NIAP 2016 Report

2016 was a year of growth for NIAP – increasing evaluated products available for National Security System procurement, collaborating with industry and government in the development of Protection Profiles which define security requirements and assurance activities for a wide range of commercial technologies, and representing the US in the Common Criteria Recognition Arrangement, including serving as the CCRA Development Board chair.

Protection Profiles (PPs)

During 2016, NIAP published 8 new Protection Profiles, 5 minor revisions to Protection Profiles in use, and 6 major revisions to correct previous versions of Protection Profiles.

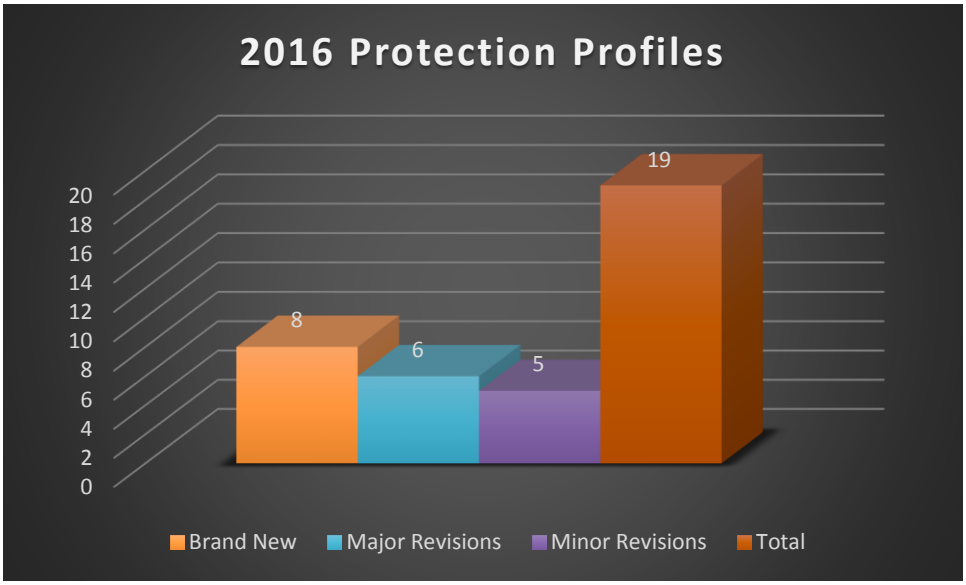

Figure 1. 2016 Completed Protection Profiles

Evaluated Products

A total of 52 evaluations were completed in 2016, bringing the total number of evaluated configuration over 800. During the 4th quarter of 2016, 6 new evaluations were completed. Implementation of strategies to streamline and improve both the evaluation and validation process while also ensuring consistency amongst all evaluations was clearly successful, making more products eligible for procurement on National Security Systems.

Mobile device remained a significant portion of evaluations, but network devices comprised the majority of evaluations this year. This indicates the importance of ensuring any device installed on the network will "behave" and can be trusted to do no harm, regardless of the ultimate security purpose of the device.

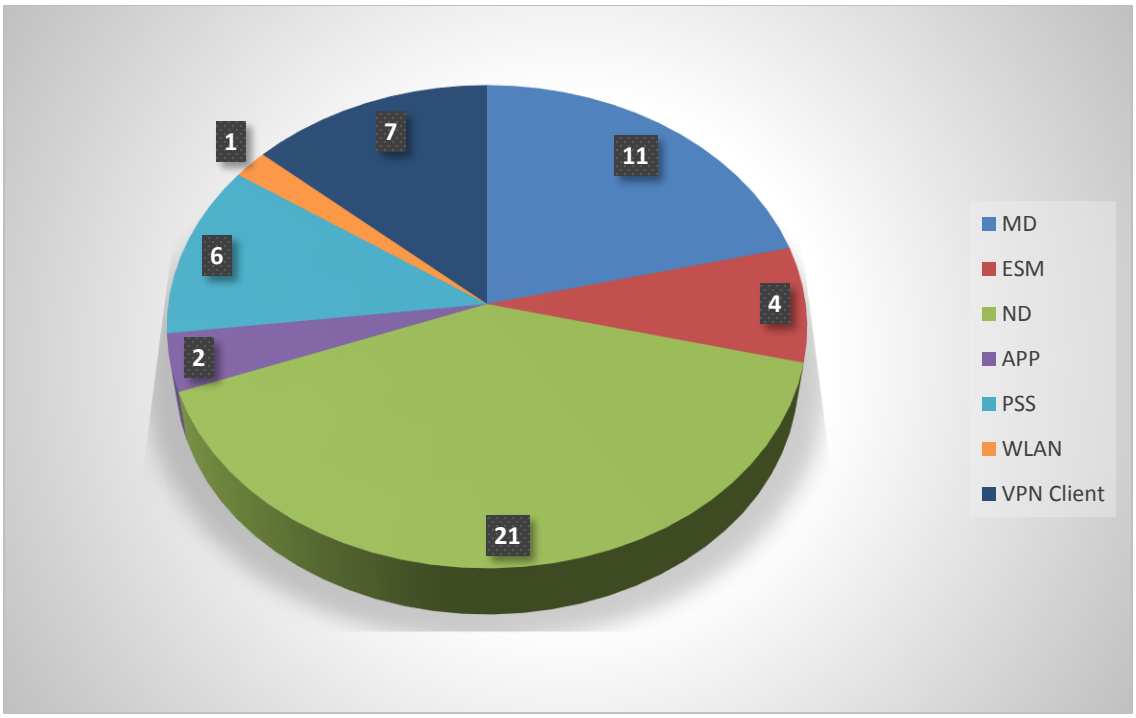

Figure 2. 2016 Completed Evaluations by Technology Type

Common Criteria Recognition Arrangement (CCRA)

Collaborative Protection Profiles (cPPs)

NIAP continued to fully support development of cPPs according to the terms of the CCRA. During 2016, we saw industry take a leading role in International Technical Communities (iTCs) – serving as iTC leads, technical editors, participating through regular teleconferences, and setting and driving cPP development schedules. This active industry participation and collaboration with governments underpins the value of the Arrangement, and serves to keep it relevant and viable.

Network Device and Stateful Traffic Filter Firewall cPPs

2016 marked the first year that contributing member nations evaluated products against the international cPPs. NIAP was the first scheme to evaluate a product against the international Network Device cPP. Three evaluations were completed against the ND cPP this year with four more Network Device evaluations currently in process. NIAP is the first scheme to begin an evaluation against the Stateful Traffic Filter Firewall cPP as well.

During the course of the ND cPP evaluations, NIAP's Network Device Technical Rapid Response Team received numerous inquiries on the cPP. NIAP worked with the Network iTC during the initial stand-up of the Network iTC Interpretation Team (NIT) and forwarded 28 requests for interpretation this year, far more than any other scheme so far. This resulted in 25 Technical Decisions and 9 Technical Recommendations published by the NIT. NIAP published thirteen NIT Technical Decisions applicable in our

scheme, making these available for all evaluations against the ND cPP. This ensures consistent and clear interpretation of the cPP requirements and evaluation activities across numerous evaluations.

Full Drive Encryption cPPs

The Full Drive Encryption iTC completed and published version 2 of both the Authorization Acquisition and Encryption Engine cPPs. These revisions incorporated additional use cases developed by iTC and set the stage for the addition of an enterprise management module, coming soon. NIAP is currently preparing for evaluations against these cPPs and will have a couple evaluation efforts beginning shortly.

New international Technical Communities

NIAP participated in the start-up of international Technical Communities for Software Applications and Dedicated Security Components. These iTCs made progress in 2016 with support from industry and several CCRA nations.

Commercial Solutions for Classified

U.S. Government customers increasingly require immediate use of the market's most modern commercial hardware and software technologies within NSS, in order to achieve mission objectives. The NSA is developing new ways to leverage emerging technologies to deliver more timely IA solutions for rapidly evolving customer requirements. While NIAP oversees evaluation of COTS IT products for NSS, the NSA's Commercial Solutions for Classified (CSfC) process enables commercial products to be used in layered solutions to protect classified NSS information. This provides the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

A NIAP evaluation is the foundational requirement for a product to be included as part of the CSfC program. Vendors who wish to have their products eligible as CSfC components of a composed, layered IA solution must build their products in accordance with the applicable NIAP-approved Protection Profile(s) and have their product evaluated according to NIAP requirements. The Central Intelligence Agency (CIA), Department of Homeland Security (DHS), and Southern Combatant Command (SOCOM) are all utilizing CSfC components and NIAP-certified products within their mobility infrastructure, and have registered use case solutions against CSfC's Mobile Access Capability Package.

Collaboration with NIST

NIST and NIAP continued collaborations in 2016 to align the NIAP evaluation processes with the NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) – commonly referred to as FIPS. This alignment contributes to ensuring current evaluated products are available for DoD use by leveraging NIST CAVP/CMVP validations in Common Criteria evaluations. NIAP evaluations require that each product's cryptography have at least a CAVP certificate and preferably a CMVP certificate. NIAP PPs are written so that they can be used internationally by nations that do not participate in FIPS, but a CAVP or CMVP certificate eliminates the need for the Common Criteria Test Lab to conduct some of the PP assurance tests. By eliminating redundant cryptographic testing, CC evaluations are expedited, saving government and industry both time and money.

As a result of the NIAP/NIST alignment, during 2016:

- NIAP continued to support and participate in NIST's CMVP Industry Collaboration Working Group (CMVPWG). The CMVPWG, comprised of both industry and government representatives, met regularly throughout the year to explore opportunities for streamlining the CMVP evaluation timeline to improve the operational impact of FIPS 140 validated modules. Working group activities included research and documentation of processes for design, development, testing, and maintenance of cryptographic implementations, as well as prototypes of new testing techniques and processes that may be implemented in future releases of CMVP. The emphasis is on automated solutions that produce artifacts or evidence that can be verified efficiently by test laboratories.
- NIAP participated in the 2016 NIST Crypto Algorithm Validation Program and Crypto Module Validation Program (CAVP/CMVP) and Chemical Science and Technology Laboratory (CSTL) Manager meeting held in Ottawa, Canada. NIAP's participation was valuable in providing updates on NIST's CAVP and CMVP programs, advance information about updates to NIST Implementation Guidance and Derived Test Requirements, updates on new Special Publications, and the current status of NIST's efforts to automate CAVP testing. NIAP's attendance strengthened our efforts as we continue to use NIST's CAVP and CMVP programs to satisfy the cryptographic security functionality requirements in NIAP Common Criteria evaluations.
- NIAP participated in the 2016 International Cryptographic Modules Conference held in Ottawa. NIAP and NIST's Computer Security Division (CST) jointly briefed on National Institute of Standards and Technology (NIST) and NIAP's continued collaborative efforts. NIAP also briefed their approach for cryptographic evaluations, specifically the use of NIST's Crypto Algorithm Validation Program (CAVP) and Crypto Module Validation Program (CMVP) programs to satisfy the cryptographic security functionality requirements in NIAP Common Criteria evaluations.

- NIST joined NIAP at the CC Crypto Working Group meeting in Reading, UK. The CC Crypto WG develops internationally-accepted cryptographic evaluation requirements and assurance activities. NIST was able to provide WG participants with much needed insight into NIST's current CAVP and CMVP testing programs as well as efforts toward the development of automated solutions for algorithm and module testing. The information provided by NIST assists the WG in the continued development of security requirements and evaluation activities for incorporation into collaborative Protection Profiles.
- NIAP updated NIAP CCEVS Policy #5, "Applicability and Relationship of NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) to NIAP's Common Criteria Evaluation and Validation Scheme (CCEVS)" and "Frequently Asked Questions for NIAP Policy #5" to fully leverage NIST cryptographic testing. In addition, an accompanying CAVP Mapping Document was developed. Policy #5, Policy #5 FAQ, and the CAVP mapping document provide clarification and guidance on how NIST's algorithm and module validations are determined to be acceptable as evidence for meeting cryptographic PP/cPP assurance activities in NIAP evaluations.

Outreach

Throughout 2016, NIAP continued to spread the word on the importance of evaluating commercial IT products to ensure the IT security needs of the NSS Community are met. Outreach focused on delivering tailored messages suitable for the intended audience in different environments.

The primary vehicle for outreach, the NIAP website, was constantly updated throughout 2016 to reflect up-to-date news, policy changes, and a current list of certified products. NIAP was present at a number of security conferences and forums in 2016 to engage directly with users and developers. These engagements helped bridge the gap between user requirements and product capabilities and how the NIAP process works. Notable conferences attended included RSA, ICMC, IAS, as well as a number of AFCEA TechNets. This year, NIAP briefed 2 classes at the National Defense University to a class of future Information Security Officers and Designated Accrediting Authorities who gained an appreciation for integrating certified products in their enterprises to ensure their security requirements are met.

Outreach activities also included workshops for members of our evaluation and validation communities to address issues that arise during product evaluation and present policy and procedural changes both at the national and international level.

Process Improvements

NIAP continued to focus on infrastructure improvements through website enhancements and development of web tools used to assist in the evaluation process. The website was restructured to provide a user-friendly interface to ensure customers can find information quickly and easily. NIAP added

content to describe relationships, the evaluation process, as well as a new Frequently Asked Questions (FAQ) page to assist customers with finding quick answers to common questions.

A web support tool was implemented to increase efficiency of Technical Rapid Response Teams (TRRT) communication and provide an effective tracking mechanism. The tool has enabled NIAP personnel to collaborate more efficiently with the teams, and improved response time to inquiries. Since the initial roll-out of the tool, NIAP has implemented several improvements to further enhance efficient communication among TRRT members.

NIAP also implemented a CCTL Project Check-in tool as well as enhancements to the Evaluation Consistency Review (ECR) tool to facilitate consistent and technically sound product validations. Both tools will assist with the documentation and project information sharing among Validators and Common Criteria Testing Labs (CCTLs). The development of these web support tools has assisted NIAP in its goal to streamline, improve, and ensure consistency of all evaluations.

Looking Forward

NIAP projects steady increases in the number of evaluated commercial products available for procurement during 2017. We will continue to foster collaboration with industry and other CCRA partners to develop Protection Profiles for evaluating COTS products needed for U.S. National Security Systems. The US looks forward to continuing as CCRA Development Board Chair, to facilitate full implementation of the updated CCRA by the agreed transition deadline of September 2017.