National Information Assurance Partnership (NIAP)
2017 Report

NIAP continued to grow and make a difference in 2017 – from increasing the number of evaluated products available for U.S. National Security System (NSS) procurement, to further collaboration with industry and U.S. government (USG), and to representing the U.S. in the international Common Criteria Recognition Arrangement (CCRA), including serving as the CCRA Development Board chair.

Protection Profiles (PPs)

In 2017, NIAP published 6 updates to existing Protection Profiles (PPs), which define security requirements and test activities for a wide range of commercial technologies: 1 conversion of an Extended Package to a Module, (in alignment with Common Criteria v3.1 Release 5), 4 minor revisions to existing Protection Profiles, and 1 internationally developed major revision to the Network Device collaborative Protection Profile.

PPs Completed in CY2017

Product	New/Revision	Technology Type
VPN Gateways EP (v2.1)	Minor Revision	Virtual Private Network
collaborative PP for Network Devices (v2.0)	Major Revision	Network Device
Intrusion Prevention Systems EP (v2.11)	Minor Revision	IDS/IPS
Mobile Device Fundamentals (v3.1)	Minor Revision	Mobility
VPN Client PP-Module (v2.1)	Minor Revision	Virtual Private Network
Certificate Authorities (v2.1)	Minor Revision	Certificate Authority

Figure 1. 2017 Completed Protection Profiles

Evaluated Products

A total of 63 evaluations were completed in 2017 (a 21% increase from 2016): 1st quarter 12 evaluations, 2nd quarter 16 evaluations, 3rd quarter 18 evaluations, and 4th quarter 17 evaluations. NIAP continued to implement strategies to streamline and improve both the evaluation and validation processes. These strategies ensured consistency among evaluations, increased output, and made more products eligible for NSS procurement.

Network devices comprised the majority of evaluations this year, though a significant portion of validated products were in the mobility technology area. This indicates the continued priority 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.

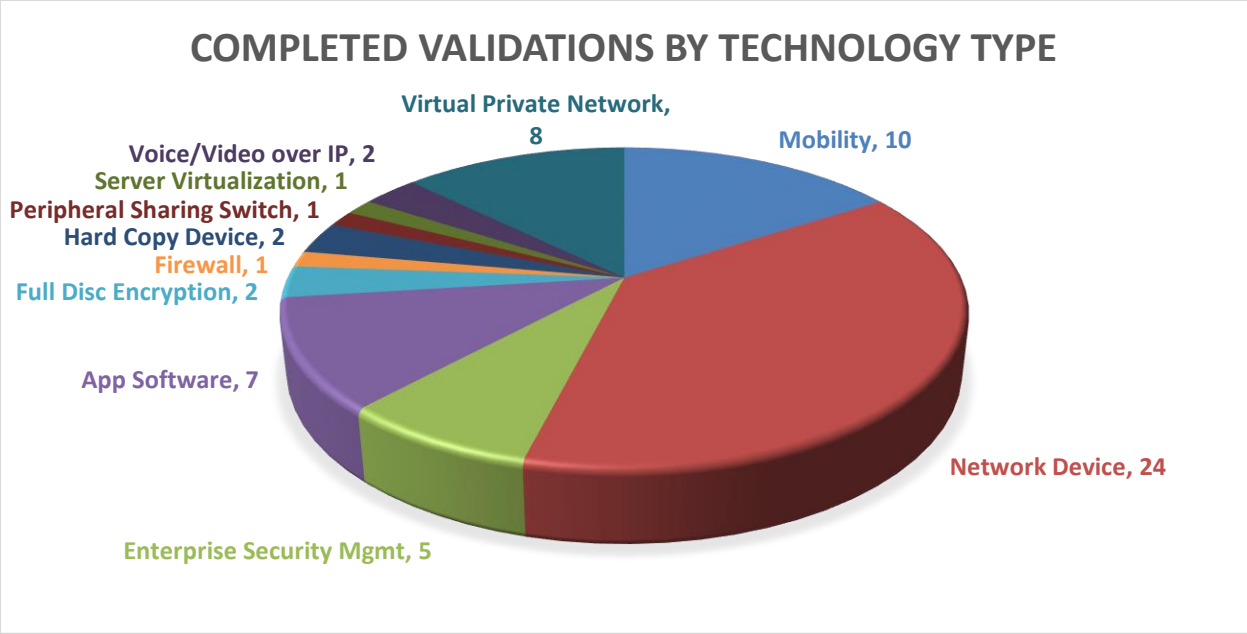

Figure 2. 2017 Completed Validations by Technology Type

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 2017, industry continued to lead cPP development 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 government underpins the value of the CCRA, and serves to keep it relevant and viable.

Network Device and Stateful Traffic Filter Firewall cPPs

2017 marked the second consecutive year that contributing member nations evaluated products against the international cPPs. NIAP completed 24 evaluations against the Network Device (ND) cPP, comprising 89% of all Network Device evaluations completed in the CCRA; with 24 more Network Device evaluations currently in process.

NIAP was the first scheme to complete an evaluation against the Stateful Traffic Filter Firewall cPP; finishing 2 evaluations against the cPP this year with 3 Stateful Traffic Filter Firewall evaluations currently in process.

NIAP's validation of products against cPPs is significant in two ways:
it provides NSS users with assurance in validated commercial products, while furthering the CCRA objective of allowing industry to evaluate a product once and sell to many nations.

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 and the Network iTC Interpretation Team (NIT) and forwarded 15 requests for interpretation this year, far more than any other scheme. NIAP also published 44 Network Device Interpretation Team (NIT) Technical Decisions applicable in our scheme, making these available for all evaluations against the ND cPP. Collaboration with the NIT to resolve cPP questions ensures consistent and clear interpretation of cPP requirements and evaluation activities among all CCRA member nations and across numerous evaluations.

Full Drive Encryption cPPs

NIAP participated in the Full Drive Encryption (FDE) iTC, which began work on an enterprise management use case and need for NSS users. The FDE iTC stood up an Interpretations Team (FIT) to address questions on the cPPs. NIAP collaborated closely with the iTC and the FIT to resolve questions on the cPPs to ensure consistent application of the requirements during product evaluations. NIAP is currently preparing for evaluations against these cPPs and will validate evaluations beginning in 2018.

Ongoing international Technical Communities

NIAP continued participation in both the Dedicated Security Component and Software Application iTCs by collaborating with industry to define security functionality and test activities for these technologies. These iTCs are industry-led, demonstrating a firm commitment to industry and government collaboration.

Commercial Solutions for Classified

NIAP continued to validate products used in Commercial Solutions for Classified (CSfC) by demonstrating the value of NIAP-validated products for NSS users. As part of this effort, NIAP provided information, lessons-learned, and support to other CCRA nations exploring the composition of Common Criteria-validated commercial products in securing IT systems.

A NIAP validation 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 Information Assurance (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 DHS

NIAP collaborated with the DHS to define security requirements for commercial mobility technology used throughout the USG.

NIAP collaborated with DHS on a report to Congress, entitled Study on Mobile Device Security, detailing current and emerging threats to USG use of mobile devices and recommends security improvements to the mobile device ecosystem. Mandated by the Cybersecurity Act of 2015, the study also relied on significant input from mobile industry vendors, carriers, service providers and academic researchers. It recommends adoption of mobile security criteria found in NIAP Protection Profiles as a way to provide increased assurance for mobile devices.

NIAP's collaboration with DHS also included a pilot for automated development of applications that comply with the NIAP Application Software Protection Profile, resulting in increased assurance for this growing technology area throughout the USG.

Collaboration with the National Institute of Standards and Technology (NIST)

The NIAP/NIST alignment continues to ensure current evaluated products are available for NSS users by leveraging the results of NIST cryptographic algorithm and module validation programs in NIAP evaluations.

NIST and NIAP continued collaboration in 2017 to align NIAP validation processes with the NIST Cryptographic Algorithm Validation Program (CAVP) and Cryptographic Module Validation Program (CMVP) – commonly referred to as FIPS. 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 2017:

- 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 2017 NIST Crypto Algorithm Validation Program and Crypto Module Validation Program (CAVP/CMVP) and Chemical Science and Technology Laboratory (CSTL) Manager meeting. 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 briefed 3 sessions at the 2017 International Cryptographic Module Conference. The conference provided an opportunity to collaborate with vendors, test labs, various policy makers and end users on cryptographic certification and the effect of technology advancements on our current paradigms.
- NIST continued to support NIAP at the CCRA Cryptographic Working Group (WG) meeting in Bonn, Germany. The CCRA Cryptographic WG develops internationally accepted cryptographic evaluation requirements and assurance activities. NIST continued 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 cPPs.

Outreach

Throughout 2017, NIAP continued outreach efforts to ensure the commercial IT security needs of the NSS Community are met through collaborative development of commercial product security requirements and evaluation of products against those requirements. Outreach focused on delivering tailored messages suitable for the intended audience in different environments.

NIAP participated in several security conferences and forums in 2017 to engage directly with users, developers, and Common Criteria Users Forum delegates. These engagements helped bridge the gap between user requirements and product capabilities; and enabled NIAP to explain its process as well as provide updates to NIAP policies and procedures.

Notable conferences attended included RSA, the International Cryptographic Module Conference, the Information Assurance Symposium, as well as a number of Armed Forces Communications and Electronics Association (AFCEA) TechNets. This year, NIAP briefed 2 classes of future Information Security Officers and Designated Accrediting Authorities at the National Defense University. Students gained an appreciation for integrating certified products in their enterprises ensuring their security requirements are met.

Outreach activities also included workshops and boot camps for members of our evaluation and validation communities to improve consistency, and present policy and procedural changes both at the national and international level. Other significant outreach activities included participation at an Information Assurance Tech Expo hosted by the National Security Agency (NSA) and included participation from CSfC, NIST, and other NSA organizations. This unclassified event gave vendors an opportunity to learn about unclassified technologies and standards developed or used by NSA and improve their chances of developing or selling technologies to NSA and the DoD. NIAP personnel engaged with over 100 industry reps who wanted to learn more about the NIAP mission and how it relates to CSfC and NIST, and how NIAP-validated products keep NSS customers compliant with national policy.

Process Improvements

NIAP continued to focus on infrastructure improvements through website enhancements and development of web tools used to assist in the evaluation process. NIAP completed beta testing of the Evaluation Consistency Review (ECR) tool and officially rolled out the tool for all new product evaluations. The tool serves multiple purposes for the NIAP program, including increased Validator consistency, protection of proprietary data, and increased visibility into NIAP project details, which facilitates metrics collection and process improvements.

NIAP also rolled out a new Technical Decision (TD) Digest tool to assist with customer outreach efforts and increase program transparency. This tool allows NIAP to easily share the latest updates made to Protection Profiles, providing Common Criteria Testing Labs (CCTLs) and vendors with the current information needed to successfully evaluate commercial products for use in NSS. These features have improved communications and increased evaluation efficiency.

The development of these web support tools has assisted NIAP in its goal to streamline, improve, and ensure consistency of all evaluations. The result is significant – validation time has dropped from up to 3 years to 90 days.

International Organization for Standardization (ISO) Common Criteria Update

The Common Criteria is an international standard (ISO 15408) that provides the specification language used to define security functional requirements and test activities for evaluation of commercial IT products. The standard is used by NIAP to develop Protection Profiles used in evaluation of commercial products eligible for NSS procurement. The ISO working group (WG3) solicited comments on the first working drafts of the updated standard, with the goal of sufficiently addressing the evolution of security functionality in commercial IT products. NIAP reviewed and provided comments on the working drafts to ensure USG interests are embodied in the update.

Looking Forward

NIAP projects steady increases in the number of evaluated commercial products eligible for procurement during 2018. 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.