Development Process

For

US Government Protection Profiles (PP)

National
Information
Assurance
Partnership

Version 3.0

1 March 2004

Protection Profile Development Process

Section 1: Introduction

In accordance with their respective responsibilities under Public Law 100-235 (Computer Security Act of 1987), the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have agreed to cooperate on the development of security requirements for key technology areas necessary for the protection of Federal information systems and networks, including those comprising the critical infrastructure within the United States. The principles that guide the NIST-NSA development effort are contained in Attachment A. Whenever possible, security requirements will be expressed as protection profiles using ISO/IEC Standard 15408, or Common Criteria. Hereafter, the terms *security requirements* and *protection profile* will be considered equivalent.

NIST and NSA are undertaking this effort:

- To ensure the U.S. Government has a consistent comprehensive set of recommended protection profiles for key technology areas;
- To forge partnerships with public and private sector constituencies to develop and gain consensus on PPs important for critical infrastructure protection; and
- To facilitate national and international convergence of protection profiles in key technology areas.

This document describes the process that will be followed by NIST and NSA for the development and maintenance of protection profiles within each technology area to include the modification of existing requirements, transition to new requirements, and elimination of older requirements. The components of this process are described below.

Section 2: Protection Profile Life Cycle

Technology Area Development List (TADL)

The Technology Area Development List (TADL) is a prioritized list of protection profiles that NIST and NSA developed or plan on developing, subject to resource constraints. Table 1 below represents the top ten key technology areas and provides information related to validated and in process protection profiles. Additional information about any of the key technologies or Protection Profiles can be obtained via email to the Technology Area Leader (TAL).. The hierarchical relationship among protection profiles within a particular technology area is represented by increasing levels of robustness (i.e., strength of functions and assurances) based on threat assumptions and associated security objectives. Products successfully evaluated and validated against a protection profile in a particular technology area family would by definition, be in compliance with any lower level profiles in that same family.

Table 1

Top Ten Technology Areas Development List and Recommended Protection Profiles List								
Technology	TAL	Robustness	Links to NIAP validated PP	PP in development	Status of Profiles in Development			
					Development	Review	Address Comments	NIAP Eval. Process
Operating Systems	Hugo Badillo habadil@missi.ncsc.mil	Basic	Controlled Access PP (Basic Robustness/C2), Version 1.d Dated Oct. 99					
		Basic	Labeled Security PP (Medium Robustness/B1) Version. I.b Dated Oct. 99					
		Basic		Operating System	√			
		Medium	Multi-Level Operating Systems in Medium Robustness Environments PP Version 1.22 Dated Jun. 01					
		Medium	Single-Level Operating Systems in Medium Robustness Environments PP Version 1.22 Dated Jun. 01					
		High		Separation Kernel	√			
Database Systems	Hugo Badillo habadil@missi.ncsc.mil	Basic		DBMS on IATF web site	√			
Firewalls	Mark Roberts mcrober@missi.ncsc.mil	Basic	Application-Level Firewall for Basic Robustness Environments PP Version 1.0 Dated Jan. 00.					
		Basic	Traffic Filter Firewall PP for Low Risk Environments PP Version 1.1 Dated Apr. 99					
		Medium	Application-Level Firewall for Medium Robustness Environments PP Version 1.0 Dated Jun. 00					
		Medium	Traffic Filter Firewall PP for Medium Robustness Environments Version 1.4 Dated Jun. 00					
		Medium	U.S. Government Firewall Protection Profile for Medium Robustness Environments Version 1.0 Dated Oct. 00					
Token	Dave Rhude dlrhude@missi.ncsc.mil	Medium	Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP					
Biometric Devices	Dave Rhude dlrhude@missi.ncsc.mil	Medium	U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (MRE)					
Web	Quanna Bluford qjblufo@missi.ncsc.mil	Basic		U.S. Government Web Server Protection Profile			√	
		Basic		U.S. Government Web Browser Protection Profile	√			

Top Ten Technology Areas Development List and Recommended Protection Profiles List								
Technology	TAL	Robustness	Links to NIAP validated PP	PP in development	Status of Profiles in Development			
					Development	Review	Address Comments	NIAP Eval. Process
Intrusion Detection	Mark Roberts mcrober@missi.ncsc.mil	Basic	Intrusion Detection System (Analyzer) PP Version 1.1 Dated Jun. 02					
		Basic	Intrusion Detection System (Sensor) PP Version 1.1 Dated Jun. 02					
		Basic	Intrusion Detection System (Scanner) PP Version 1.1 Dated Jun. 02					
		Basic	Intrusion Detection System (System) PP Version 1.1 Dated Jun. 02					
		Medium		Intrusion Detection System (Analyzer) PP	√			
		Medium		Intrusion Detection System (Sensor) PP	√			
		Medium		Intrusion Detection System (Scanner) PP	√			
		Medium		Intrusion Detection System (System) PP	√			
PKI	Paul Perry Pjperr1@missi.ncsc.mil		Certificate-Issuing and Management Components Family, Security Level 1 PP Version 1.0 Dated Oct. 01					
			Certificate-Issuing and Management Components Family, Security Level 2 PP Version 1.0 Dated Oct. 01					
			Certificate-Issuing and Management Components Family, Security Level 3 PP Version 1.0 Dated Oct. 01					
			Certificate-Issuing and Management Components Family, Security Level 4 PP Version 1.0 Dated Oct. 01					
VPN	Mark Roberts mcrober@missi.ncsc.mil	Medium		U.S. Government Virtual Private Network (VPN) Boundary Gateway Protection Profile	√			
				U.S. Government Firewall with Virtual Private Network (VPN) Boundary Gateway Protection Profile	√			
Wireless	Tim Havighurst tjhavig@missi.ncsc.mil	Medium		Wireless email (desktop)	√			
		Medium		Wireless email (Handheld)	√			
		Medium		Wireless email (Network)	√			
		Medium		PDA App: A- GSM/GPRS with internet	√			
		Medium		PDA App: B- GMS/GPRS with email	√			
		Medium		PDA App: C- GSM with Voice	√			
		Medium		PDA App: D- Synchronization	√			
		Medium		Bluetooth-enabled Electronic Device	√			

Top Ten Technology Areas Development List and Recommended Protection Profiles List								
Technology	TAL	Robustness	Links to NIAP validated PP	PP in development	Status of Profiles in Development			
					Development	Review	Address Comments	NIAP Eval. Process
	Anna Entrichel zaentri@missi.ncsc.mil	Basic		US Government Wireless Local Area Network (WLAN) Access System Protection Profile				√
		Basic		US Government Wireless Local Area Network (WLAN) Client Protection Profile				√

Technology Area Leader (TAL)

For each technology area selected for development from the TADL, a Technology Area Leader (TAL) will be appointed who is responsible for managing the development of the protection profiles specified in that particular technology area, including development and implementation of the TA Plan. The TAL will be given the resources necessary to complete the development effort and is responsible for all phases of the family's development, including maintenance. Table 1 above list the TAL associated with their technology area.

Technology Area Development Consistency

NSA and NIST have produced a number of Common Criteria Protection Profiles in response to requests for procurement guidance on IA technologies. In the Department of Defense this work is being performed to support new DoD IA system policies (i.e., DoDD 8500.1 and DoDI 8500.2). In the National Security Community, this work is being performed to support the NIST FISMA (Federal Information Security Management Act) Implementation Project and the development of NIST SP 800-37. In November 2001, NSA and the National Institute of Standards and Technology agreed to work together to create a joint set of profiles that would represent the two organizations' collective interests.

With many profiles being developed by numerous organizations within NIST and NSA, it has become apparent that in order for the organizations to lead in this area, IA Protection Profile efforts need to be closely coordinated to facilitate representing a consistent strategic view to our customer base. Such consistency is important to create and maintain our customer's confidence in our products and guidance.

To this end, a corporate PP consistency-working group, called the PP Review Board (PPRB), has been formed to review all proposed PPs and work with the PP authors to offer comments to make them as consistent as possible. The first activity of this group was to review a number of Protection Profiles and offer comments to the authors on areas that should be addressed to improve consistency. In the context of this first reviews, a number of consistent items have been captured and recorded in a document referred to as the Consistency Manual. There is a consistency manual for each level of robustness (Basic and Medium, High to be developed) that will offer PP authors guidance on how to make U.S. Government PPs more consistent.

The document presents instructions for a PP author. The instructions are presented for all PP authors to consider and either **include** the recommendation in their PP **or justify** why the

recommendation does not apply to the profile. This methodology will ensure that all PP authors address the minimal security considerations or perform an analysis as to why they are not addressed. Each instruction is self-contained and offers either text for specific sections of a PP or specific common criteria functional/security requirements so that all PP are consistent in addressing minimum-security concerns for all Robustness PP.

It should be noted that the final authority for the content of the PP is the PP owner. However, the profile must be consistent with other profiles of the same robustness thus the author should review other profile at the same robustness level. The author should also ensure that the functional requirements are consistent with the technology and may want to consult with other experts in the technology area.

As PP reviews continue, the guidance will be updated to offer new instructions as they become available.

Recommended Protection Profile List (RPPL)

The Recommended Protection Profile List (RPPL) contains a list of protection profiles in development and profiles that have been completed and evaluated/validated. When a technology area family is selected from the TADL for development, a notation is made in the RPPL to inform the public and private sectors that the developmental activity has been initiated.

Once the family of protection profiles has been completed and evaluated/validated, the status on the RPPL will be changed to reflect this. When completed, the family represents a NIST and NSA recommended set of requirements for that particular technology area. It is a statement by NIST and NSA that the set of requirements provide acceptable protection for the respective, designated threat environments. When federal agencies are involved in system development, integration or modification, NIST and NSA strongly encourage the agencies to select technology area products for use in their systems (based upon threat environments) that have been evaluated/validated against the Common Criteria protection profiles contained in the RPPL.

It is possible that product developers in a particular technology area will have to modify their offerings to meet a newly adopted family of protection profiles in that technology area (i.e., when a completed technology area family is placed on the RPPL). To facilitate transition to the newly developed technology area family, it is suggested that developers monitor the TADL and the RPPL on a regular basis:

- To determine if their technology area is being considered for protection profile development;
- To determine if development efforts in their technology area have been initiated;
- To monitor the progress of protection profile development in their technology area; and
- To obtain the final version of the technology area family of protection profiles.

When a technology area family of protection profiles is first placed on the RPPL, government agencies are encouraged to reference the protection profiles in their acquisition documents and will be expected to acquire products that fully conform to the profiles (as demonstrated by a Common Criteria certificate). However, it is recognized that there may be a lag time before developers in a technology area can demonstrate full conformance to a newly introduced protection profile in their technology area since conformance may require modifications to their product and subsequent evaluation/re-evaluation. In addition, some developers may already have a valid Common Criteria certificate for an evaluation performed against their own security target

or against an existing protection profile in that technology area. Until developers have had a chance to transition to the newly introduced protection profiles, the following guidance is provided to government consumers and to product developers:

- Government agencies should select evaluated/validated products that come closest to meeting the newly introduced protection profiles and to meeting their system specific requirements. In making this decision, they should rely on an independent assessment, conducted by an accredited Common Criteria Testing Laboratory, of the extent to which a particular product conforms to a newly introduced protection profile;
- Developers with evaluated/validated products that wish to demonstrate the extent to which they conform to a newly introduced protection profile, should contract with an accredited Common Criteria Testing Laboratory to perform an assessment that documents the extent to which the developer's ST conforms to a newly introduced PP.

Protection Profile Maintenance

Once developed and placed on the RPPL, a technology area family should be reviewed periodically to determine if the family of requirements (i.e., protection profiles) is still acceptable in the face of rapidly changing technology, increasing threat levels, and other conditions. On the other hand, since developers will have made a significant investment in meeting the requirements and in undergoing evaluations to demonstrate conformance to the requirements, they would like stability in the requirements to maximize their return on investment. NIST and NSA recognize the balance that must be reached between the need for modifying or sun setting requirements sets and maximizing the return on investment made by developers. Consequently, each technology area family must include plans for periodic review, modification, and sun setting of requirements. However, the following rules will apply to modification or sun setting of protection profiles.

(1) Modification and sun setting decisions for protection profiles will be made and vetted whenever possible, in an open, public process in full partnership with industry, consortia, and standards groups to ensure maximum acceptance and usability;

(2) When modifications to a technology area family of protection profiles are completed, developers will be given an 18-month transition period to demonstrate conformance to the new or modified protection profiles;

(3) Products that comply with previous versions of protection profiles will be accepted as equivalent or comparable to the new profiles during the 18-month transition period.

National and International Convergence of Protection Profiles

Through the Common Criteria Recognition Agreement (CCRA) Executive Subcommittee awareness of national and international protection profile development efforts by other government and private sector organizations, (e.g., Federal agencies, Common Criteria Recognition Arrangement participants, industry, consortia, NATO, European Union, national bodies) will be maintained. In that regard, the members of the Executive committee are in the best position to recognize opportunities for national and international convergence of protection profiles. Whenever possible, the members should make TALs aware of related protection profile development efforts in their respective technology areas and encourage the TALs to consider the suitability of these profiles for adoption or adaptation prior to initiating new/different development efforts for the same technology area. It is also the responsibility of each TAL to

search for related protection profile efforts and consider the suitability of the resulting profiles for adoption or adaptation prior to initiating their development efforts.

The CCRA Executive Subcommittee country representative will be proactive in attempting to foster partnerships between the US government's protection profile development efforts and those development efforts of other government and private sector organizations for the purpose of achieving acceptance and convergence of profiles in key technology areas. In particular, country representative to the CCRA Executive Subcommittee will work through the Common Criteria Management Committee and Executive Subcommittee or directly with the Common Criteria Recognition Arrangement participants to coordinate protection profile developments in order to avoid proliferation of competing profiles within a technology area.

Critical Infrastructure Protection (CIP)-related Sector Development of Security Requirements

NIST and NSA, through the National Information Assurance Partnership (NIAP), will encourage communities-of-interest within CIP-related sectors (including government (e.g., DOD, DHS) and private sector organizations (e.g., bank, medical) to develop and converge on security requirements for their respective constituencies. When resources are available, NIAP may host these community-based profile development activities, provide limited administrative assistance, and provide limited technical support or guidance on use of the Common Criteria and the NIAP evaluation/validation scheme. However, communities-of-interest are expected to take ownership of the development activities, including providing leadership, funding/resources, and technical expertise. NIST and NSA recommend that the communities-of-interest adopt and enforce the requirements through their respective acquisition processes and use Common Criteria Testing Laboratories to validate conformance to their requirements. In addition, use of NIAP evaluated and validated protection profile may assist many organizations conform to and meet the requirements of the Federal Information Security Management Act (FISMA).

Attachment A

Protection Profile Development Principles

- Security requirements will be expressed, whenever possible, using international standard ISO/IEC 15408 (Common Criteria) and be delivered in the form of protection profiles.
- Protection profiles will be targeted at high impact areas within the critical infrastructure with broad constituency support to ensure adequate participation by industry.
- Protection profiles will be developed in key technology areas, (e.g., operating systems, database systems, firewalls, tokens, biometrics devices, public key infrastructure components, virtual private networks) and will employ a variety of security features and assurances according to projected environments of use.
- Security requirements within the same technology area, (e.g., operating systems) will be characterized, whenever possible, by a family of protection profiles, hierarchically-related to promote comparability for consumers and cost-effective testing and evaluation for industry.
- Protection profiles will be developed and vetted, whenever possible, in an open, public process in full partnership with industry, consortia, and standards groups to ensure maximum acceptance and usability.
- Protection profiles recommended for U.S. Government use will be evaluated by independent, private sector, Common Criteria Testing Laboratories and validated by the National Information Assurance Partnership (NIAP) or equivalent organizations
- Protection profiles will be managed in a life cycle process with adequate transition time between versions, (i.e., new releases), to balance advances in technology against a desire for stability of requirements and to protect previous investments in product and system security evaluations.
- Federal agencies will be encouraged to use protection profiles recommended by NIST and NSA for their respective constituencies (based upon respective authorities) according to the security and assurance needs of the organization or specific policies currently in effect.
- Protection profiles recommended by NIST and NSA will be promoted to the national and international standards communities to facilitate consensus building on security requirements for critical infrastructure protection-related applications.

Attachment B

Life Cycle Process for Developing and Maintaining Families of Protection Profiles

Protection Profile Development

Phase I – ***Development Preparation:***

For each technology area in the TADL, the TAL will coordinate a development activity within the TAL's organization. Suggested activities:

(1) Scope of the protection profile family development effort, including considerations such as the specific threat environments to be addressed, the boundary of the technology area under consideration, and the assumed interfaces and environmental controls outside the stated boundary;

(2) Recommendations on prospective participants in the protection profile development process to facilitate adoption/acceptance, including public and private sector constituencies both nationally and internationally;

(3) A milestone chart establishing the family's development tasks, with emphasis on achieving rapid convergence on requirements;

(4) A resource allocation plan describing how resources will be spent for the development effort;

(5) Recommendations on initial prototype protection profiles, if any, to be used as starting points in the development process;

(6) Schedule of working group meetings, public workshops, or other forums proposed to achieve rapid convergence on the family of protection profiles;

(7) Schedule for public review and vetting of draft protection profiles by government, industry, academe, and international Common Criteria Recognition Arrangement partners.

(8) Schedule for periodic review, modification, and sun setting of protection profiles.

Phase II – ***Development of Initial Drafts of Protection Profiles and Review of Draft Protection Profiles by the PPRB:*** Within **60-180 days** after approval to prepare the Protection Profile.

- The variation in time to complete this task depends on the complexity of the protection profile and technology area and the availability of candidate protection profiles from other sources.

- PPRB works with TAL to ensure draft protection profiles comply with the stated development principles and meet consistency standards established in the consistency Manual.
- PPRB makes recommendations to the TAL regarding acceptability of proposed protection profiles for public review.

Phase III –***Public Comment Period for Draft Protection Profiles:*** Within **15 days** after initial drafts of protection profiles are completed.

- Public comment period shall be 30-60 days depending on complexity and interest in the profile.
- Protection profiles shall be posted on the NIAP web site and other government web sites as appropriate at the discretion of the TAL.
- Specific feedback on draft protection profiles shall be obtained from a representative cross section of consumers and producers of the information technology products and systems addressed by the family of profiles.
- At the discretion of the TAL, subject experts may be asked to review the profile to ensure that all appropriate assurance aspects are addressed.
- At the discretion of the TAL, an IATF Forum may be held to introduce and discuss the profile and convene a workshop if appropriate.

Phase IV – *Revision of Draft Protection Profiles Based on Public Comments:* Within **30 days** after completion of public comment period.

- At the discretion of the TAL, depending on the number and complexity of the comments and the resultant changes made to the PP, an additional comment period may be scheduled.

Phase V – *Evaluation and Validation of Protection Profiles:* Within **90-120 days** after submission of protection profiles to a NIAP lab.

Phase VI – *Publication of Protection Profiles:* Immediately upon completion of evaluation and validation of protection profiles and issuance of Common Criteria certificates.

- Update RPPL on the NIAP web site.
- Publish the validated Profile on the NIAP and IAF web sites
- Prepare public announcements, as appropriate.