National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2022 Report

As 2022 came to a close, NIAP continued to focus on increasing the number of products on the Product Compliance List (PCL) and closed with 81 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 continuously strives to make infrastructure improvements through website enhancements, expansion of business procedure capabilities, and development of web tools used to assist in the product evaluation process. In 2022, NIAP awarded a contract to Quevera, LLC to design, build, and install a new modernized public facing website to replace NIAP's legacy system to provide a superior customer experience, streamline usability, offer detailed reporting/metrics, and enhanced business practices for simplicity and mobile usage. In collaboration with NIAP, Quevera has systematically collected requirements to learn current operational procedures for product evaluations and development of Protection Profiles. Multiple walkthrough meetings outlining existing business functions were organized with various stakeholders such as validators and Common Criteria Testing Labs (CCTLs) to capture the "as-is" process and, thus, serve to underpin innovative and contemporary proposed enhancements to implement in the new system.

While the website is under development, Quevera fully transitioned the existing underlying databases, applications, technologies, as well as completed a knowledge transfer from the previous contractor to perform tasks and assume the operational support and maintenance of the current legacy website independently. This subsequently ensures there is no loss of mission capabilities and, thus, reduces inherent government risk for support of international reliant websites. The contractor provides NIAP weekly status updates and development progression of the new website which will feature enhanced business automation procedures that will constantly evolve to support the demands of the NIAP mission.

The upgraded, modernized, and mobile-optimized website system is expected to be fully operational by the Fall/Winter of 2023.

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 piloted the ST Tool in early 2022, continuing to refine and expand the tool's capabilities. Ultimately, the ST Tool will support generating STs for all NIAP PPs, Modules, and Packages. The Automation team used their tools to evaluate multiple PPs and cPPs prior to being published, identifying areas for improvement. These efforts also identified areas in which NIAP can continue to strengthen PP development. Additionally, the Automation team began initial work on a strategic plan to ensure a more efficient process in developing PPs.

Evaluated Products

NIAP certified 81 evaluations in 2022. Network devices comprised most evaluations this year.

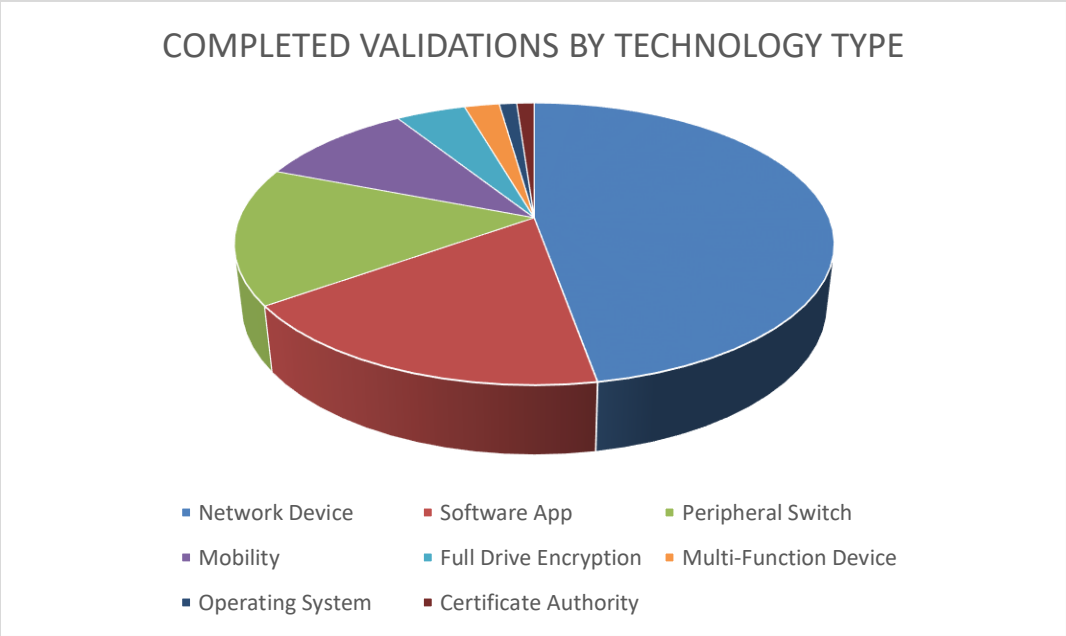


Figure 1. 2022 Completed Validations by Technology Type

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

In 2022, 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. The Figure below depicts the changes to the Protection Profiles in Calendar Year 2022.

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 CY2022

Product	New/Revision	Technology Type
PP for General Purpose Computing Platform v1.0	New	HW Platform and Components
PP-Module for VPN Client v2.4	Minor	Virtual Private Network
PP-Module for VPN Gateway v1.2	Minor	Virtual Private Network
PP-Module for Wireless LAN Access System v1.0	Major	Wireless LAN
PP-Module for Wireless LAN Client v1.0	Major	Wireless LAN
cPP-Module for Biometrics (unlocking the device) v.1.1	New	Biometrics
PP for Mobile Device Fundamentals v3.3	Minor	Mobility
PP for General Purpose Operating Systems v4.3	Minor	Operating System
PP-Module for SSL/TLS Inspection Proxy v1.1	Minor	Traffic Monitoring
PP-Module for Session Border Controller v1.0	Minor	Network Device
Functional Package for TLS v2.0	Major	Network Encryption

Figure 2. 2022 Completed Protection Profiles

Common Criteria Recognition Arrangement (CCRA)

NIAP accepted the role and chaired the Common Criteria Management Committee (CCMC) during the Spain CCRA meetings in November. 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 2022, 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 2022 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 few CSfC vendor engagements.

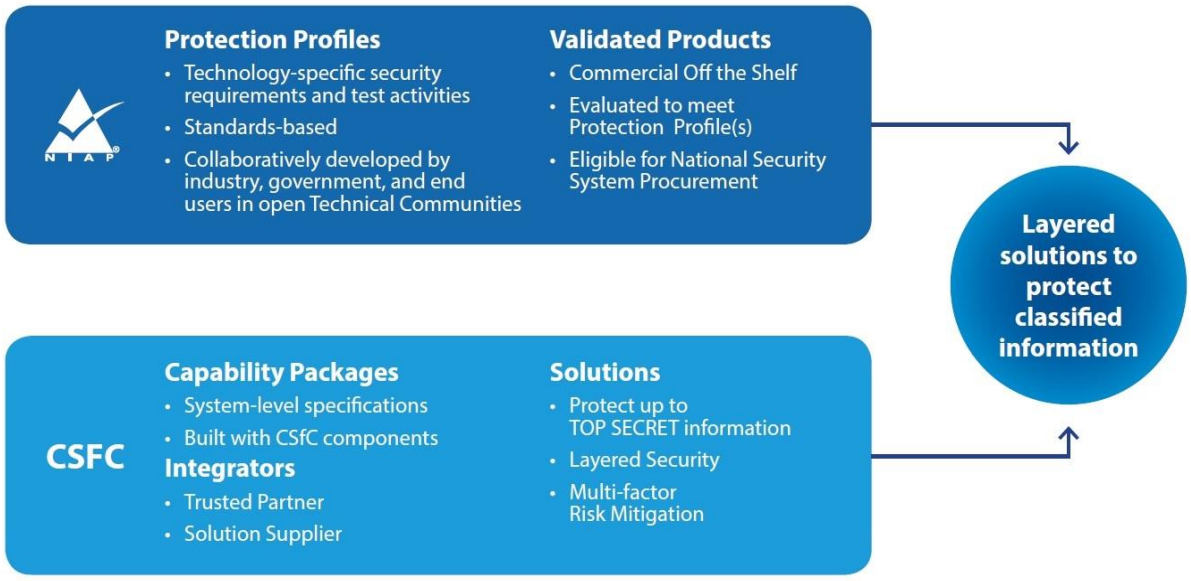
Upcoming Engagements:	
CSfC Conference	ICCC
EU CSA	March 2023
CCUF	Spring 2023
RSA	April 2023
ICMC	September 2023

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 attended and spoke at the Common Criteria Day on 9 May 2022 to industry security products providers and government integrators of CSfC solutions for use in classified systems. NIAP personnel also presented at NSA's Commercial Solutions for Classified (CSfC) Virtual Conference on 10 May. 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 and Common Criteria Evaluation Methodology are international standards (ISO/IEC 15408 and 18045) that provide 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.

These ISO standards, which have major revisions every 5 years, were published in August 2022. They were converted to Common Criteria documents, accepted by the CCRA and published on the Common Criteria

portal. NIAP continues to review and provide comments on ongoing work in ISO/IEC SC27 WG3 to ensure USG interests are embodied in updates and revisions.

Looking Forward

2023 looks to be a very busy year with many opportunities to improve security capabilities in commercial products through NIAP evaluations and improved security requirements in Protection Profiles.

In 2023, NIAP plans for 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 be launching a new web site in the latter half of 2023 focused on improved automation, access, and ability to modernize. In addition, the Common Criteria Portal managed by NIAP will be updated to a more modern platform and enhanced search and management capabilities for our international partners.

NIAP will continue to serve as the Common Criteria Management Committee (CCMC) chair through the fall 2023 CCRA meetings. In addition, the ICCC and CCRA meetings will be hosted in Washington, D.C. in October and November 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 cloud environments where the platform is ever-changing. Additional focus and resources will be put on the plans to update Protection Profiles to address CNSA 2.0 post quantum algorithm guidance and the new Common Criteria:2022 versions.