NSA CYBERSECURITY

NIAP Overview

JONATHAN ROLF

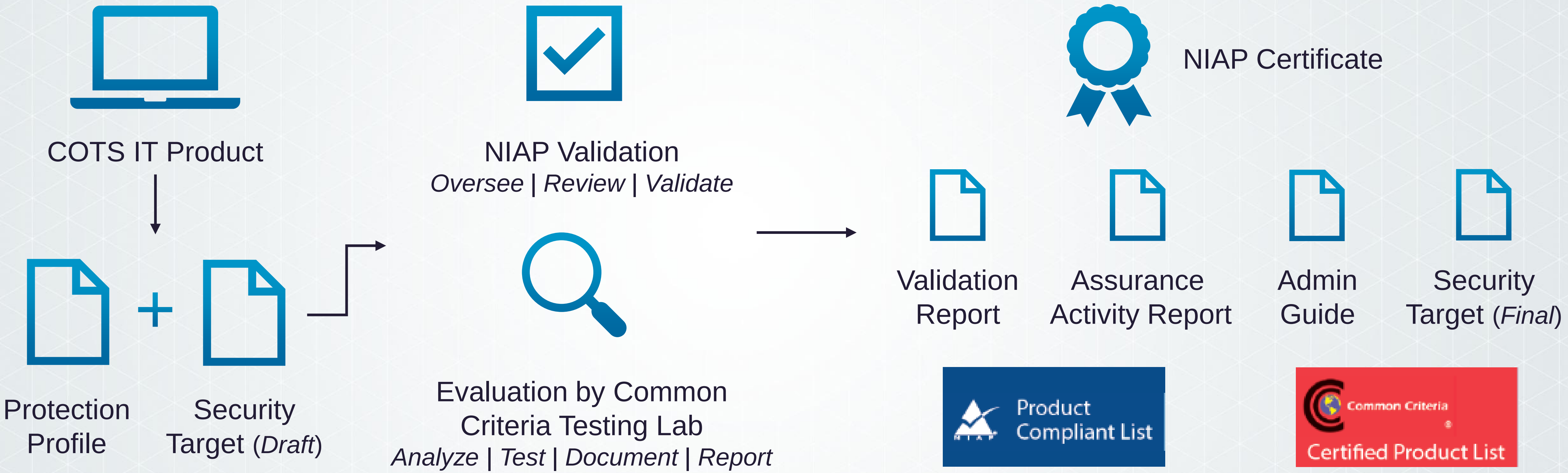
4 DEC 2023

SECURE BY DESIGN/SECURE TO MARKET/SECURE BY DEFAULT

NIAP-CCEVS.ORG

COTS Product Validation

Establish and implement processes to oversee COTS product evaluations under the terms of the Common Criteria Recognition Arrangement to ensure evaluated COTS IT products are available for use in NSS.



COTS IT Product

Protection Profile + Security Target (*Draft*)

NIAP Validation
Oversee | *Review* | *Validate*

Evaluation by Common Criteria Testing Lab
Analyze | *Test* | *Document* | *Report*

NIAP Certificate

Validation Report

Assurance Activity Report

Admin Guide

Security Target (*Final*)

Product Compliant List

Common Criteria Certified Product List

215+ Products & 1000+ Product Configurations

NIAP Portfolio

Mobility

Secure Component

Automation

Encrypted Storage

Computing Platform

Network

Apps

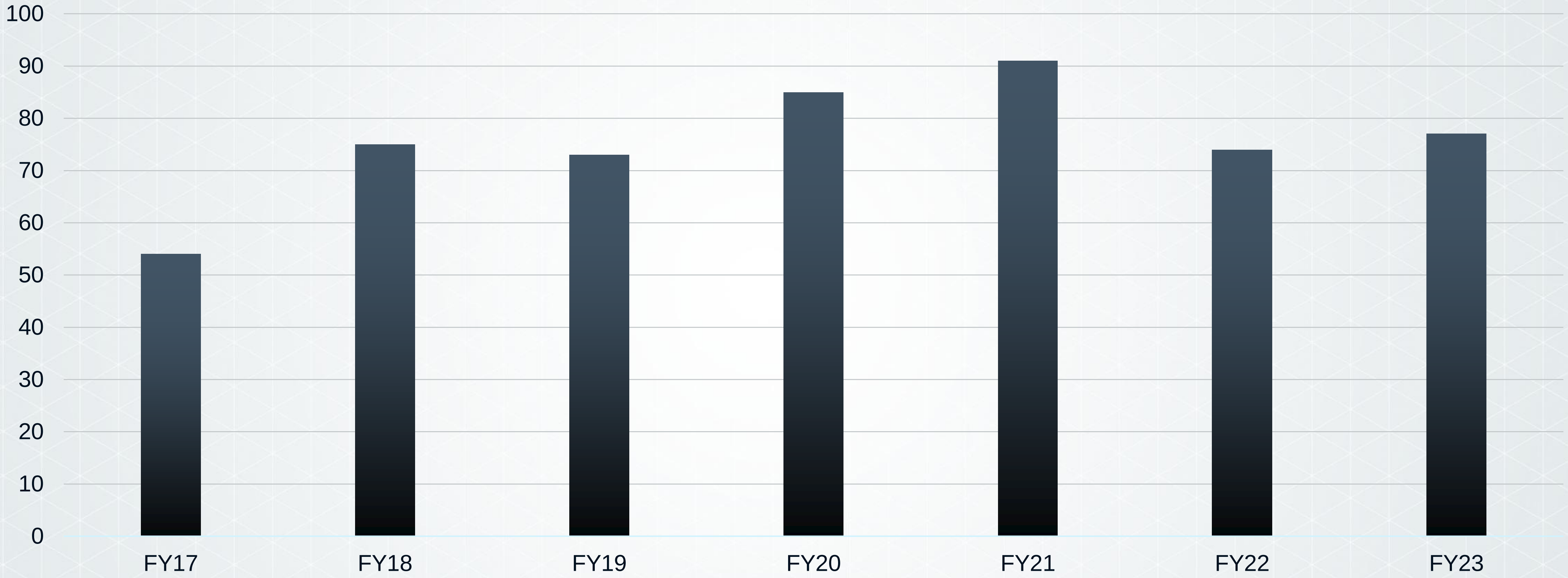
Cloud

Virtualization

Security Mgmt

NIAP-CCEVS.ORG

Total NIAP Evaluations by Fiscal Year



Continued growth of PP coverage and product evaluations

NIAP Today

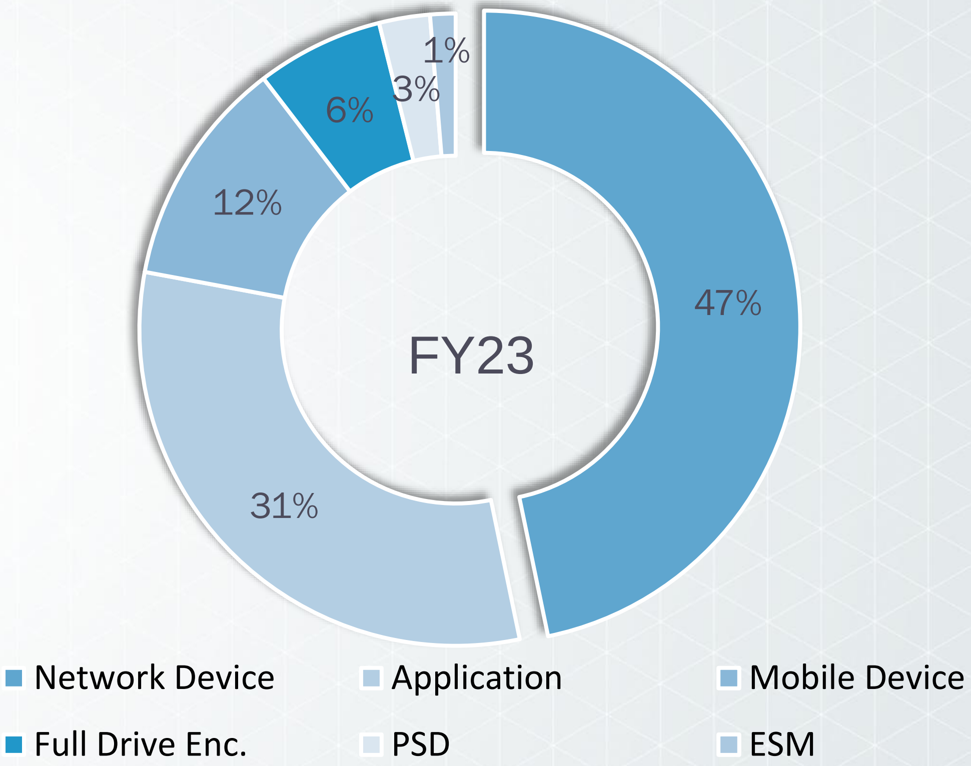
- Mature COTS Product Evaluation for National Security Systems
- Define minimum security requirements for commercial technologies
- Represent US in Common Criteria Recognition Arrangement
- CNSSP 11 Enforcement Mechanism

77
FY23 Product Evaluations

52
Protection Profiles

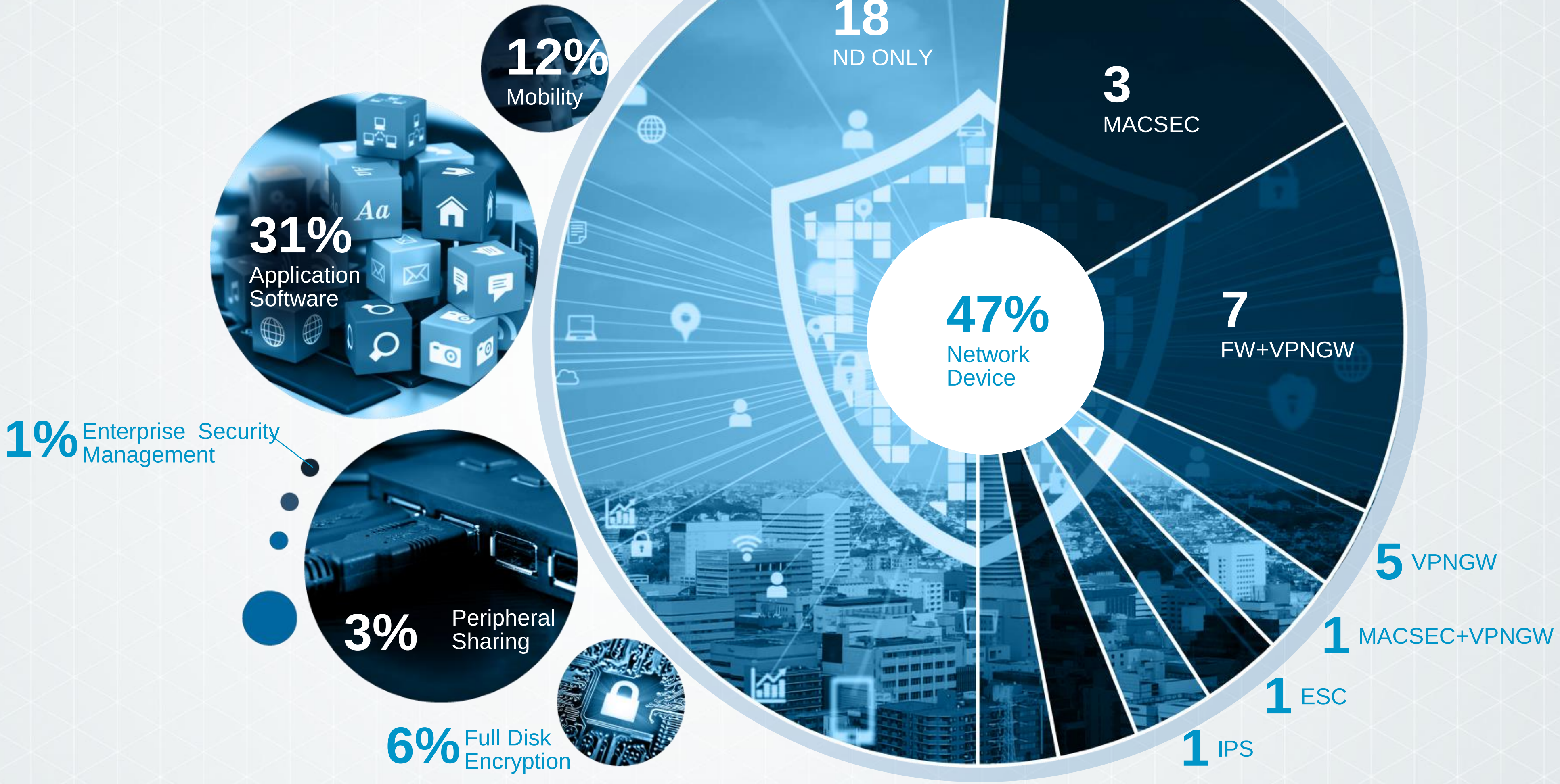
31
Nation Partnerships

FY23 Evaluations by Technology



- 77 Evaluations
- 264 Configurations

FY23 Evaluations by Technology



Represent U.S. in CCRA

Position the U.S. as a leader among Common Criteria Recognition Agreement (CCRA) nations. Further U.S. government and industry objectives to eliminate trade barriers and ensure transparent, meaningful, and repeatable evaluations.

Certificate Producers

- Australia
- Canada
- France
- Germany
- India
- Italy
- Japan
- Malaysia
- Netherlands
- Norway
- Poland
- Qatar
- Republic of Korea
- Singapore
- Spain
- Sweden
- Turkey
- United States

Certificate Consumers

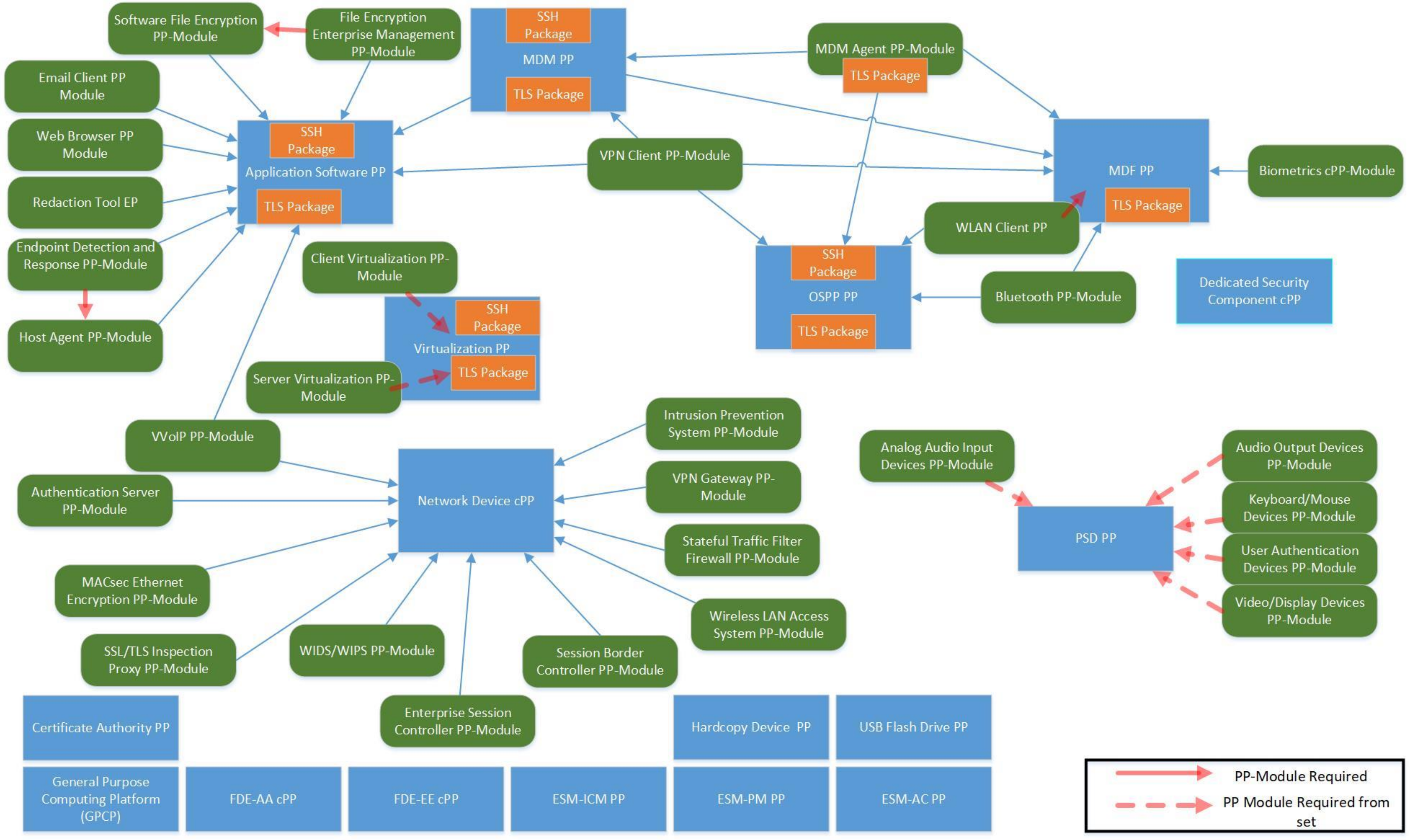
- Austria
- Czech Republic
- Denmark
- Ethiopia
- Finland
- Greece
- Hungary
- Indonesia
- Israel
- New Zealand
- Pakistan
- Slovak Republic
- United Kingdom

Requirements Driving Protection Profile Development (2023)

- Post Quantum updates to algorithms – CNSA 2.0
- International standards updates to all Protection profiles – CC:2022
- Cybersecurity Requirements Updates – Supply Chain, Vulnerability tracking, SSDF, Zero Trust
- Commercial Solutions for Classified Roadmap coordination and product availability - CSfC
- Cloud strategy – Operational Requirements, Whole of government coordination, Industry and International Coordination

- Big Picture drivers: Secure by Design/Secure to Market/Secure by Default

The Inter-connections of PP's


Software File Encryption PP-Module
File Encryption Enterprise Management PP-Module
SSH Package
MDM PP
TLS Package
MDM Agent PP-Module
TLS Package
Email Client PP Module
Web Browser PP Module
Redaction Tool EP
Endpoint Detection and Response PP-Module
Host Agent PP-Module
SSH Package
Application Software PP
TLS Package
VPN Client PP-Module
MDF PP
TLS Package
Biometrics cPP-Module
WLAN Client PP
Client Virtualization PP-Module
SSH Package
Virtualization PP
TLS Package
Server Virtualization PP-Module
SSH Package
OSPP PP
TLS Package
Bluetooth PP-Module
Dedicated Security Component cPP
VVoIP PP-Module
Intrusion Prevention System PP-Module
VPN Gateway PP-Module
Stateful Traffic Filter Firewall PP-Module
Wireless LAN Access System PP-Module
Authentication Server PP-Module
Network Device cPP
MACsec Ethernet Encryption PP-Module
SSL/TLS Inspection Proxy PP-Module
WIDS/WIPS PP-Module
Session Border Controller PP-Module
Enterprise Session Controller PP-Module
Analog Audio Input Devices PP-Module
PSD PP
Audio Output Devices PP-Module
Keyboard/Mouse Devices PP-Module
User Authentication Devices PP-Module
Video/Display Devices PP-Module
Certificate Authority PP
Hardcopy Device PP
USB Flash Drive PP
General Purpose Computing Platform (GPCP)
FDE-AA cPP
FDE-EE cPP
ESM-ICM PP
ESM-PM PP
ESM-AC PP
PP-Module Required
PP Module Required from set

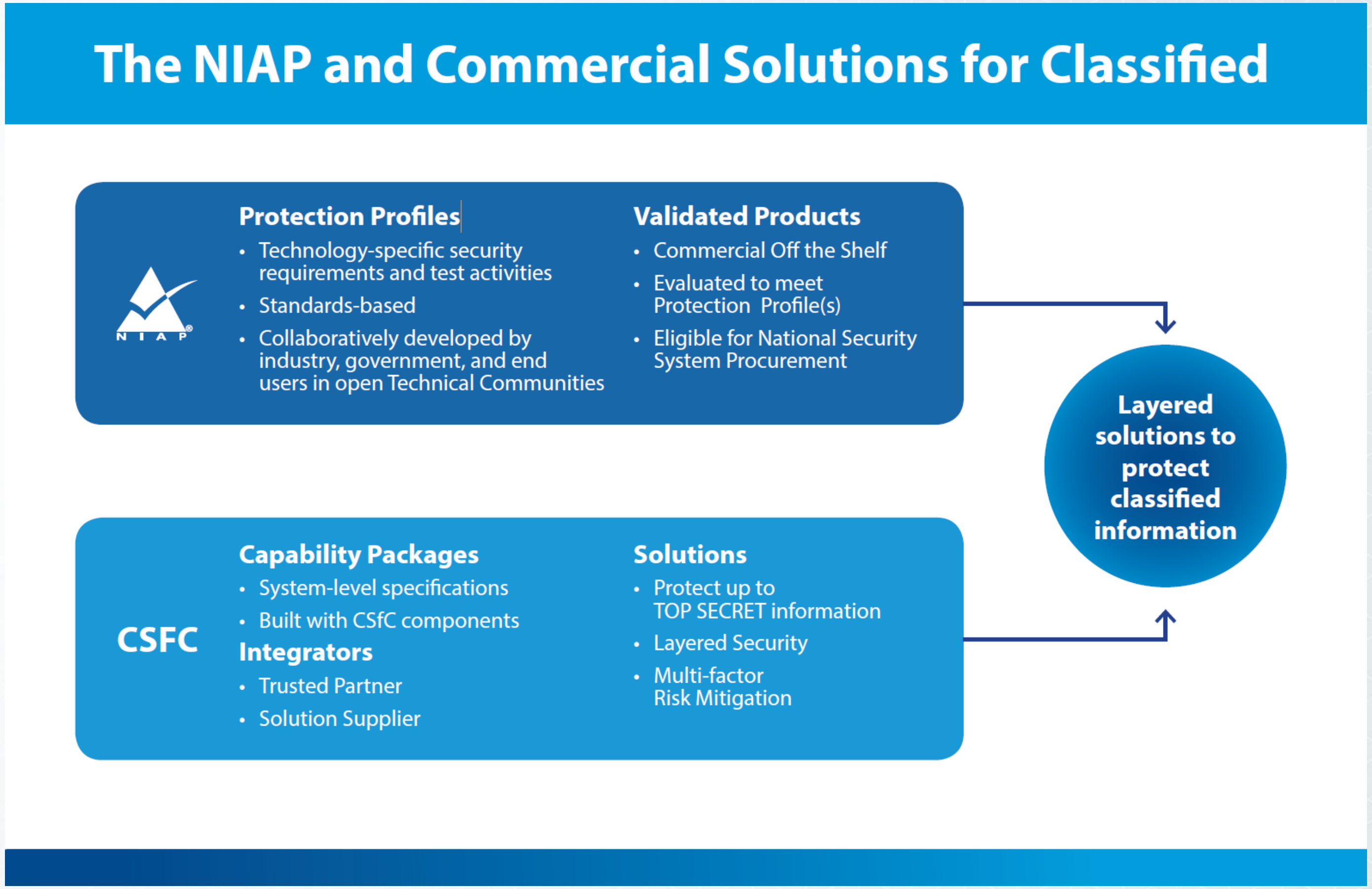
Protection Profile Roadmap

Priorities:

- CC:2022 Conversion
  - App SW Group
  - Mobility Group
  - ND Group
  - PSD Group
  - Virtualization Group
  - Individual PPs
- CNSA 2.0
  - LMS/XMSS
  - CRYSTALS Kyber/Dilithium

Relationship Between NIAP and CSfC

- CSfC enables products on NIAP Product Compliant List to be used in layered solutions to protect classified National Security Systems (NSS).
- After receiving NIAP validation, a vendor follows a separate process with CSfC to obtain approval to be used in CSfC.
- CSfC may require a product to support certain, more secure selections that are only optional for NIAP compliance.
- Approved products are added to the CSfC Components List.



The NIAP and Commercial Solutions for Classified

NIAP

Protection Profiles
- Technology-specific security requirements and test activities
- Standards-based
- Collaboratively developed by industry, government, and end users in open Technical Communities

Validated Products
- Commercial Off the Shelf
- Evaluated to meet Protection Profile(s)
- Eligible for National Security System Procurement

CSFC

Capability Packages
- System-level specifications
- Built with CSfC components

Integrators
- Trusted Partner
- Solution Supplier

Solutions
- Protect up to TOP SECRET information
- Layered Security
- Multi-factor Risk Mitigation

Layered solutions to protect classified information

CNSA 2.0 Overview

Motivation for Transition

NSM-8

Goal: Fortify cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.

- All federal agencies must use NSA-approved cryptography to protect NSS.
- NSA must update CNSSP 15: Use of Public Standards for Secure Information Sharing from CNSA 1.0 to CNSA 2.0 algorithms.
- NSA must provide PQ crypto planning.

NSM-10

Goal: Promote US leadership in quantum computing while mitigating risks to vulnerable systems.

- US must develop partnerships, promote collaboration with industry, academia, and overseas allies.
- NSA must provide guidance on quantum-resistant cryptography migration, implementation, and oversight for NSS.
- NSA must release timeline for deprecation of vulnerable cryptography in NSS.

CNSA 2.0 Overview

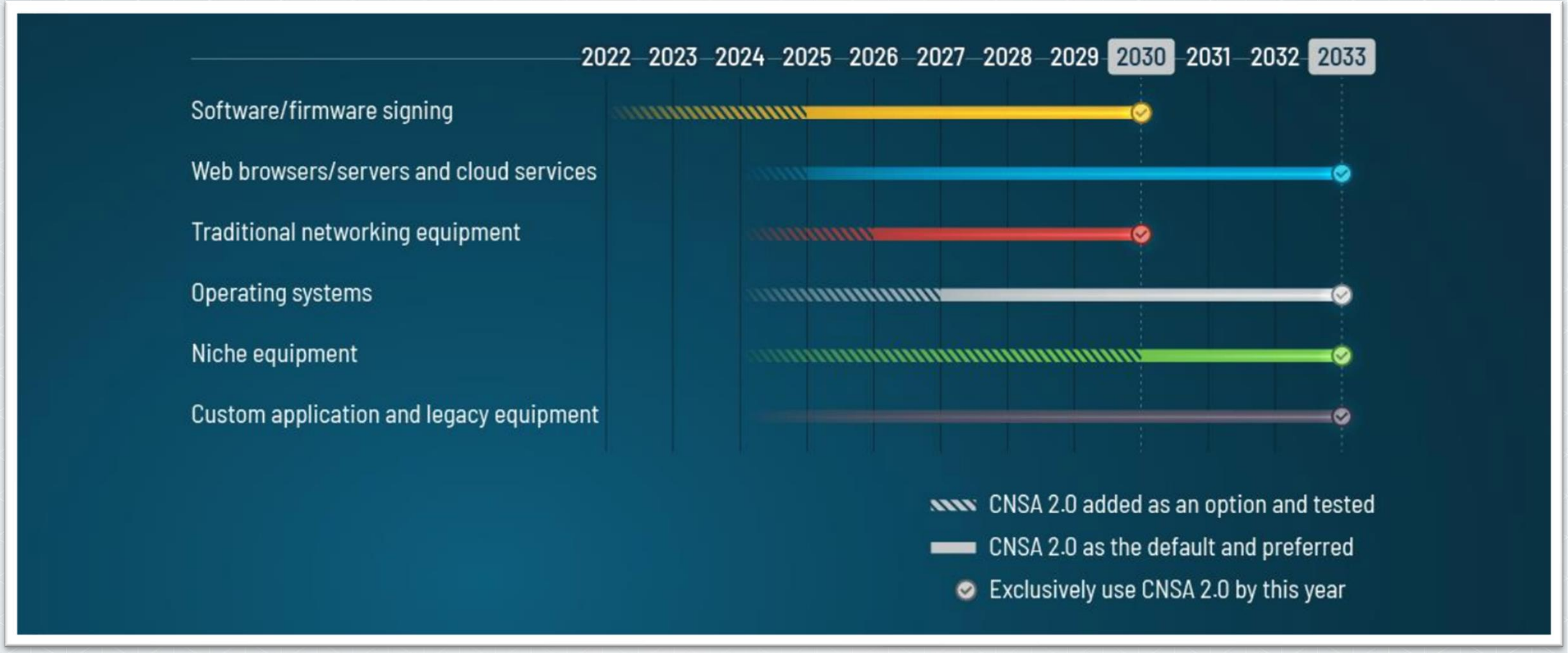
Algorithms

Function	Algorithm	Specification	Use Case	Parameters	CNSA 1.0
Symmetric Key Encryption	AES	FIPS PUB 197	General	AES-256	AES-256
Hash Algorithm	SHA2	FIPS PUB 180-4	General	SHA-384 SHA-512	SHA-384
Digital Signature	Leighton-Micali Signature (LMS)	NIST SP 800-208 RFC 8554	Software and firmware signing	All parameters in SP 800-208*	ECDSA (P-384) RSA (3072 bit min)
Digital Signature	eXtended Merkle Signature Scheme (XMSS)	NIST SP 800-208 RFC 8391	Software and firmware signing	All parameters in SP 800-208*	ECDSA (P-384) RSA (3072 bit min)
Asymmetric Key Establishment	CRYSTALS-Kyber (ML-KEM)	NIST FIPS 203	General	Level V	ECDH (P-384) DH (3072 bit min)
Digital Signature	CRYSTALS-Dilithium (ML-DSA)	NIST FIPS 204	General	Level V	ECDSA (P-384) RSA (3072 bit min)

*All parameters for LMS and XMSS are approved, but use of LMS with parameter SHA-256/192 is preferred.

CNSA 2.0 Overview

Anticipated Timeline



General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes algorithm standard.

1

LMS

- For software and firmware signing
- Standardized by NIST in SP 800-208

2

XMSS

- For software and firmware signing
- Standardized by NIST in SP 800-208

3

CRYSTALS-Kyber (ML-KEM)

- For key establishment
- Draft standard FIPS 203 released by NIST; can expect final standard sometime in 2024
- NIST will publish SP 800-227 on the general properties of KEMs

4

CRYSTALS-Dilithium (ML-DSA)

- For general purpose digital signatures
- Draft standard FIPS 204 released by NIST
- Can expect final standard FIPS 204 sometime in 2024

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. **NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.**

General Process for NIAP Implementation of CNSA 2.0

2. NIST adds support for algorithm to CAVP.

"All cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated (CAVP and/or CMVP). At minimum an appropriate NIST CAVP certificate is required before a NIAP CC Certificate will be awarded." (NIAP Policy Letter 5)

NIAP's CAVP Mapping document will need updates to incorporate the new algorithms.

General Process for NIAP Implementation of CNSA 2.0

2. NIST adds support for algorithm to CAVP.

NIST’s Automated Cryptographic Validation Program (ACVP) should expedite this process.

LMS and XMSS may require Cryptographic Module Validation Program (CMVP) validation in addition to CAVP validation.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. **NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.**

General Process for NIAP Implementation of CNSA 2.0

3. NIAP updates PPs to support use of algorithm.

Algorithm-Specific Updates

The algorithm is added in as a selection to all relevant PPs. This is determined by:

- what type of algorithm it is (encryption vs. authentication), and
- whether it is for general use, or approved only for a specific use case (e.g. software and firmware updates for LMS and XMSS).

SFRs, testing activities, application notes, and more may need to be updated in order to account for additional considerations that arise through use of the algorithm.

Protocol-Specific Updates

SDOs publish new standards documents that update existing standards in order to allow for the use of the new algorithm in a specific protocol standard.

Updates may be made to the CNSA RFC that profiles the protocol in question.

All PPs that use the given protocol need to incorporate updates to align with new SDO documents and CNSA profile.

SFRs, testing activities, threats, assumptions, and more may need to be updated.

In both cases, updates need to be traced through PPs on which revised PPs are dependent (i.e., the dependency a PP-Module has on a base-PP) in order to ensure consistency throughout updates.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.
4. **New equipment must meet the updated Protection Profile requirements in order to be validated; already validated equipment must meet the updated requirements when it is due for its next update in order to remain compliant.**

General Process for NIAP Implementation of CNSA 2.0

4. Equipment must meet updated PP requirements in order to be validated or remain compliant.

New equipment:

- Equipment that has not yet been validated must meet the updated Protection Profile requirements in order to be validated.

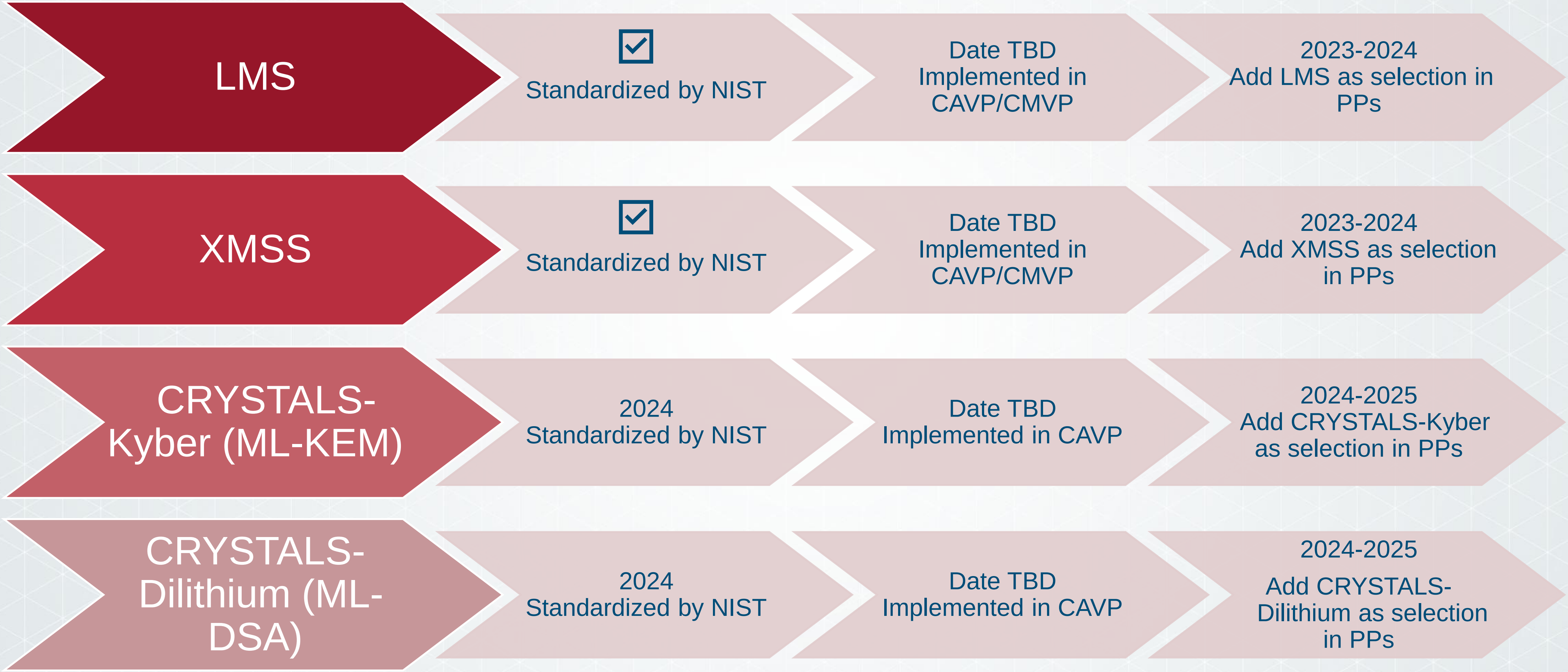
Already validated equipment:

- Equipment that has already been validated must meet the updated Protection Profile requirements when it is due for its next update in order to remain compliant.
- NIAP certifications typically last for two years with the possibility of an additional year.
- Certifications for some technologies may last for up to five years (e.g. Peripheral Sharing Devices).
- For more information on the re-evaluation process, see NIAP-CCEVS Publication 6, Assurance Continuity: Guidance for Maintenance and Re-Evaluation.

General Process for NIAP Implementation of CNSA 2.0

1. NIST publishes the specification of an algorithm.
2. NIST adds in support for the algorithm to their Cryptographic Algorithm Validation Program.
3. NIAP updates the relevant Protection Profiles to include the newly-standardized algorithm as the preferred configuration option.
4. New equipment must meet the updated Protection Profile requirements in order to be validated; already validated equipment must meet the updated requirements when it is due for its next update in order to remain compliant.
5. **After some time, non-CNSA 2.0-approved algorithms will be removed as options from Protection Profiles.**

Predicted Timeline for Adding Algorithms to PPs



LMS	☑ Standardized by NIST	Date TBD Implemented in CAVP/CMVP	2023-2024 Add LMS as selection in PPs
XMSS	☑ Standardized by NIST	Date TBD Implemented in CAVP/CMVP	2023-2024 Add XMSS as selection in PPs
CRYSTALS-Kyber (ML-KEM)	2024 Standardized by NIST	Date TBD Implemented in CAVP	2024-2025 Add CRYSTALS-Kyber as selection in PPs
CRYSTALS-Dilithium (ML-DSA)	2024 Standardized by NIST	Date TBD Implemented in CAVP	2024-2025 Add CRYSTALS-Dilithium as selection in PPs

NIAP Cryptographic Technical Community

Support Efforts to Update PPs

- Members can provide technical input to the development and maintenance of cryptographic Security Functional Requirements (SFRs).
- TC is focused on incorporating quantum-resistant algorithms from CNSA 2.0 into Protection Profiles.
- First round of updates will enable use of LMS and XMSS stateful hash-based digital signatures for software and firmware signing.
  - Incorporate requirements into Protection Profiles, beginning with Application Software, General Purpose Operating System, and Mobile Device Fundamentals.
  - Make recommendations for collaborative Protection Profiles, beginning with Network Device and Dedicated Security Component.
- Future updates will add support for CRYSTALS-Kyber (ML-KEM) for key establishment, and CRYSTALS-Dilithium (ML-DSA) for digital signatures.
- The TC is open to all participants.

References

- CNSA Suite 2.0 Cybersecurity Advisory
- CNSA Suite 2.0 FAQ
- NIST SP 800-208
- CNSSP 15
- CAVP Mapping
- NIAP Policy Letter 5
- NIAP-CCEVS Publication 6
- NSM 8
- NSM 10
- Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process
- RFC 7383, IKEv2 Message Fragmentation
- RFC 9242, Intermediate Exchange in IKEv2
- RFC 9370, Multiple Key Exchanges in IKEv2

How to Contribute

- Technical Communities
- Common Criteria User Forum
- GitHub site: https://github.com/commoncriteria

For More Information…

Visit the NIAP Website: www.niap-ccevs.org

Contact Us via E-mail: niap@niap-ccevs.org

CCRA: www.commoncriteriaportal.org