National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2020 Report

Through the unprecedented times COVID-19 presented in 2020, NIAP continued to make a difference despite having to temporarily shut down operations and limit staffing resources. NIAP continued to focus on increasing the number of evaluated products available for U.S. National Security System (NSS) procurement, establishing new virtual mechanisms to further collaborate with industry and U.S. government (USG), as well as representing the U.S. in the international Common Criteria Recognition Arrangement (CCRA). NIAP continues to adjust operations as needed in today's environment to pursue activities which provide the most value for our users, meeting U.S. government National Security Customer needs.

Process Improvements

NIAP continued to strive to make significant improvements through website enhancements and development of web tools used to improve existing processes. In 2020, NIAP implemented new collaboration tools to increase efficiency and productivity, as well as adapted to a new working environment to support virtual engagements. New tools and enhancements were also introduced to increase visibility and improve communication for the Entropy Assessment Report (EAR) required for NIAP evaluations. Internal modules were created to aid validators in managing workloads, to include improvements in tracking progress and prioritizing various assignments. NIAP is dedicated to enhancing business automation processes to constantly evolve in order to meet the demands of the NIAP mission.

Automation

NIAP continued to support automation efforts to improve efficiency and collaboration through the use of next-generation tooling to support automated testing and development of Protection Profiles (PPs).

NIAP partnered with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in a joint pilot effort to determine to what extent NIAP evaluations of mobile application software could be automated. The pilot was successful and the published report, titled *Automating National Information Assurance Partnership Requirements Testing for Mobile Apps*, demonstrates that automated testing tools and methodologies are reliable and efficient. By making strides in these areas of automation, DHS and NIAP offer agencies the ability to quickly, affordably, and reliably determine if

their applications meet stringent security requirements. NIAP encourages stakeholders from both the federal government and industry to continue developing these types of tools to address the increasing scale and complexity of certifying mobile applications.

Throughout 2020, NIAP continued to develop and refine a formally defined XML schema that provides structure for PPs. Use of this schema, and tooling available on GitHub, enabled collaborative development of PPs through the use of the Git versioning system, with all changes fully transparent on GitHub. Using such a schema allowed PPs to be viewed as web pages, creating a more dynamic document experience.

NIAP also participates in the Common Criteria Users Forum (CCUF) Test Automation Working Group which is focused on developing and publishing a set of best practice recommendations for test automation in CC. NIAP is supportive of test automation, where it makes sense, and focusing evaluation time on harder (less prescriptive) security testing.

Evaluated Products

Despite the numerous challenges in 2020, NIAP certified more products than any other year with a total of 81 evaluations completed. Network devices comprised the majority of evaluations again this year. This indicates the continued priority of ensuring a device will "behave," regardless of the ultimate security purpose of the device.

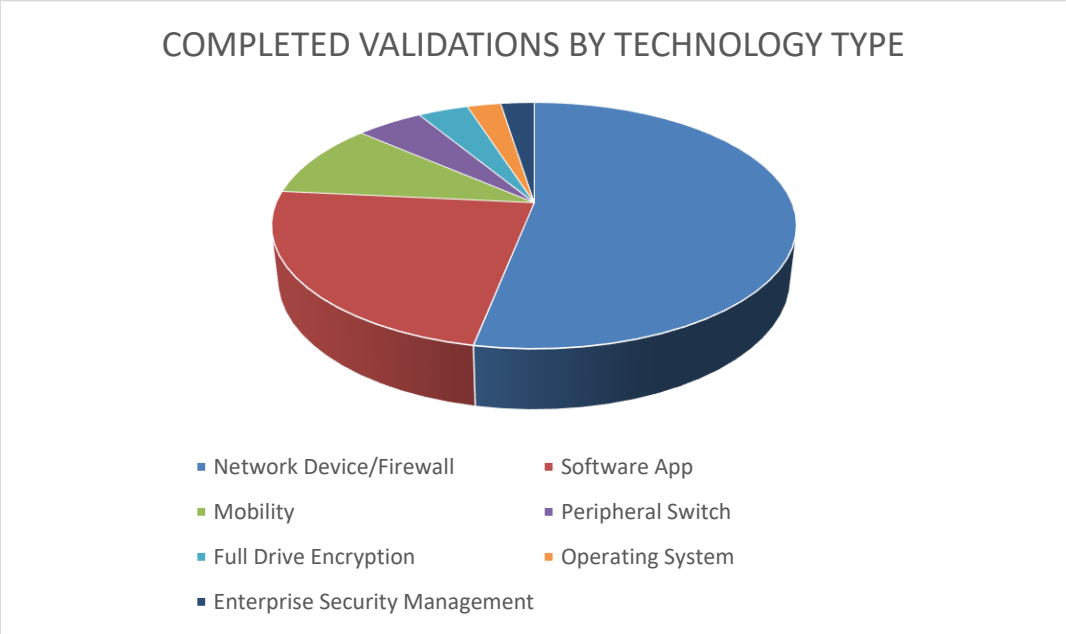


Figure 1. 2020 Completed Validations by Technology Type

Protection Profiles (PPs) and collaborative Protection Profiles (cPPs)

While continuing to serve our customers in 2020, NIAP developed and published two new Protection Profile Modules (PP-Modules), which define security requirements and test activities for TOE types complementary to one or more PPs. NIAP also converted three Extended Packages (EPs) to PP-Modules, in alignment with Common Criteria v3.1 Release 5, and during the process of converting the EPs, NIAP made updates to two of them. Additionally, NIAP endorsed one new collaborative Protection Profile (cPP) and two updated cPPs.

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.

PPs Completed in CY2020

Product	New/Revision	Technology Type
cPP for Network Devices v2.2e	Minor	Network Device
PP-Module for VPN Gateways v1.1	Minor	Virtual Private Network
cPP-Module for Stateful Traffic Filter Firewalls v1.4e	Minor	Firewall
cPP for Dedicated Security Component v1.0	New	HW Platform and Components
PP-Module for WIDS/WIPS v1.0	Major/Conversion	Wireless Monitoring
PP-Module for Host Agent v1.0	New	Enterprise Security Management
PP-Module for Endpoint Detection and Response v1.0	New	Enterprise Security Management
PP-Module for Voice and Video over IP v1.0	Minor/Conversion	VoIP
PP-Module for Enterprise Session Controller v1.0	Conversion	SIP Server

Figure 2. 2020 Completed Protection Profiles

Common Criteria Recognition Arrangement (CCRA)

NIAP continues as Common Criteria Development Board (CCDB) liaison to the Common Criteria Users Forum (CCUF) since 2019 and looks forward to continued close collaboration between the CCDB and CCUF. NIAP is participating in the Common Criteria Users Forum (CCUF) CC in the Cloud Technical Working Group (TWG). The TWG has recently been established by vendors and is exploring options and approaches for the CC evaluations of cloud products. The main goal is to determine how the Common Criteria (CC) may be applied to cloud service deployments of traditional on-premise products and to new cloud services developed specifically for the cloud. NIAP is also participating in a CCRA working group to explore possible solutions to ensure the harmonization of the CCRA and the future European Union Cybersecurity Certification (EUCC) Scheme being developed in accordance with the EU Cybersecurity Act (EU CSA).

collaborative Protection Profiles (cPPs)

During 2020, 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. NIAP fully supports development of cPPs according to the terms of the CCRA.

CCDB Crypto Working Group

The CCDB Crypto Working Group (WG) continued to meet virtually and focused on refining the specification of a generic set of Security Functional Requirements (SFRs) to model cryptographic protocols for inclusion in the ISO 15408 Part 2. Inclusion of mutually agreed upon cryptographic requirements enables harmonization of such requirements for use in PPs and product evaluations across all CC Schemes.

Voluntary Periodic Assessment (VPA)

In early March, NIAP hosted CCRA member nations as part of its mandatory Voluntary Periodic Assessment (VPA). The purpose of a VPA is to determine that the constitution and procedures of the certification body continue to comply with the requirements of the CCRA. The VPA team found NIAP was fully compliant.

Outreach

Throughout 2020, NIAP continued outreach efforts to ensure the commercial IT security needs of the NSS Community were 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 2020 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 and forums attended included RSA, the International Cryptographic Module Conference (ICMC), International Common Criteria Conference (ICCC), one Common Criteria Users Forums (CCUF), as well as a number of CSfC vendor engagements.

NIAP briefed two sessions at the virtual 2020 International Cryptographic Module Conference (ICMC). The NIAP Director and a representative from NIST's Computer Security Division jointly briefed on NIST and NIAP's continued collaborative efforts. NIAP also briefed current efforts and approach for determining and allowing for processor equivalency for NIAP cryptographic evaluations. NIAP participated in panel discussions related to cryptography and hardware security modules (HSMs) in the cloud and CPU equivalency. This conference facilitated collaboration with key stakeholders on a variety of topics regarding cryptographic certification.

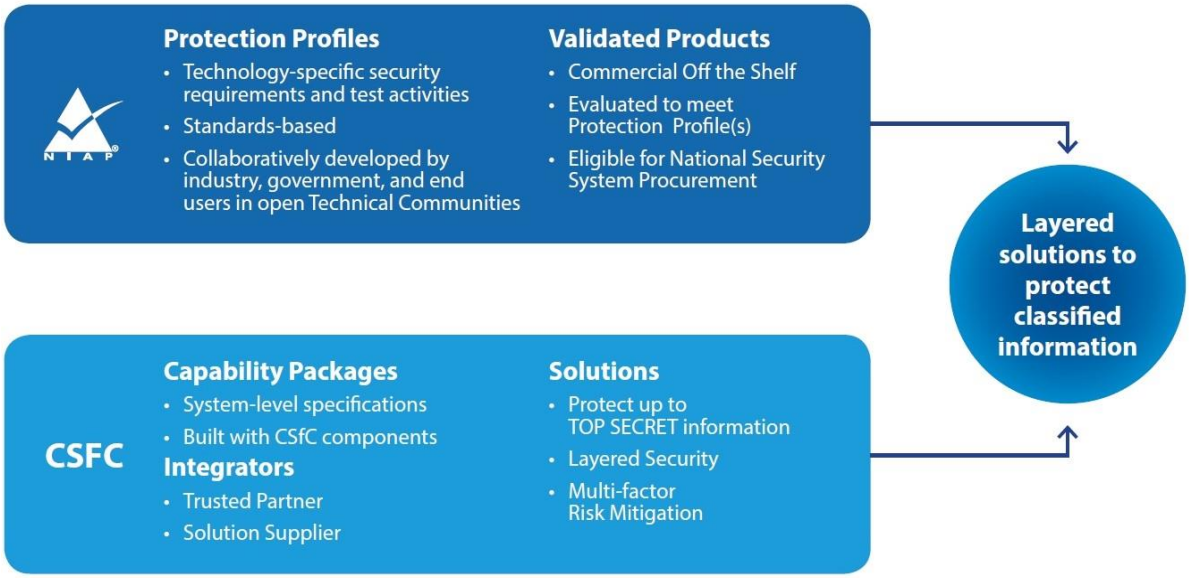
Upcoming Engagements:	
EU CSA	March 2021
CCUF	May 2021
RSA	May 2021
ICMC	September 2021

Commercial Solutions for Classified (CSfC)

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.

CSfC selections define the specific PP requirements that must be included as part of a Common Criteria Evaluation for a product to be eligible for use in a CSfC solution. See https://www.nsa.gov/Resources/Everyone/csfc/Components-List/ for selections per technology.

NIAP personnel presented at NSA's Commercial Solutions for Classified (CSfC) Virtual Conference on 30 September. NIAP provided an overview of the NIAP program and its relationship to CSfC and participated in a panel with CSfC personnel taking questions from the audience on wide-ranging topics including mutual recognition of cybersecurity certifications with international partners, impacts from COVID-19, and support for upcoming technologies.



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

NIST Cryptographic Algorithm Validation Program (CAVP) and/or Cryptographic Module Validation Programs (CMVP) certificates continue to help eliminate redundant cryptographic testing within the USG, thereby, CC evaluations are expedited, saving government and industry both time and money.

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.

NIAP fully supports NIST ACVP testing and updated its 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 align with NIST's ACVP. The updated NIAP Policy #5 took effect 01 March 2020. Throughout 2020, NIAP received many questions from Common Criteria Testing Laboratories (CCTLs) and vendors on the updated policy and it's FAQ. As a result, both will be updated in 2021 to provide more clarity regarding equivalency and certificate reporting requirements. NIAP also continues to collaborate and coordinate with NIST CAVP/CMVP on transitions, policy/IG revisions, and entropy testing (and new certification scope).

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 standards are currently moving forward to the Final Draft International Standard (FDIS) stage and are expected to be sent out for a final vote mid-year 2021. If no objections are raised, they will be published in Fall 2021. NIAP continued to review and provide comments on the drafts and worked with the ISO editorial team throughout the year to ensure USG interests are embodied in the update.

Looking Forward

In 2021, NIAP projects further increases in the number of evaluated Commercial-Off-the-Shelf (COTS) IT products eligible for procurement. NIAP will continue to focus on automation efforts as work continues to streamline, improve, and ensure consistency in evaluations.

NIAP also anticipates increased virtual collaboration with industry and other CCRA partners to develop Protection Profiles for evaluating COTS products needed for U.S. National Security Systems. This includes efforts to provide solutions for conducting evaluations of products residing in virtual environments where the platform is ever-changing.