National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2021 Report

In spite of the challenges that COVID-19 presented this year, NIAP continued to focus on the increase of evaluations and closed with 90 completed product evaluations. NIAP remained supportive of the Protection Profiles (PPs) methodology and found significant value in collaboratively applying resources to develop sound PPs as opposed to analyzing the product after the fact. Through PPs and the Technical Community (TC) process for developing them, NIAP plans to reach consensus with industry on security requirements specific to each technology while being vendor agnostic. PP updates allowed NIAP to raise the bar on security to make better and more secure products for government end-users. Due to the transparent, objective, testable, and repeatable requirements within the PPs, vendors know exactly what they must do to pass a NIAP evaluation.

Process Improvements

NIAP focused on developing major website improvements that enhanced business automation processes, as well as assisted in supporting virtual engagements needed due to the Covid-19 pandemic. In 2021, NIAP implemented new features to web tools such as the Entropy Assessment Report (EAR) and Evaluation Consistency Review (ECR) by adding visibility/privacy options, sync session requirements, and notification alerts which improved official communication between validators and CCTLs. The development of these web support tools allowed teams to collaborate more efficiently, reduced the dependence on emails, and ensured all evaluations were consistent. In addition, these upgrades enhanced the training resources between senior validators and trainees. NIAP also improved Protection Profile (PP) documentation postings, expanded the Assurance Maintenance tool, and generated search capabilities for Validation IDs with the same conformance claims to increase productivity, transparency, and improve tracking capabilities for validators and the NIAP team. NIAP is committed to working diligently on improving the website infrastructure to enhance communications, expand collaboration tools, and streamline evaluation processes which underpin NIAP's mission and goals.

Automation

NIAP continued to support automation efforts to improve efficiency of evaluations by using next-generation tooling to support development of Protection Profiles (PPs) and Security Targets (STs).

NIAP largely completed refinement of its XML schemas for PPs, Modules, and Functional Packages, and continued development of its Security Target (ST) Generation Tool. The ST Tool ingests the XML documents and allowed labs to input information about a product to generate a Security Target. The tool applied validation rules to the generated ST, thus relieving validators and automatically ensuring that the STs are valid. NIAP plans to pilot the ST Tool on an actual evaluation in early 2022 as it continues to refine and expand the tool's capabilities. Ultimately, the ST Tool will support generating STs for all NIAP PPs, Modules, and Packages.

NIAP participated in the Common Criteria Users Forum (CCUF) Test Automation Working Group which focused on developing and publishing a set of best practice recommendations for test automation in Common Criteria (CC). The working group worked on recommendations for technical communities to specify what constitutes sufficient evidence to show that test results meet requirements. This helped validators better understand the expectations of the technical community when they wrote requirements.

Evaluated Products

NIAP certified 90 evaluations in 2021. Network devices comprised most evaluations this year.

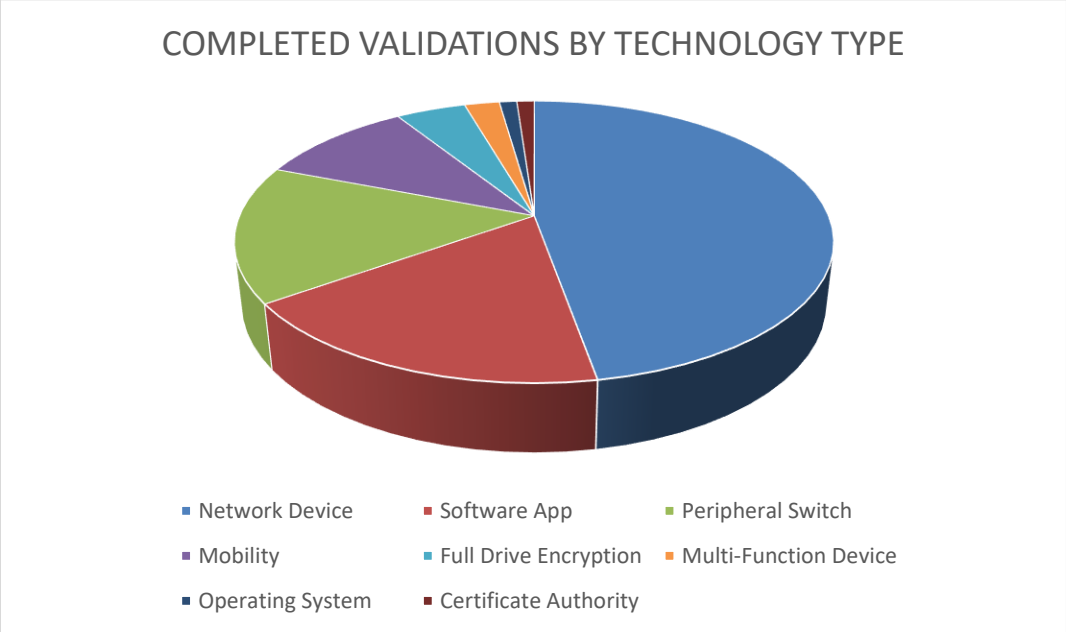


Figure 1. 2021 Completed Validations by Technology Type

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

In 2021, NIAP focused on updating its existing PPs, issuing revisions for three PPs and one PP-Module. NIAP also converted four Extended Packages (EPs) to three PP-Modules and one Functional Package, in alignment with Common Criteria v3.1 Release 5. NIAP also developed and published one new PP-Module, which defined security requirements and tested activities for Target of Evaluation (TOE) types complementary to one or more PPs.

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.

The Figure below depicts the changes to the Protection Profiles in Calendar Year 2021.

PPs Completed in CY2021

Product	New/Revision	Technology Type
PP for Application Software v1.4	Minor	Application Software
PP-Module for VPN Client v2.3	Minor	Virtual Private Network
PP-Module for Client Virtualization v1.1	Minor	Virtualization
PP-Module for Server Virtualization v1.1	Minor	Virtualization
PP for Virtualization v1.1	Minor	Virtualization
Functional Package for SSH v.1.0	Minor	Remote Access
PP-Module for Intrusion Prevention Systems (IPS) v1.0	Minor	Wireless Monitoring
PP-Module for Bluetooth v1.0	New	Wireless PAN
PP for Mobile Device Fundamentals v3.2	Minor	Mobility

Figure 2. 2021 Completed Protection Profiles

Common Criteria Recognition Arrangement (CCRA)

NIAP continued as Common Criteria Development Board (CCDB) liaison to the Common Criteria Users Forum (CCUF) since 2019 and looks forward to continuing close collaboration between the CCDB and CCUF. NIAP participated in the CCUF Common Criteria (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 CC may be applied to cloud service deployments of traditional on-premises products and to new cloud services developed specifically for the cloud. NIAP is also participating in the CCDB and received approval for both a short and long-term solution

to present to the EU Commissioner 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 2021, 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.

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.

Outreach

Throughout 2021, 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 2021 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 at the virtual 2021 International Cryptographic Module Conference (ICMC). NIAP provided updates on policy and collaboration efforts with NIST, ensuring industry partners can properly implement cryptographic functions in their products and improve security in U.S. and ally systems. This conference facilitated collaboration with key stakeholders on a variety of topics regarding cryptographic certification.

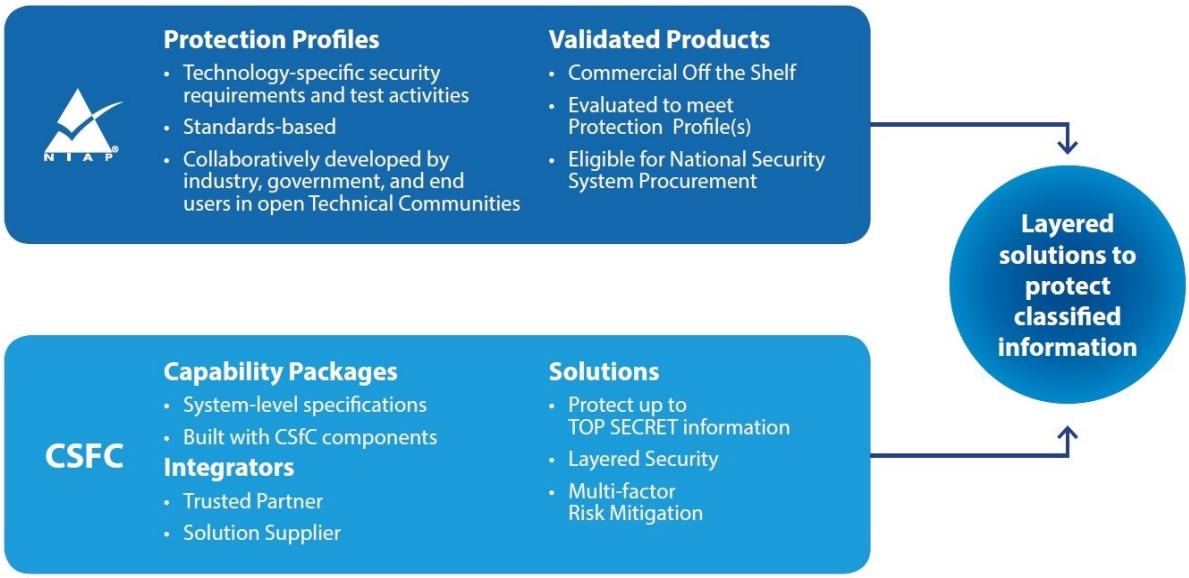
Upcoming Engagements:	
CSfC Conference	May 2022
EU CSA	May 2022
CCUF	Spring 2022
RSA	June 2022
ICMC	September 2022
ICCC	November 2022

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 31 August. NIAP provided an update briefing during the conference, addressing NIAP's history and evaluation processes, and provided customers with a deeper understanding of what products can be evaluated and procured for use in National Security Systems.



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

NIST Cryptographic Algorithm Validation Program (CAVP) and/or Cryptographic Module Validation Programs (CMVP) certificates helped eliminate redundant cryptographic testing within the USG, thereby expediting CC evaluations and 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 will continue to collaborate and coordinate with NIST CAVP/CMVP on transitions, policy/IG revisions, and entropy testing to ensure adherence to the most recent NIST standards.

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 Spring 2022. If no objections are raised, they will be published later in 2022. 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 2022, NIAP projects 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 will serve as the Common Criteria Management Committee (CCMC) chair through 2023. In addition, the ICCC will be located in the U.S. and will allow for discussion on the policy and application of CC and provide an opportunity for professional networking for those in charge of specification, development, evaluation, and certification.

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.