Technical Communities: A Collaborative Approach for Protection Profile Development

Version 1.0

December 2011

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

NIAP is evolving the process for evaluation of commercial products. The objectives are to define a new evaluation process that is less subjective, can be completed in a more timely fashion with consistently repeatable results, and that produces outcomes with increased relevance and value to the operational user community. The current evaluation process is being analyzed to determine how it can best be streamlined and restructured to achieve these objectives and result in a more timely transition of products through evaluation and onto the NIAP Product Compliant List (PCL). As part of this effort, NIAP, with the help of the vendor community, is developing new Protection Profiles (PPs) that enable value-added improvements in the overall evaluation process.

The new PPs are focused on defining *technology-specific* threats and objectives and outlining the core minimum set of security functional requirements (SFRs) for the technology. The PPs will also establish a set of basic Security Assurance Requirements (SARs) and assurance activities for technology-specific documentation and testing to enable increased consistency among evaluations.

Development of new PPs is being conducted through a partnership between Industry, Government (and their representatives), Common Criteria Testing Labs (CCTL), and other international Common Criteria (CC) Schemes. The new PPs will embrace various technology areas. Each PP will be created by an interdisciplinary group, referred to as a Technical Community, comprised of individuals with the core competencies appropriate for the PP.

This white paper outlines initial efforts focused on the organizational aspects of building a vibrant and collaborative set of Technical Communities to develop PPs that support NIAP's goals.

The Technical Community Concept

Technical Communities represent a potential way forward for greater collaboration and partnership between Government and Industry. Adoption of the Technical Communities concept is motivated by a desire to increase industry involvement in the process of specifying and testing IT products. Harnessing the specialized expertise of the commercial industry will enable the creation of PPs that are more technically relevant, better target the threats of the operational environment, and contain assurance activities that reflect commercial best practices in functional and security testing.

Technical Communities will be formed around major technology areas. Members of a technical community will represent diverse perspectives, have clear roles and responsibilities, and will be committed to developing objective, measurable, and relevant criteria against which commercial products can be effectively evaluated. NIAP has presented this concept to the international CC community, and invited them to participate in and help foster these Technical Communities, which will bring an even broader perspective to the groups.

Technical Community Purpose and Approach

Technical Communities are intended to be Government/Industry partnerships formed for the purposes of

- ensuring PP content reflects the current state and practice for secure use of identified technologies and
- influencing the evolution of identified technologies to ensure they are able to satisfy government protection needs in the face of changing threats.

A key goal for the Technical Communities is to ensure that PPs are not generated by any party (e.g., government or industry) in a vacuum; rather they are the result of close collaboration between communities with knowledge of the threats and capabilities for particular technologies and with responsibility for building and commercializing the technologies. Through this collaboration, NIAP hopes to gradually raise the security bar for commercial products, integrating emerging security capabilities and practices over time.

Technical Communities will be responsible for the following PP content:

- A set of technology-specific threats derived from operational knowledge and technical expertise,
- The minimal functionality sufficient to mitigate the identified threats, and
- A collection of assurance activities tailored to the technology and each functional requirement. These activities are to be objective, measurable, repeatable, and scoped such that they can be completed within a reasonable timeframe.

This approach differs from what has been done for PPs in the past. Under the new approach, Subject Matter Experts (SMEs) within the Technical Community are empowered to make decisions about content within the PP. Threat information will be provided by domain experts, and Security Functional Requirements (SFRs) and threats will be tightly integrated – only those capabilities that support government needs and are required to counter technology-specific threats will be included as SFRs in the PP. Assurance activities will be carefully crafted by SMEs from various Technical Communities in an effort to produce results that can be compared across technology areas.

Roles within the Technical Community

In order to achieve its goal, the Technical Community must be comprised of the right mix of individuals, each filling a particular role within the Community. The following paragraphs describe the roles and responsibilities of key participants within the Community.

Technical Community Lead

Every Technical Community will have a leader who oversees and manages the PP development activities of the group and is held responsible for the health and success of the Technical Community. While every effort will be made to make Technical Community decisions in a collaborative manner the lead will make decisions in cases where disagreements occur. The Technical Community Lead role is to be fulfilled by a

representative from NIAP. That representative has the option to designate a non-NIAP individual to fulfill the role.

The Technical Community Lead will be responsible for:

- Taking the lead in building the Technical Community membership, documenting and communicating the benefits of joining the Technical Community, and ensuring the Technical Community participants represent the necessary mix of SMEs from industry, Government, and elsewhere,
- Establishing the roadmap and schedule for PPs that address the spectrum of relevant capabilities of products within the technology area,
- Planning and leading a kick-off meeting for the Technical Community as a way to jump start the PP development effort,
- Identifying a Technical Editor for each PP to be developed,
- Participating in meetings with the Technical Community to oversee progress, set direction, and make key decisions as required,
- Coordinating final government approval of the PPs developed by the Technical Community.

Industry Subject Matter Expert (SME)

Within the Technical Community, commercial industry participants serve as the primary technology SMEs. Industry has the deepest knowledge of their technology functionality and is well-positioned to contribute to the PP development process. Participation in Technical Communities is one way for industry to influence changes to PPs and the evaluation process. Each Technical Community must have a mix of industry SMEs, preferably a *balance* of experts who can work together with the rest of the Community to develop a baseline for threats and core security functional requirements. Having industry SMEs with expertise in product testing is also helpful when drafting assurance activities within the PPs.

Industry SMEs are responsible for

- Helping to build Technical Community membership by reaching out to internal experts within their companies as well as to other industry SMEs,
- Contributing to the effort to define the scope and establish the roadmap (plan) for development of PPs by the group, and
- Leading the development of content for each PP.

Solution/Operational Subject Matter Expert

Each Technical Community must have one or more Solution/Operational SMEs. These individuals must possess a solid understanding of the operational considerations for the technology within the context of the relevant government solutions it needs to support. Expertise in the particular technology for which the PPs are being generated is also helpful.

Solution/Operational SMEs are responsible for

- Communicating technology-specific threat information and critical security requirements derived from government solutions, and
- Reviewing the PPs throughout the development process and providing feedback to ensure that the documents satisfy operational requirements.

Common Criteria Subject Matter Expert

CC expertise is required because the evaluation process relies on the CC as the form for expression of SFRs and Security Assurance Requirements (SARs). One or more CC SMEs should participate in the Technical Community to perform the task of ensuring that PPs comply, to the extent necessary, with the Common Criteria format. NIAP Validators can be assigned to Technical Communities as CC SMEs where their knowledge and experience can be applied.

CC SMEs are responsible for

- Ensuring that the PP contains the core content needed to ensure mutual recognition of the PPs by the international CC community, and
- Translation of SFRs and SARs to comply with the CC, which enables a CCTL to use the PP for evaluation.

Contributor/Reviewer

All participants in the Technical Community will be considered contributors/reviewers for the PPs. In addition to the SMEs listed in the paragraphs above, individuals from industry, government, CCTLs, and other international schemes are encouraged to participate. Individuals with expertise in product testing and evaluation will be asked to review PP drafts, focusing primarily on the set of assurance activities used to demonstrate satisfaction of the stated requirements.

CCTLs may also help in defining standard approaches and tools for testing the new requirements. Without a common approach to testing, and in some cases, a standard set of test tools, the goal of objective evaluations cannot be satisfied. NIAP will encourage the CCTLs to work together to achieve a greater degree of consistency among procedures and tools.

Technical Editor

The Technical Community Lead will identify a Technical Editor to serve as primary author for the PPs. The Technical Editor will be responsible for:

- Leading the effort to develop the PPs by maintaining the official draft,
- Working with the various SMEs to develop and incorporate PP content,
- Leading discussions in meetings to resolve technical issues and comments on PP drafts, and
- Delivering the PPs to the Technical Community Lead for final approval.

Oversight

NIAP serves in the oversight role with a number of important near-term and longer-term responsibilities. NIAP oversight will include:

- Generating a roadmap for PP development and assigning Leads to organize and kick off new Technical Communities chartered with developing PPs,
- Coordinating with Mutual Recognition Arrangement member schemes to foster adoption and to convey international concerns back to the Technology Community,
- Coordinating with other US Government agencies to ensure that the new evaluation process integrates well with other IA initiatives (e.g., DISA STIGS),
- Socializing the new approach within the operational user community and addressing outstanding concerns,
- Interacting with industry and CCTLs to determine the effectiveness of the PPs and to determine any adjustments necessary, and
- Introducing new concepts and evaluation methodologies into the PPs, such as an increased focus on testing for product vulnerabilities.

Executing the Technical Community Concept

Forming the Technical Community

NIAP will assign Leads to organize and kick off new Technical Communities. To facilitate establishment of new communities, NIAP will do the following:

- Conduct an ***Industry Day*** to announce the formation of a Technical Community and to engage with technical SMEs. At this event, NIAP will communicate the goals for the Technical Community, make introductions, and energize the group, and
- Present a ***compelling value proposition*** for participation to generate interest and to enlist a core set of committed Industry participants.

Once an initial set of members has signed on, the Technical Community Lead will be responsible for the ***logistics*** involved in launching the group's activities, such as setting up a collaborative work space, a mailing list and establishing regular meetings.

Developing the Protection Profiles

Once the key roles within the Technical Community have been filled, the group will begin to develop the PPs.

- First, the Technical Community Lead will identify a primary author for the PPs. This person will serve in the role of ***Technical Editor.***
- The Technical Community Lead will work with the community to develop and ***agree to a set of milestones*** that support completion of new PPs according to the roadmap generated by NIAP oversight.
- The Technical Community Lead will solicit ***volunteers to lead efforts to create content*** for the various sections of the PP (Threats, SFRs, Assurance Activities, and

SARs). Teams of SMEs and Reviewers/Contributors will begin the process of developing content for the PPs. As described above, Solution/Operational Subject Matter Experts will contribute heavily to the process of developing Threats and SFRs.

- The teams will need to ***meet frequently*** to discuss issues and progress and ensure a consistent approach is followed. It will be important for the Technical Community Lead to maintain a regular presence at meetings, particularly at the start of the effort, to provide high level direction and support.
- The Technical Community Lead ***will approve distribution of drafts*** of the PPs beyond the Technical Community for broader Industry review.

Maintaining the Protection Profiles

- The PPs developed by the Technical Communities will need to be ***reviewed on a regular basis*** (e.g., annually, or as technology changes) to determine whether updates are needed (e.g., to accommodate new threats or functionality, to review decisions arising out of evaluations), to determine whether new PPs are needed, or existing PPs should be sunset. Technical Community Leads will set the schedule for PP review.
- As the number of PPs grows and the Technical Community concept matures, there will be a need for a ***Review Committee*** that is responsible for monitoring and advising the Communities, appraising their results for consistency and impact, and facilitating longer term goals that will serve to advance the state of the practice in IT security. The Review Committee will be comprised of NIAP Leadership as well as Technical Community Leads. The Review Committee may also draw from the expertise of the NIAP Observation Decisions Review Board (ODRB).

Conclusion – Progress through Partnership

Through the formation of Technical Communities, NIAP is implementing a strategy that allows it to establish a strong partnership with various stakeholders in defining and executing a more relevant and value added commercial product security evaluation program. Technical Communities also offer the opportunity for increased collaboration between vendors and as a potential forum for developing joint security standards related to their technology area. Technical Communities allow participation from a broad set of stakeholders and consequently the opportunity for greater ownership and influence over the security-relevant capabilities of commercial products.

Longer term, it is envisioned that Technical Communities will lead to a gradually increasing resiliency of commercial products in the face of cyber threats, be it for government or civil use. The establishment of Technical Communities is a positive way forward for NIAP. With a strong organizational component and clear responsibilities these groups will be positioned for success.