanding of the product. The IPTR will also verify the vendor's readiness for evaluation. The length of an IPTR is variable but will generally last 7-10 days and involve approximately 5 evaluators. An IPTR is expected to occur when the vendor, the advice givers, and the NSA project manager agree that the product is ready for evaluation. Assuming an evaluation team could be assembled immediately after a product passes an IPTR, it should begin about 8 months before product release.

The vendor needs to have both presentations and documentation prepared for the IPTR. The presentations should be given by developers who are knowledgeable about the product to be evaluated. There should be at least two hard copies of the documentation along with an on- line version, available to the IPTR team. The team will spot check each document for completeness. The vendor will insure that appropriate experienced developers knowledgeable about the product are available during the IPTR team document review to answer questions.

3.7.1 Items Required During an IPTR

The vendor must provide the Architecture Summary Document (ASD), the Interface Summary Document (ISD), a Philosophy of Protection (POP), as described in the Form and Content of Vendor Design Documentation document and a Test Matrix Document (TMD) as described in the Form and Content of Vendor Test Documentation document. These documents describe information required to evaluate a product against the TCSEC and detail the format to be used. This will help the IPTR team to quickly summarize the product's architecture and security policy and begin their analysis. Most of the content of the documents identified above encourage reference to existing documents, if they exist.

In addition to the ASD, ISD, POP, and TMD, all evaluation evidence as required by the TCSEC should be available to the IPTR team; these include:

o Detailed design documentation for security important components and interface documentation for the rest of the TCB

o List of TCB Components

o Philosophy of Testing and complete test plans and test procedures. The vendor need only demonstrate that progress is being made on the actual code for individual test cases.

o Trusted Facility Manual (TFM)

o Security Features User's Guide (SFUG)

o Informal Model (for B1 products)

o A Rating Maintenance Plan (RM Plan) including samples of information needed for a RAMP audit

Sample IPTR Schedule

This sample schedule is to guide vendors and IPTR teams as to what must be covered/accomplished during the IPTR. This agenda should be customized for each product depending upon the size and complexity of the product, any unique features about the product, and/or the status of any of the items listed below.

For C2-B1 Levels of Trust:

o Vendor product overview presentation (.1 day)

The overview is intended to orient the IPTR team so they will be thinking about the right type of product in the types of environment that it would be intended for trusted use. The Vendor should describe the type of product, size, performance range, intended environments including the administrative and user, networking, distribution, usual type of applications, etc. The history of the product and the company should be summarized. The schedule of the trusted product development should be summarized.

o Vendor hardware architecture presentation (.3 day)

The hardware architecture presentation should concentrate on the security relevant parts of the hardware architecture. For the CPU, the discussion should include such things as execution modes, privileged instructions, the I/O instruction interface, a summary of interrupts and exceptions, memory management, and any hardware support for process management. The security aspects of other hardware components should be discussed including network interfaces, support of peripheral controllers, operator consoles and maintenance consoles.

o Vendor software architecture presentation (1 day)

The software architecture presentation should begin with a TCB definition including a pointer to a list of TCB components and a definition of the TCB interface. TCB structuring should be described (e.g., kernel subsystems, trusted processes) including a discussion of criteria and philosophy behind their use of trusted processes. Then the security relevant aspects of the software implementation of memory management, process management, interprocess communication, filesystem and I/O, network communications, batch processing, I&A, logon, printer, tape and disk services, mail, import and export, backup and restore, system installation, initialization and shutdown, auditing, etc. should be discussed. The security relevant data structures should be described. Any software support for networking and window systems must also be described.

o Vendor presentation of Subjects and Objects (.2 day)

The TCB's protected resources should be described, beginning with the product's subject(s) and their relation to users and the various user roles (including the methodology for defining administrative roles). The product's objects including devices, deferred execution resources (e.g., crontab) and network resources, should be discussed.

o Vendor presentation of protection policies and access control (.7 day)

If appropriate, the B1 security model should be summarized and its style and view described. The protection policies (e.g., DAC, MAC, object reuse) supported by the product should be described and how they apply to the already discussed subjects and objects. I&A, audit, and privilege mechanisms (e.g., reserved ids, reserved labels, privilege vectors) should be covered.

o Vendor presentation of system architecture assurances (.1 day)

The argument as to how the TCB is protected from tampering and is always invoked, and the argument for process separation should be made.

o Vendor presentation of RAMP process/procedures (.3 day)

The vendor should present an overview of their RAMP Plan and explain their processes and procedures. They should also describe how the IPTR team can review some of their RAMP evidence for changes to the product.

o Vendor presentation of documentation overview (.2 day)

The vendor should give an overview of how their documentation is organized. For the design documentation the vendor's overall approach should be described and then an argument should be made for the completeness of Architecture Summary Document and the TCB Interface Summary Document and the mappings to the detailed documents. (see the PAT Guidance Working Group, Form and Content of Vendor Design Documentation. T contents of the Philosophy of Protection should be summarized. For test documentation the vendor's overall approach should be described and (see the PAT Guidance Working Group, Form and Content of Vendor Test Documentation) then examples presented of the Vendor's high and lower level matrices, test plans and test procedures. The vendor should then make an argument about the completeness of the documents, plans and procedures. The vendor should also summarize the contents of the TFM and the SFUG. The vendor should describe how to access the documents on- line (if available) and any tools available to support that access.

o IPTR team reviews user and administrator documentation (.5 day)

o IPTR team reviews design documentation (2 days)

o IPTR team reviews test documentation (1 day)

o IPTR team reviews RMPlan and looks at RAMP audit evidence (.5 day)

The entire IPTR team should read the POP, and at B1, the model, and skim the TFM and SFUG. During the earlier presentations the security enforcing portions of the TCB will have been identified. The documentation and the tests on these subsystems (especially the trusted processes) should be divided among the team members and portions reviewed extensively to check its consistency, its thoroughness, and its completeness, especially in relation to the vendor's presentation of its contents. This review should check for consistency between both the design, user, and test documentation. The interface documentation for the non-security enforcing portions of the TCB should also be sampled. The RMPlan should be read and a mini-RAMP audit conducted to see if the Plan reflects actual procedure.

o Prepare IPTR Report (2 days)

In most cases, evaluators will provide the necessary computer equipment for writing this report. The vendor will be asked to supply adequate space and a postscript printer.

3.7.2 Team Composition and IPTR Preparation

It is likely that at least one technical assessment will have occurred before the IPTR. The report from that technical assessment should be available to the IPTR team, on-line before they attend the IPTR. The advice givers (whether NSA or commercial) for a product that has been receiving advice should also provide the IPTR team with a written assessment of why they think that the product is ready for an IPTR. The NSA manager in charge of the product should have approved and added their input to that assessment. Each member of the IPTR team should be given an advanced copy of product proposal and the completed product questionnaire before traveling to the IPTR.

At least some of the Advice givers and likely evaluation team members should be included on the IPTR team. When the IPTR team members are assigned, a IPTR team leader will be appointed and will be responsible for ensuring that all IPTR team members have received the necessary information. The team leader of the resulting evaluation will also be appointed at this time so that they can participate in the IPTR.

3.8 IPTR Results

The result of an IPTR is the IPTR Report which is prepared by the evaluators who compose the IPTR team. The IPTR Report will include: hardware and software architecture descriptions, the TCB definition, subjects and objects, access control mechanisms, a description of documentation reviewed, the degree of completeness of each type or subset of types of documentation, and what still needs to be done, a brief assessment of the product against each of the TCSEC (TNI, TDI) requirements and approved interpretations, technical issues identified, management issues identified, recommendations and a projected evaluation schedule if a transition to evaluation is recommended. This schedule will be the consolidation of the best estimate from the entire IPTR team. The IPTR team leader and the appointed evaluation team leader must document the schedule, have it reviewed by the vendor, and, along with the IPTR report, by NSA management and senior evaluators. The schedule will depict major evaluation milestones and obligations. This schedule will be attached to the Evaluation Agreement to be signed by vendor and NSA at the start of evaluation.

If the team does not feel the product is ready for evaluation, the IPTR report should discuss the type of deficiencies discovered in as much detail as possible and give their best estimate of the effort required for the vendor to fix those deficiencies and provide assurance that others do not exist. It is important to note that the IPTR report, due to resource and time constraints, is not entirely comprehensive. It is the team's best effort at finding issues and should give a good indication whether the vendor has provided the correct level of detail both in their presentations and documentation.The IPTR report should be finished before the team leaves the vendor site and the vendor should be given a copy of the team's report. The team's report should contain a recommendation to NSA management:

o That the vendor proceed to evaluation, or

o That the vendor proceed to evaluation after minor issues are resolved, (and verified as resolved by a small set of evaluators)

o That the vendor be offered additional NSA guidance, or

o That the vendor seek advice from another source, or

o That the product and/or evidence are found severely lacking and that the advice should be terminated.

If, after a second IPTR, the vendor is not prepared to enter evaluation, NSA will terminate the project, and ask the vendor to resubmit a product proposal when the vendor can document substantial progress toward preparation for an evaluation.

The vendor and advice givers must work together following the IPTR to resolve the identified issues. Depending on the severity of the issues, it is likely that the advice givers will perform the second, limited review to ensure

that the deficiencies have been corrected. The evaluation team, after undergoing system training at the vendor site, will review the projected evaluation schedule as it pertains to evaluation activities and will notify NSA management if modification is thought necessary.

In the event that NSA had previously been providing advice to a vendor but at the IPTR recommends that the vendor seek commercial advice, the vendor is responsible for educating the new commercial advice givers. However, the vendor may request that NSA schedule a transition meeting with the new advice givers and NSA advice givers will be obligated to attend at least one meeting for this purpose.

3.9 NSA Decision

The IPTR report recommendations will be reviewed by NSA management and senior evaluators to make the final decision whether or not to proceed to evaluation. A letter containing the results of this decision will be sent to the vendor. If the decision is made to proceed to evaluation, and evaluator resources exist, NSA will assign an evaluation team and the evaluation can begin. If resources are not immediately available, the formation of the team and beginning of the evaluation will be deferred.

4.0 Evaluation

4.1 Evaluation Agreement

This is the legal agreement between the vendor and NSA which outlines the roles and responsibilities of each party in the evaluation. The Evaluation Agreement (EA) incorporates these TPEP Procedures by reference. The Evaluation Agreement will contain an approved configuration as agreed to by NSA and the vendor during Pre-Evaluation activities, a projected schedule of the evaluation as agreed during the IPTR, and assumptions or considerations that are contingencies to the evaluation, signed by both NSA and the vendor. The projected schedule will be referenced throughout the evaluation and will be an important factor in determining progress and appropriate use of resources. Since the schedule is negotiated between the vendor and NSA, each party needs to understand the other's process and prepare the schedule to the level of detail sufficient to make these judgments.

NSA, in an effort to monitor the overall effectiveness of evaluated products in terms of market penetration, will gather and maintain sales information on TPEP evaluated products. On January 1 and July 1 of each year, TPEP vendors will provide to NSA through the Business Relations Branch, sales statistics on their particular evaluated products(s) to include the purchaser's name, quantity purchased, and date purchased. This information is agreed to by NSA and vendors when the TPEP Evaluation Agreement (EA) is executed. The vendor's sales information will be protected as proprietary information and is solely for internal DoD use for the management of the TPEP

and for making future business decisions on what products to accept into the TPEP.

4.2 Roles and Responsibilities

4.2.1 Vendor

The vendor remains obligated throughout the evaluation to assist the team by providing necessary documentation, making changes to that documentation and accomplishing these in the shortest possible time. Vendor corporate and development team personnel must remain committed to the evaluation task to the extent that no other priority distracts from the work the team has to do. Vendors are obligated to name their development team members, Vendor Security Analysts and other involved personnel critical to the evaluation, and to notify NSA of personnel status changes, and in the case of departing personnel, when an equivalent replacement will be assigned.

4.2.2 NSA

NSA and the vendor jointly establish the schedule based on the evaluation factors of system size and complexity, amount of documentation, team size and capabilities, release date of the product and priority factors. NSA will estimate the task, and assign personnel in the appropriate skills to a team, providing the vendor the names of team members. NSA will advise the vendor of changes to the team and provide replacement information as soon as it is available.

4.2.3 Types of Evaluations

NSA performs evaluations on a variety of products in three basic categories: Operating Systems, Networks, and Applications.

Operating Systems - A product is considered an operating system if it addresses all of the requirements of a given class of the TCSEC.

Network and Network Components - A product is evaluated as a network if it meets all of the requirements of the TCSEC and it is configured as a closed system, (i.e., it will not be connected to other networks or network components).

A product is considered a network component if: it meets a subset of the TCSEC requirements as defined in the Trusted Network Interpretation (TNI) (Mandatory Access Control (MAC), Discretionary Access Control (DAC), Identification and Authentication (I&A), and Audit.). A product is also considered a network component if it is expected to be connected with other network components regardless of whether it meets one or all four of the above requirements.

Application Systems - Products that build on an already existing and identified operating system, but provide a separate subset of subjects and objects at a more detailed level of granularity, such as a database management system. Such products are evaluated against the subset of the TCSEC requirements as defined in the Trusted Database Interpretation (TDI).

NOTE: Subsystems, defined as hardware, firmware and/or software which can be added to a computer system to enhance security of the overall system, are evaluated against the Computer Security Subsystem Interpretation (CSSI), and receive a D-Level rating. These evaluations are being curtailed, with new starts commencing only for those products whose proposals demonstrate extraordinary technical features or market superiority.

4.2.4 Team Assignment

When an EA is fully executed, NSA will assign an evaluation team. An evaluation team consists of a Team Leader and team members sufficient to perform the technical analysis. If TPEP resource constraints cause a queue of products awaiting evaluation team assignments, this queue of products will be regularly prioritized depending on DoD and Intelligence Community needs (contracts) and the product's market share.

The vendor may provide a team member (a Vendor Security Analyst) if both NSA and the vendor agree that such a member would be beneficial to the evaluation. This vendor team member should help to provide technical insight into the mechanisms and security philosophy of the product and to provide guidance about the security documentation. The vendor team member will be expected to participate as a full team member and attend all required meetings, training, etc. Occasionally, the vendor team member may be excused from a meeting if the other team members wish to discuss information proprietary to another vendor.

4.2.5 Vendor Product Training

Shortly after team assignment and the creation of Dockmaster accounts and team forums, the vendor should schedule training for evaluation team members. This training typically takes place at the vendor's site and averages 2-3 weeks. Vendors are encouraged to provide preliminary information to the team so they may prepare for training. The length of time required depends upon the complexity and size of the product in evaluation and the number and type of training aids available to the team before training actually begins. The evaluator trainees need to receive a designer/developers view of the product under evaluation.

4.2.6 Design Evaluation (For Products at the C2-B1 Level of Trust)

An analysis of the product design (both hardware and software components of the system), the vendor's design documentation, user documentation, test documentation and Rating Maintenance (RM) documentation is done by the evaluation team. The team analyzes the product's design against each TCSEC requirement by reviewing the design documentation, user documentation, test documentation, and the RM Plan. All test documentation is reviewed to ensure that the appropriate level of testing is performed to meet the targeted level of trust.The time required for review and analysis will depend on the quantity and complexity of the documentation.

The result of the analysis by the team is an Initial Product Assessment Report (IPAR). The IPAR focuses on security aspects of the system, including areas such as Hardware, Software Architecture, Trusted Processes, Security Mechanisms, Assurances and Requirements. Team members individually write sections of the IPAR, then work together to review this document. The team members update this draft and review and update the second draft. The third draft of the IPAR is then distributed to the NSA Project Manager and the TRB. In addition to the IPAR, the evaluation team prepares a test plan.

4.2.7 Initial Product Assessment Report Review

The evaluation team prepares a presentation for the TRB that contains the details of product and protection mechanisms, test coverage, and the testing plans. The TRB judges whether or not the team's analysis is complete and the product is ready to undergo testing.

4.2.8 Implementation evaluation

Following successful completion of the TRB, the team responds to any requirements identified by NSA management based on the TRB and conducts functional tests and a RAMP audit. The tests and audit are conducted at the vendor's site

4.2.9 Technical Review Board (TRB) Testing

In some cases (usually for products at lower levels of trust), this Testing TRB may be combined with the IPAR review. When it is not combined, the team will present a high-level overview of the system at this separate TRB, indicating any changes in the team's understanding of the security architecture since IPAR TRB. The team will also present their Functional Test and Penetration Test Plans and how the plans meet the TCSEC requirements.

4.2.10 Final TRB Review

Upon completion of the implementation evaluation, the team documents the test results and modifies the IPAR into the Final Evaluation Report (FER). The FER will also include a section with high level guidance advising the vendor on the changes necessary to raise the security rating of the product. This FER is then presented to the TRB. The purpose of this TRB is to ensure that the team has performed sufficient analysis and testing to support assignment of the recommended rating and placement of the product on the Evaluated Products List (EPL), and that the FER adequately reflects the product and the evaluation. The evaluation team should discuss the results of testing and close any outstanding issues from earlier during the evaluations.

4.3 Evaluated Products List (EPL) Entries

Products that have successfully completed TPEP evaluation are placed on the Evaluated Products Listing (EPL). The EPL is published as Chapter 4 of the Information Systems Security Products and Services Catalogue. The EPL is updated quarterly and is available through the Government Printing Office. In addition, an electronic copy of the EPL is available on Dockmaster by typing "openair". It is also available to all Dockmaster users via the EPL forum.

NSA evaluates all products on the EPL against established criteria and interpretations. The rating given to a product is the highest class for which that product met or exceeded each of the individual requirements for the general evaluation class. NSA issues a Final Evaluation Report for each product evaluated which is available from the Government Printing Office.

Only the company, product name, targeted level of trust and estimated completion date are listed in the EPL before a product completes the IPAR/Test TRB. After completion of this TRB, a more descriptive, one-page Product Bulletin is published in the EPL. The Product Bulletin includes a brief description of the product, the status of the development of the product, and the status of the evaluation. The vendor is provided the opportunity to review the Product Bulletin before publication. At completion of the evaluation, the EPL entry containing a summary of the evaluated configuration and the TCSEC requirements is then published after the vendor has given approval, in parallel with the Final Evaluation Report.

The general ratings given in the EPL apply only to the specific hardware and software configurations/versions listed. Each product is tested according to the detailed security testing specified in the TCSEC. However, such testing is not sufficient to guarantee the absence of flaws in the product. The EPL entry does not constitute an endorsement of the product by the Government. Neither does it constitute a Department of Defense certification or accreditation of the trusted computer product for use in classified or unclassified processing environments. Rather, the security evaluation provides an essential part of the technical evidence required for follow-on certification and accreditation.

4.4 Termination Process

Continued participation in the TPEP is authorized only if the vendor continues to satisfy the eligibility requirements and the conditions set forth in the Evaluation Agreement and its attachments. Since evaluator resources represent a significant cost to the Government, any delay in the evaluation schedule will be immediately scrutinized by NSA and termination efforts may be initiated. Examples of such delays are:

o any 30-day vendor delay

o Vendor inactivity (i.e., vendor budget constraints preclude attention to this effort for an extended or unreasonable period of time)

o The product changes from originally approved configuration (i.e., approved configurations must remain frozen from the date of the Evaluation Agreement)

o Market loss and/or change of product market (i.e., proposed product was accepted for a TPEP evaluation based on its potential for winning a contract award but the contract was not awarded to that vendor)

o Vendor refusal to participate in RAMP or meet RAMP requirements as the evaluation proceeds, i.e., configuration management, RAMP audit etc., or refusal to execute RAMP activities after enhancements or changes have been made to the product

o Vendor knowingly misrepresenting any aspect of the product or its RAMP process

o Vendor voluntarily terminates participation in the program

o Product, as designed, fails to meet the TCSEC design requirements

4.4.1 Termination Procedures

NSA will notify the vendor by certified letter that NSA is considering termination of the TPEP evaluation. The letter will contain the details or reasons why termination is being considered, and ask the vendor to show cause for continuation of the evaluation.

The vendor will have 15 working days from the receipt of the letter to respond to the proposed termination. Extensions of up to 30 days to allow the vendor to respond may be granted by NSA management upon a showing of good cause; however, granting of an extension is discretionary. Vendor responses should be mailed to the following address:

Trusted Product Evaluation Program
National Security Agency
9800 Savage Road Suite 6740
Ft. George G. Meade, MD 20755-6740

Within 10 days of receipt of vendor reclama information, NSA will render a decision on the termination proposal and notify the vendor's Responsible Corporate Officer (RCO) by telephone. This action will be followed up with a certified letter detailing the grounds for NSA's decision.

The vendor may appeal the termination decision by sending further arguments or reclama information to NSA by certified letter within 10 days after receipt of the termination decision from NSA.

A Final Termination Decision will be rendered by the NSA management chain above the TPEP management level within 7 days of receipt of the vendor's appeal.

NSA will notify the vendor of the final decision by telephone to the vendor's Responsible Corporate Officer and follow-up with a certified letter detailing the reasons for NSA's final decision. The vendor should note that NSA reserves the right to publish a Final Evaluation Report (FER) on the vendor's product, noting the results determined to date and stating failure to complete the evaluation.

5.0 Post Evaluation - Rating Maintenance Phase (RAMP)

5.1 Rationale/Background

When a vendor releases a new version of a product that had previously received an EPL rating, the new version does not carry the original EPL rating, and it is not an evaluated product. Because of the continuing technological evolution of software with frequent new releases and limited evaluation resources, full evaluation of each release is impractical. RAMP was established to provide a mechanism to extend the original rating to a new version of an evaluated computer product. RAMP seeks to reduce evaluation time and effort required to maintain a rating by using the personnel involved in the maintenance and continual development of the product to manage the change process and perform security analysis. Thus, the burden of proof for RAMP effort lies with those responsible for system maintenance (i.e., the vendor) instead of with an evaluation team.

Preparation for RAMP begins during Evaluation. A Vendor Security Analyst (VSA) is invited to join the team to help provide technical insight into the mechanisms and security philosophy of the product and to provide direction into reading the security documentation. The Ratings Maintenance Plan is developed during Evaluation, and configuration management of the hardware, software, and documentation also is initiated. RAMP is an integral part of the TPEP because it supports the end user's desire for timely evaluations and provides for the availability of current product versions on the EPL.

During RAMP, all changes to the vendor's system must be managed by the vendor. For each RAMP cycle, the vendor must be able to identify all changes to the system that occur in the new release, and perform security analysis of those changes. The procedures the vendor follows to manage changes to the system are described in the Rating Maintenance Plan (RM Plan). This document is written by the vendor and is approved by NSA during the original evaluation. The RM Plan describes how the vendor will meet the RAMP requirements and describes the system to which the plan applies.

5.2 Personnel

During the original evaluation, the vendor identifies the vendor personnel who are responsible for the security of the system. These personnel will attend an NSA Vendor Security Analyst (VSA) training class to learn basic security fundamentals and the RAMP procedures. The VSA is responsible for understanding the design details of the evaluated product and how the security requirements map to that particular product.

The vendor's Responsible Corporate Officer (RCO) who has signed the Evaluation Agreement is responsible for ensuring that the procedures outlined in the RM-Plan are being followed. The VSA's are responsible for reviewing the security analysis of all changes that are made to the system, and for determining that the originally evaluated security features and assurances of the system are upheld. The VSA may consult with an NSA assigned Technical Point of Contact (TPOC) to assist with any technical questions regarding the application of the TCSEC requirements.

During the course of the evaluation, the vendor may need to identify new VSA's or RCO's because of personnel changes. The vendor must notify NSA whenever such changes occur. Assignment of a new VSA may increase some risk to the successful completion of the evaluation if the VSA is unable to attend a VSA training class during an appropriate time frame.

5.3 RAMP Evidence/TRB

RAMP evidence will be recorded for every change of the original product, detailing the security analysis of the change. This information is used when a RAMP audit is performed by either NSA or the vendor, and is used as

the basis for a Rating Maintenance Report (RMR). An RMR is a document that is submitted to NSA for every system release that is to be evaluated. It summarizes all the changes since the last evaluated release, and describes why the security features and assurances are upheld. The RMR is ultimately presented to the TRB for a technical and consistency check prior to receiving a new EPL rating. Based on the TRB's recommendation, NSA decides whether or not to extend the rating to the new version.

5.4 Applicability of RAMP

RAMP applies to all products that have been evaluated against the TCSEC, the TNI, and the TDI. However, the Rating Maintenance Phase always builds upon a product evaluation; it provides no opportunity to avoid an evaluation. RAMP applies at all levels of the criteria, from C2 through A1.

RAMP is limited to extending the same rating that was originally received through evaluation. It does not allow new ratings, either higher or lower.

RAMP applies to the same vendor that originally received the rating. If an evaluated product becomes the property of a new vendor, RAMP must be negotiated with NSA. RAMP assumes that the vendor has gone through an evaluation and thus, by experience, understands the evaluation process, and the types of technical questions that should be asked when performing a technical analysis.

The types of changes that may be performed under RAMP are not limited, but will vary depending on the system and level of trust. At the lower levels of trust the vendor may consult with the TRB for this judgment. NSA reserves the right to transfer it into a pre-evaluation if the technical changes are so vast as to require a new evaluation.

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

5.5 RAMP Process

A product formally begins RAMP when the original EPL entry is published. Considerable planning takes place prior to this point (during the actual evaluation), and all of the procedures and activities that will take place during RAMP must be in place prior to the team's testing of the Trusted Computing Base (TCB) during the evaluation phase.

RAMP planning involves the generation and subsequent NSA approval of the RM- Plan, as well as a demonstration via the RAMP audit that the policies and procedures for the RAMP as described in the plan are in place. The RAMP audit also demonstrates that security analysis of changes is being carried out correctly by the VSA's. The approved RM Plan must be in place, and the audit must be conducted prior to commencement of testing.

5.5.1 Technical Point of Contact (TPOC) Duties

A Technical Point of Contact (TPOC) is an evaluator, assigned by NSA, who serves as a consultant to a vendor while the vendor is in the Rating Maintenance Phase (RAMP) of TPEP. The TPOC is the interface between the vendor and NSA, and reports to an NSA manager who is responsible for the RAMP activity associated with the product. The TPOC is assigned by NSA during the Evaluation Phase, and is a member of the Evaluation Phase Team. NSA may assign more than one TPOC for a product.

5.5.2 TPOC Requirements

The TPOC shall provide technical guidance concerning satisfying the TCSEC requirements for the product under the TPEP RAMP. The TPOC shall represent the vendor point of view in technical discussions that involve the evaluation community.

The TPOC shall provide quarterly status reports to the vendor evaluation forum by the fifth working day of the month during the months of January, April, July, and October.

The TPOC shall examine all Rating Maintenance Plan (RM Plan) revisions while the vendor is participating in the RAMP and shall recommend to NSA whether to accept or reject the revisions.

The TPOC, together with the Vendor Security Analyst (VSA), shall conduct at least one RAMP Audit for each RAMP cycle. The results of the audit shall be included in the next Quarterly Status Report (QSR) following the RAMP audit.

The TPOC, in cooperation with NSA management, shall be responsible for scheduling RAMP TRB meetings.

The TPOC shall review the updated FER and shall write a statement addressing its quality and accuracy, and provide NSA management a copy of this statement.

At least four weeks prior to the scheduled RAMP TRB, the TPOC shall provide NSA, and post to the vendor forum, a written report that describes the vendor's RAMP activity, the activity of the TPOC during the RAMP cycle, and the results of the RAMP audit. This report should also contain the TPOCs statement of quality and accuracy of the updated FER noted above.

The TPOC shall direct the vendor where to send the following materials, and the number of copies necessary for TRB members and management:

-Rating Maintenance Report (RMR)

-Approved Rating Maintenance Plan (RM Plan)

-Updated FER

-Proposed product description for the EPL entry

The TPOC shall ensure that the update to the FER has been completed

The TPOC shall be responsible for any updates to the Evaluator's Comments section of the updated FER.

Appendix A: Policy for Handling Vendor Proprietary Information

Introduction

NSA appreciates the value of the vendor proprietary information entrusted to its care, and is committed to affording all reasonable and prudent protection for safekeeping this information. Both the vendor and NSA share the responsibility for identifying what is proprietary so this objective can be met.

Definition of Proprietary

Proprietary information is information owned and held as "company confidential" by the vendor, the unauthorized release or disclosure of which could potentially cause financial damage to the vendor. It may be technological or market oriented. Information that is publicly available in open literature cannot be claimed as proprietary by the vendor with expectations that special protection will be afforded by NSA.

Marking Proprietary Information

All proprietary information received by NSA from a vendor must be marked as Proprietary or PROPIN. This information may be received in hard copy or electronic form and shall be appropriately marked and protected in whatever form the information is received. NOTE: NSA evaluation teams may develop new documents that are based on proprietary information or that contain proprietary information. These documents will be marked "For Official Use Only - Contains Proprietary Information."

Vendor Responsibilities

Vendors must mark all documents that are considered proprietary. If the information is obtainable in open source literature, the vendor should not mark similar information as proprietary or expect protective measures to be taken by NSA evaluators. Information that has a definable life should be labeled with a clear expiration date when the disclosure would no longer be harmful. Vendors are also responsible for the review of NSA documents (for example, the Final Evaluation Report (FER)) prior to publication to certify that proprietary information is not contained in the release or disclosure. Prior to approval for publication, NSA will provide a copy of the report to the vendor for this purpose. A one-two week response time from the vendor is necessary to preclude hindrance to publication.

NSA Responsibilities

Recipients of proprietary information will safeguard it from disclosure. In the workplace, the material will be protected from review by storing it in a lockable container or cabinet. Persons extracting information from proprietary documents must insure that the generated document is marked to protect the proprietary information.

Protection of Vendor Proprietary Information

Proprietary information in electronic form must be protected while it is being processed, stored, or transmitted. This is accomplished by the prudent use of access control measures to deny unauthorized access. These measures are a combination of physical, procedural, and computer security access controls.

Non-Disclosure Agreements: All evaluators are required to sign non-disclosure agreements to confirm their knowledge and understanding of the need to protect proprietary information.

Internal -NSA evaluators are covered by the non-disclosure clauses that appear in the Evaluation Agreement (EA) between NSA and the vendor. As a reminder, all NSA evaluators are required to sign a statement of personal responsibility annually. No additional non-disclosure agreement is necessary.

External - Evaluators at the MITRE Corporation or at the Aerospace Corporation are covered by the non-disclosure clauses that appear in the contract between MITRE and the Army and between Aerospace and the Air Force. No additional non-disclosure agreement is necessary.

All other evaluators, including those from the Mitretek, The Institute for Defense Analysis (IDA), the U.S. Armed Forces, or any independent consultant must sign a non-disclosure agreement that confirms that the evaluator understands and agrees to the non-disclosure policy of NSA and TPEP.

Release of Proprietary Information

Internal - Within NSA, it may be in NSA's best interest to share proprietary information with other organizations or individuals. Whenever such information is requested, TPEP management will determine if sharing the information is authorized. TPEP management is also responsible for coordinating release of information with the vendor. Persons presenting briefings containing proprietary information must insure that the audience has a valid request for the information and understands the responsibility for protecting this information from unauthorized

disclosure. Appropriate non-disclosure agreements must be signed by the audience of a briefing or the recipient of a document, or else they will not be given access to the proprietary information.

External - All external NSA requests for release of proprietary information shall be made in writing and coordinated with the vendor who ultimately owns the information. NSA will notify the vendor in writing who is requesting the release, what specific information is being requested, the purpose of the release, and the time frame requested to release the information. The vendor will make the ultimate decision whether they are willing to share their proprietary information with the requestor and will send their decision rationale to NSA. NSA will then reply to the requestor with the vendor's decision. If there is a case where the information is needed quickly and no time is available to coordinate the release in writing via the postal system, a FAX is suggested as expeditious written approval.

Freedom of Information Act (FOIA) Request - In the event that NSA receives a FOIA request regarding a vendor's proprietary information, the cognizant NSA policy office will review the information on a line-by-line basis to determine if the information should be exempted from release based on the trade secrets and confidential commercial information exemption (5 U.S.C.A. 552(b) (4)) of the FOIA. The vendor's proprietary markings would be used as guidance, but is not the final disposition authority. NSA will provide the vendor with a copy of the information that it intended to release under the FOIA and the intended date of release. The vendor will then have an opportunity to provide comments or pursue legal avenues to prevent release if they disagree with NSA's determination of the information in question.

Termination of Obligation for Protecting Vendor Proprietary Information

Proprietary information will be protected through its declared life as defined by the vendor. Proprietary information that has no defined life will continue to be protected unless it is returned to the vendor or destroyed.

Appendix B: The Technical Review Board

The Technical Review Board (TRB) was established as a technical advisory panel to the Chief of the Trusted Product and Network Security Evaluations Division. One of the primary concerns of the TPEP is to ensure quality, uniformity and consistency across evaluations from both a technical and procedural point of view. The main purpose of the TRB is to assist NSA management in reaching this goal.

The TRB is comprised of the most senior computer security practitioners of the TPEP community. Although they are usually TPEP evaluators, they may be members of academia, other NSA organizations, or members of the Federal community who have displayed a thorough technical understanding of TPEP evaluations and have no explicit conflict of interest with TPEP vendors.

TRB members are charged with assuring that evaluation team members understand the product they are evaluating and if the documentation satisfies the Criteria. The TRB is also charged with assuring the integrity of the evaluation through quality control and consistency checks during their meeting to review the evaluation. At the IPAR and Test TRB's, the board examines the team's work and assessment conclusions and hears how the team will prove the system by the tests derived by both the vendor and the evaluation teams. At the Final TRB, the board hears the results of testing and any final details of the evaluation to gain assurance that it was properly executed to the equivalence of other products listed on the Evaluated Products List. Types of TRBs are:

IPAR TRB - An IPAR TRB is held at the conclusion of the design evaluation. The purpose of this TRB is to ensure that the team has performed sufficient analysis of the product design to determine that the design supports the candidate rating. This TRB also judges the team and product readiness and for formal evaluation and makes recommendations to NSA management accordingly.

TEST TRB - The purpose of the TEST TRB is to ensure that the team is prepared to perform thorough product testing and to ensure that product implementation analysis has been adequately performed. The evaluation team

is also responsible for addressing the specific changes made to the report and all outstanding issues from the IPAR TRB.

IPAR/TEST TRB - A combined IPAR/Test TRB is a requirement under the new TPEP process for products aiming for a B1 or below level of trust. The combined IPAR/Test replaces the separate TRBs.

FINAL TRB - The purpose of this TRB is to ensure that the team has performed sufficient analysis and testing to support assignment of the recommended rating and placement of the product on the Evaluated Products List (EPL), and that the FER adequately reflects the product and the evaluation. Again, the team is responsible for addressing specific changes made to the report and all evaluation issues that have been cleared since Testing TRB.

The NSA-assigned Technical Point of Contact (TPOC) must be involved in this decision. No documentation is required for this TRB, but an agenda is necessary so that the TRB members may review the changes. The vendor presents the types of changes to be made during the RAMP cycle along with a preliminary security analysis of the proposed changes. The purpose of this TRB is to recommend the composition of the Security Analysis Team and the method of presentation to the RAMP TRB.

RAMP TRB - The required documentation for the RAMP TRB includes the NSA approved RM Plan, the vendor's Rating Maintenance Report (RMR), an updated FER, and a draft RAMP EPL entry.

The vendor presents the changes to the product and the reasons why those changes do not affect the product's rating. The purpose of the RAMP TRB is to ensure that the evaluation Criteria is interpreted correctly by each Vendor Security Analyst (VSA); to ensure that the vendor's RM Plan has adequate configuration management and supportive evidence to sufficiently maintain a product's rating; and to ensure that the vendor's conclusions are supportable from the evidence presented.

Commercial Product Evaluations | TPEP Main Page | TTAP Main Page]

Last updated Wed Nov 25 08:51:41 1998
URL: http://www.radium.ncsc.mil/tpep/process/procedures.html
Questions/Comments