National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

2023 Report

As 2023 came to a close, NIAP continued to focus on increasing the number of products on the Product Compliance List (PCL) and closed with 87 completed product evaluations. NIAP continued to support the Protection Profile (PP) 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

In 2023, NIAP has been diligently working in collaboration with Quevera, LLC designing, building, and developing the new NIAP portal to provide a superior user experience for all stakeholders. The legacy website and data migration transitioned from ColdFusion to Amazon Web Services (AWS) for a more reliable, scalable, and secure infrastructure inclusive of Multifactor Authentication. The website has a modernized design that allows for increased transparency for users that includes an updated project evaluation status and a vendor login account feature. Furthermore, with an improved ticketing system coupled with automation procedures (i.e. DocuSign), these collectively provide a more streamlined workflow. NIAP also transitioned the email platform from CFDynamics to Microsoft 365 offering a better customer experience with email correspondence that also mitigates the amount of spam received and allows for a more comprehensive management of distribution lists. Moreover, NIAP is streamlining several business workflow functions and has conducted multiple walkthroughs and UAT sessions for various tools and features in the new portal, which have subsequently revealed process gaps, “bugs”, and issues that were addressed.

Despite the many challenges that have arisen in developing the new website which has delayed launching of the portal, NIAP and Quevera have remained resilient and determined by developing solutions to overcome these challenges. Robust testing of the site will continue to ensure the portal works as intended to support NIAP’s mission. Training sessions and artifacts for stakeholders are planned to ensure they understand the upgrades and changes implemented to the site. Launch date of the new modernized, mobile-optimized website is expected in Summer of 2024.

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 refined its XML schemas for PPs, Modules, and Functional Packages, while also continuing development of its Security Target (ST) Generation Tool. The ST Tool's primary function is to ingest XML and allow labs to input information about a product to generate a Security Target. The tool also applies various audits and checks to the generated ST, relieving validators and automatically ensuring ST validity. NIAP piloted the ST Tool in early 2023 to obtain feedback and requirements and have continued the effort to refine and expand the tool's capabilities. Ultimately, the ST Tool will support generating STs for all NIAP PPs, Modules, and Packages. Additionally, at NIAP's request, the automation development team created a Security Functional Requirement (SFR) Database, which is currently hosted on the Common Criteria (CC) GitHub. The SFR Database is a front-end tool that allows for the search, retrieval and comparison of Threats, Objectives, and SFRs from a number of Protection Profiles, Modules, and Functional Packages that come from NIAP and Common Criteria documentation. PP authors, validators, and SMEs can use the SFR Database to clarify and understand various relationships between key elements across PP's, saving time, effort, and creating greater accessibility.

Vulnerabilities

In early 2023, NIAP announced that a Software Bill of Materials (SBOM) pilot would be launched in response to EO14028 (spring 2021). The SBOM serves as a list of ingredients used in the creation of a piece of software, enabling producers and consumers to better track vulnerabilities risks of products listed on the PCL. A commercial tool was selected for SBOMs management. The SBOM pilot will launch in early 2023 for AppSW v1.5.

Cloud Evaluation

NIAP continued to make progress in the evaluation of Cloud products using the Common Criteria. In February 2023, NSA's Cybersecurity Collaboration Center hosted an in-person Common Criteria in the Cloud Workshop to progress the Common Criteria in the Cloud Guidance document. This document was mostly completed in December 2023. Simultaneously, NIAP also collaborated with FedRAMP, with vendors, internal NSA Subject Matter Experts and other agencies to understand the implications of Cloud evaluations for the Mobile Device Management Protection Profile. NIAP will utilize the foundation of FedRAMP authorizations as well as adhere to the security specifications of the Protection Profiles. NIAP started its first Cloud evaluation, Microsoft Intune, in October.

Evaluated Products

NIAP certified 87 evaluations in 2023. Network devices comprised most evaluations this year.

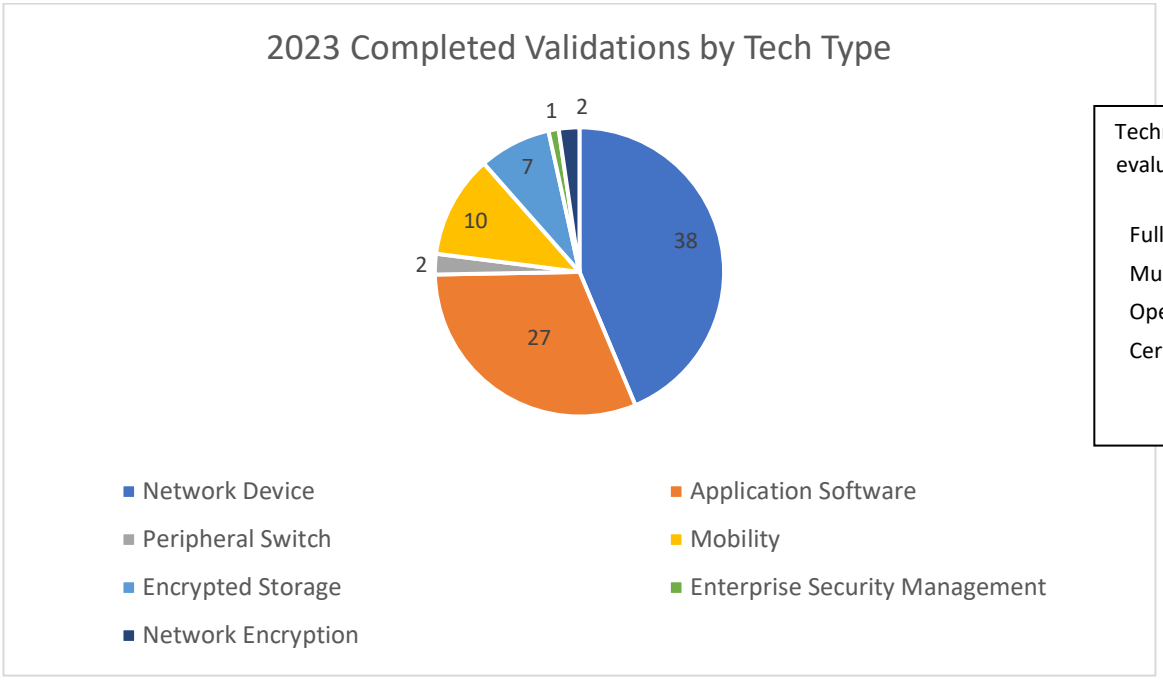


Figure 1. 2023 Completed Validations by Technology Type

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

In 2023, NIAP focused on updating its existing PPs, issuing a revision for one PP and beginning work on several more that will conclude in 2024. NIAP started one new Functional Package. NIAP also converted two Extended Packages (EPs) to PP-Modules, in alignment with Common Criteria v3.1 Release 5. NIAP also reviewed and accepted one revised cPP.

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 2023.

PPs Completed in CY2023

Product	New/Revision	Technology Type
PP-Module for Authentication Servers v1.0	**New**	**Network Device**
PP-Module for MACsec Ethernet Encryption v1.0	**New**	**Network Encryption**
PP-Module for VPN Gateway v1.3	**Minor**	**Virtual Private Network**
cPP for Network Device v3.0e	**Major**	**Network Device**

Figure 2. 2023 Completed Protection Profiles

Common Criteria Recognition Arrangement (CCRA)

NIAP chaired the Common Criteria Management Committee (CCMC) during the US/Washington D.C. CCRA meetings in late October into November 2023. 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 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. The WG completed the first draft of the "Crypto Catalog" and provided it to

the community for review. The WG is currently implementing comments submitted by multiple schemes and vendors with a goal of completion by April 2024. At that time, the team will begin drafting Evaluation Activities.

NIAP Successfully Hosted Annual CCRA Meetings in addition to representing NSA/US Scheme at ICCC Conference

Over the course of a robust, multiple-day event series, NIAP and the Leadership of NSA's Cybersecurity Collaboration Center, hosted representatives from the 31-nation CCRA (Common Criteria Recognition Arrangement) in Washington, D.C. from 25 Oct 2023 through 30 Oct 2023. These in-person sessions with international representatives allowed real time opportunities to discuss and further progress CCRA priorities in mutual recognition of commercial cybersecurity product evaluations and certifications.

The overall success of this event-series reinforces the continued strengthening and solid partnerships between this diverse group of nations focused on the advancement of internationally secure cybersecurity practices. In addition to hosting the CCRA, NIAP attended and provided critical briefings during the ICCC (International Common Criteria Conference).

Outreach

Throughout 2023, 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 2023 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.

Throughout 2023, NIAP presented and attended multiple notable conferences and forums. NIAP provided its plans for the year at the 2023 EU CyberSecurity Acts conference. The NIAP booth was well represented at the annual RSA conference with many questions from industry and international partners. The presentations at the International Cryptographic Module Conference (ICMC) included the annual look ahead, update on Entropy report, and a discussion on equivalency challenges. The International Common Criteria Conference (ICCC) covered presentations on NIAP Scheme, CCMC meeting summary, and evaluating Cloud products using NIAPs Mobile Device Management PP. During the Common Criteria Users Forums (CCUF) NIAP presented on the SBOM progression and the X509 Functional Package. There were also multiple NIAP and CSfC vendor engagements.

Future outreach events for 2024 are listed in the chart below.

EU CSA	March 2024
CCUF	April 2024
RSA	May 2024
CSfC Conference	May 2024
Validator/CCTL Workshop & Bootcamp	May 2024
ICMC	September 2024
Validator/CCTL Workshop & Bootcamp	Fall 2024
ICCC	November 2024

Commercial Solutions for Classified (CSfC)

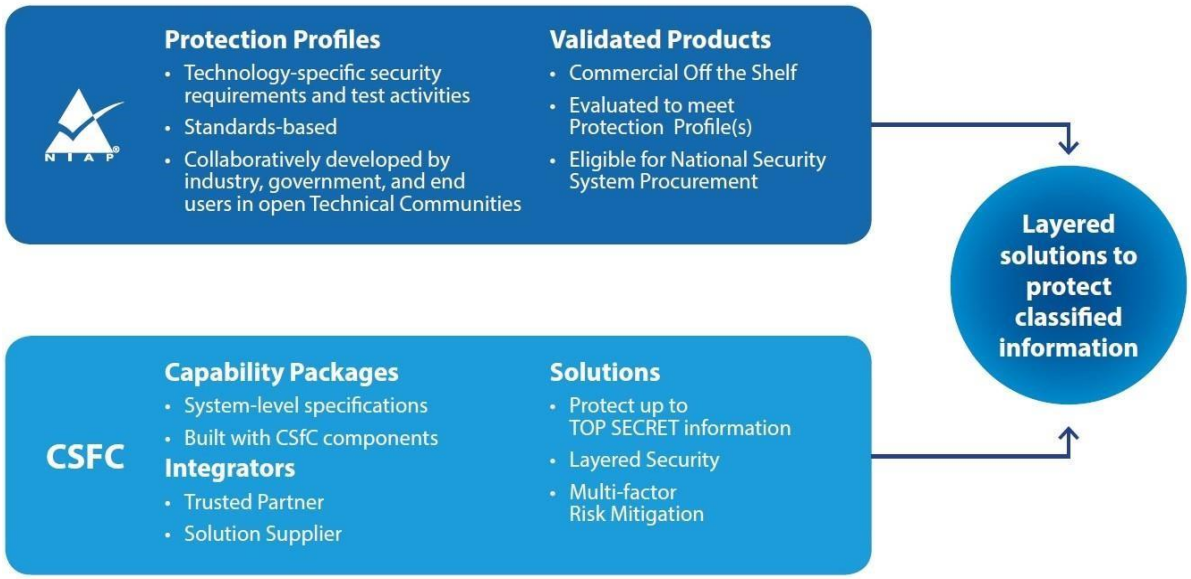
A NIAP validation is the foundational requirement for a product to be included as part of the CSfC program. Vendors who wish to have their products eligible as CSfC components of a composed, layered Information Assurance (IA) solution must build their products in accordance with the applicable NIAP-approved 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 15 May 2023 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 16 May 2023. 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.

NIAP and the CSFC program office held several meetings to coordinate status and requirements to address updates in protection profiles to meet updates in capability packages. CSfC also identified product categories that need additional NIAP tested technologies to allow CSfC customers adequate flexibility in solution architectures. Additional discussions focused on updating processes and tracking of products when they entered evaluation to make sure CSfC requirements were correctly recorded

and tracked. The new NIAP website will look to assist in better tracking NIAP and CSfC dependencies. NIAP and CSfC continue to support and work closely for continued success in both programs.



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 in December 2022. 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. An updated version of the ISO standards is underway to correct errors in the ISO standards with a desired completion date of December 2024.
NIAP has started updating Protection Profiles to be complaint with the 2022 version (CC:2022 and CEM:2022) – CCRA deadline is December 2025.

Looking Forward

2024 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 2024, 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 is still on track to be launching a new web site in the middle of 2024 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 successful completed their Common Criteria Management Committee (CCMC) chair timeline responsibility at the end of 2023. In addition, the spring 2024 CCUF & CCDB meetings will be hosted in Germany while the fall 2024 ICCC and CCRA will be held in Doha, Qatar CCRA. These meetings 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.