IDS WG Meeting Minutes
December 1, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on December 1, 2022.

Attendees

Jerry Colunga	HP
Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Ira McDonald	High North
Alan Sukert	
Mike Trent	Xerox
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
    - Al’s debrief of the 22nd (Fall 2022) CCUF Workshop and the International Common Criteria Conference (ICCC) both held in Toledo Spain
    - Special topic on Commercial National Security Algorithm (CNSA) Suite 2.0
    - Round Table
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al started with his debrief of the 22nd (Fall 2022) CCUF Workshop that was held November 8. 9 10 & 14, 2022 in Toledo Spain. A summary of what was covered at the workshop can be found in the following slide: https://ftp.pwg.org/pub/pwg/ids/Presentation/22nd CCUF Workshop _Closing_WrapUp__20221114_Kwangwoo.pdf. The key points presented at the workshop were:
    - The central theme of the Workshop was that “change is coming”. Among the changes that will be happening in the near future:
        - Certifications will be more automated
        - European Union Cybersecurity Certification (EUCC) is coming (much more on this later)
        - The revisions to ISO/IEC 15408 and ISO/IEC 18504 (the CC and the CEM) are complete and published by ISO.
        - FIPS 140-3 is being implement into CAVP (Cryptographic Algorithm Validation Program)
        - SOG/IS in the EU is being transformed into the EUCC
    - The status of the HCD iTC was presented at the workshop. Of course, the main point was that HCD cPP v1.0 and HCD SD v1.0 were both published with a 10/31/2022 date. The other big point was that the HCD Interpretation Team (HIT) is being established.

      The next big step will be getting Position Statements from the various Schemes. We know we will get Position Statements from NIAP, JISEC and ITSCC, but we may also get Position Statements from some European Schemes such as Italy.
    - One of the ITCs we are following closely is the Network Device (ND) iTC. The ND iTC released for public review ND cPP 3.0 on 10/3/2022; they expect to publish ND cPP v3.0 around the end of

January 2023. Some of the key things that will be in ND cPP v3.0 from an HCD iTC perspective are:

  - Inclusion of TLS 1.3 and the deprecation of TLS/DTLC 1.1
  - Adding as an optional assurance requirement ALC_FLR.
  - Replacing the current SSH requirements with the NIAP SSH Package
  - Removal of support for published hash. Note thar Al didn't think the HCD cPP had any published hash requirements but Jerry thought it did – will have to investigate that further

- The CCDB as part of the Joint CCDB-CCUF session on Thursday stated that it will be providing an Assurance Package for ALC_FLR for any iTC/TC to use. Note that NIP indicated they are doing the same thing. It also stated that it is actively working on an Implementation Act with EUCC for mutual recognition.
- The HCD iTC held an iTC meeting at the workshop. The key topics covered at the meeting were:
  - Kwangwoo stated that input from the Stakeholders (JISEC and ITSCC as well as NIAP) was very helpful in getting the HCD cPP and HCD SD published
  - The main part of the meeting discussed the HIT. It was noted that the ND Interpretation Team has 12 members on it; Al thought that 10 might be a good upper limit for the HIT.

    The other thing related to the HIT was that we are probably going to use GitHub and Issues to manage the HIT Requests for Interpretation (RfIs).

    Also, the plan is to have the HIT in place and functioning by the end of February 2023. Events such as CNSA 2.0 (see later in these minutes) may force that timeline to be accelerated.
  - The meeting ended with a discussion of future HCD cPP/SD releases. We agreed that the next release will be a minor release (v1.1) but the question is how soon after v1.0 is published should the next release be. It was mentioned that the ND iTC does minor releases approximately once a year. Also, the ND iTC generally does major releases every 2-3 years; the major releases are basically feature releases with a certain unspecified volume of other changes included.

    During the future release discussion, it was mentioned that one issue the NIT has is that NIAP does not always approve every Technical Decision (TD) that the NIT approves. That forces them to keep two baselines – one with all the NIT TDs included and one with just the NIT TDs that NIAP approves. The HIT may face the same issue, which would mean we would have to have two branches – the mainline branch with all the TDs and a 'NIAP branch' with only the TDs approved by NIAP. Jerry asked a good question as two which of the two baselines the ND iTC published in ND cPP v3.0; Al said he would ask the ND iTC which baseline they published because he didn't know.
- The next important presentation at the CCUF Workshop was the ISO Update on the status of the changes to ISO/IEC 15408 (the CC standard) and ISO/IEC 18045 (the CEM - Common Methodology for Information Technology Security Evaluation). It is important to note that at the time of this presentation on Nov 14th, the new versions of the CC standard and the CEM had not been officially announced.

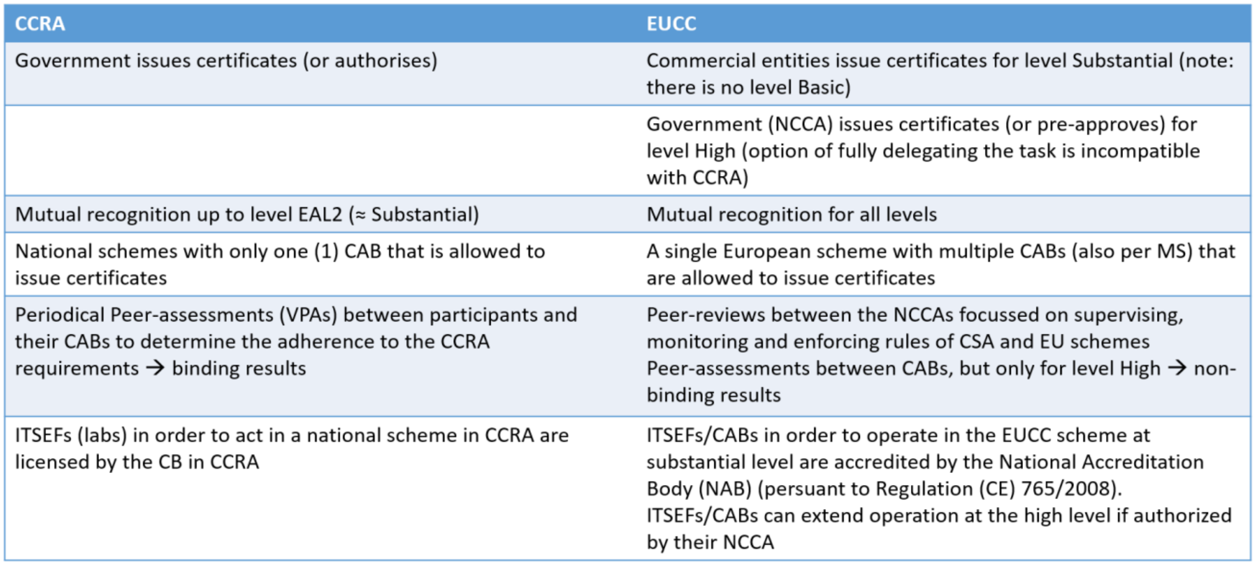
  The current ISO/IEC 15408 is the 3rd Edition (v3.0R5); the new ISO/IEC 15408 will be the 4th Edition; the new CEM will be the 3rd Edition of that document. ISO had approved and published both documents earlier in Aug 2022, which were now available on the ISO website for a price. The problem was that the ISO version of both documents had not yet been approved by the CCRA which was necessary for the new updated versions to be posted on the Common Criteria portal. Also, there was still a copyright issue with ISO that needed to be resolved so the two updated standards could be made available for free to anyone who needed them.

  The ISO JTC 1/SC 27/WG3 will now be responsible for update and maintenance of the two CC standards at the request of the CCDB which previously had that responsibility. The CCUF has a liaison status with WG3 that will allow CCUF members to provide comments on any future updates.

- The final key presentation at the CCUF Workshop was on EUCC. The actual presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/2022-11-14-ccuf-eucc.pdf. The key points from the presentation were:
  - EUCC emanates from the 2019 EU Cybersecurity Act (CSA). This act provides a common framework for EU-wide cybersecurity schemes that are based on standards. Right now, there are three schemes in the EU – EUCC, EUCS and EU5G. EUCC will represent all EU countries. The current draft version of EUCC is EUCC 1.1.1, but the final version that is implemented will likely be different.
  - As stated above, EUCC is categorized as a Scheme – the first one based on the CSA.EUCC will be based on ISO/IEC 15408 and the CC, but will require inclusion of the ALC_FLR Flaw Remediation and AVA-VAN Vulnerability Analysis Security Assurance Requirements (SARs). EUCC will also inherit the technical domains of SOG/IS (see https://sogis.org/index_en.html) and will pertain to products such as smartcards and similar devices in addition to Hardware devices with "security boxes".
  - Right now, CSA is voluntary but other EU regulations that will be discussed below may change that. The infrastructure that CSA sets up and is reflected in EUCC is that each EU member nation sets up a National Cyber Certification Authority (NCCB) that is similar to a nation Scheme in CC like NIAP. Each NCCA will implement one or more
    - Conformity Assessment Bodies (CABs) that is accredited per ISO/IEC 17065 and which actually generate the certificates for a product being certificate
    - One or more ITSEFs (i.e., Evaluation Labs) that are accredited per ISO/IEC 17025 and which perform the evaluations needed to obtain a certificate
  - EUCC is based on two assurance levels - High Assurance which equates to EAL3 and above and Substantial Assurance which equates to EAL2. What is different in EUCC from CC is that certifications done at the Substantial Assurance level are done by private CABs such as evaluation labs; only certifications done at High Assurance can be done by CABs under the auspices of SOG/IS. One thing the EU is trying to beef up in EUCC is to speed up the certificate maintenance process via including patch management requirements. Another area that EU wants to beef up in EUCC is vulnerability handling and disclosure.
  - EUCC implementation is still pending; it is probably a year away; once EUCC is implemented there will be a 1-year transition until EUCC becomes mandatory and SOG/IS will be sunset. That means any ITSEFs accredited under SOS/IS will become accredited under EUCC.
  - As stated above there are other EU Regulations that will impact EUCC and the time frames to implement it:
    - NIS2 (Network and Information Security) is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. NIS2 may require that all Information and Communications Technology (ICT) products be certified per the CRA.
    - The EU Cyber Resiliency Act (CRA) is a new regulation that applies to all digital products sold in the E. CRA. The goal of the CRA is to ensure the cybersecurity of digital products. The CRA provides essential requirements for design and development, and contains strong requirements on vulnerability handling and reporting a well as on design and development. The CRA requires that digital products be certified per the CSA and is based on the concept of "design by default".
    - There is also a new EU regulation that deals with semiconductor chips that likely won't impact HCDs.

The key will be how EUCC will be able to show compliance to CRA.

- The table below that was presented at the CCUF Workshop provides a good summary of the differences between CC and EUCC



CCRA	EUCC
Government issues certificates (or authorises)	Commercial entities issue certificates for level Substantial (note: there is no level Basic)
	Government (NCCA) issues certificates (or pre-approves) for level High (option of fully delegating the task is incompatible with CCRA)
Mutual recognition up to level EAL2 (≈ Substantial)	Mutual recognition for all levels
National schemes with only one (1) CAB that is allowed to issue certificates	A single European scheme with multiple CABs (also per MS) that are allowed to issue certificates
Periodical Peer-assessments (VPAs) between participants and their CABs to determine the adherence to the CCRA requirements → binding results	Peer-reviews between the NCCAs focussed on supervising, monitoring and enforcing rules of CSA and EU schemes Peer-assessments between CABs, but only for level High → non-binding results
ITSEFs (labs) in order to act in a national scheme in CCRA are licensed by the CB in CCRA	ITSEFs/CABs in order to operate in the EUCC scheme at substantial level are accredited by the National Accreditation Body (NAB) (persuant to Regulation (CE) 765/2008). ITSEFs/CABs can extend operation at the high level if authorized by their NCCA

The key differences are:

- The fact that certificates at the Substantial Level in EUCC are done by commercial entities and not be the OG/IS CABs whereas all certificates in CC are done by the National Schemes
- The EU has mutual recognitional at all EAL levels while the current CCRA on addresses mutual recognition at EAL2 or below
- EUCC allows multiple CABs for each nation while for CC each nation only has the one Scheme that is responsible for implementing the CC for that nation

- One last point – an important issue going forward will be how the CCRA can arrange mutual recognition with the EUCC given that commercial bodies can issue certificates for Substantial– essentially at EAL2 or below - which is what the current CCRA covers.

4. Al then did with his debrief of the ICCC 2022 that was held November 15-17, 2022 in Toledo Spain. The conference agenda can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/ICCC2022 Conference Agenda.pdf. The key points that Al got from the various presentations he attended were:

- It was reported at the beginning of ICCC 2022 that the CCRA had worked out the copyright issue with ISO and had accepted the wording of the ISO versions of the updated ISO/IEC 15408 and ISO/IEC 15804 and had aligned the technical content. The updated standards, dubbed CC2022, was posted on the Common Criteria portal and available to everyone to download as of Monday, Nov 14th.
    - In CC2022, the CC now consists of 5 parts plus the CEM instead of 3 parts plus the CEM in CC3.1R5. The 5 new parts are:
        - Part 1 – Introduction and General Model (same as CC3.1R5)
        - Part 2 – Security Functional Components (same as CC3.1R5)
        - Part 3 – Security assurance components (similar to CC3.1R5 but EALs moved to Part 5)
        - Part 4 - Framework for the specification of evaluation activities and methods (new)
        - Part 5 – Pre-defined packages of security requirements (new)

  - The criteria for transition to CC2022 is:
    - CCV3.1R5 (the current version) is the last from the 3.1 series, and may optionally be used for evaluation starting no later than the 30th of June 2024. Certifications after 6/30/2024 have to use CC2022 for evaluation.
    - STs conformant to CC:2022 based on PPs certified according to CC3.1 will be accepted up to the 31st of December 2027. This means that a ST written against the requirements in CC2022 that is conformant to a PP (or cPP) that was developed based on the CCV3.1R5 version of ISO/IEC 15408 can be certified up to 12/31/2027; after that STs can only be conformant with PPs and cPPs that have been developed or modified to be compliant with CC2022.
    - Assurance continuity activities (maintenance, re-evaluation and re-assessment) based on CC 3.1 evaluations can be started for up to 2 years from the initial certification date. This implies that assurance continuity activities based on CC2022 will follow the normal 5-year limit.
- The CCDB is still working with the CCDB to simplify the iTC process. Al note that this work has been going on for 2 years now with still no indication when it will be completed
- Some key points from the NIAP presentation:
  - NIAP will be drafting an ALC_FLR package to address the EUCC requirement. NIAP is also working on packages for IPsec, X.509 certificates, and TLS.
  - NIAP is looking into expanding PP work in services and the cloud
  - NIAP wants to build a library of crypto SFRs so they can become standard in NIAP PPs
  - In 2023 NIAP will be focusing on
    - Help the CCRA with its efforts to get mutual recognition with EUCC
    - Develop standards for SBOMs and HBOMs so NIAP knows exactly what is in each product that is being certified
    - Revamping the NIAP and CC websites – NIAP is responsible for the CC portal
    - Quantum Resistance algorithms to support rollout of CNSA 2.0 (see that topic later in the notes)
    - Transitioning to CC2022
- Al noted that since the ICCC was in Spain, there was a lot of attention paid to EUCC at the conference; Al guessed that at least 1/3 of the presentations were related to EUCC in some way. The presentation that Al attended ion EUCC made the following points:
  - An important issue for EUCC is “harmonization”. This means getting all the EU countries to buy-in to EUCC through per reviews of the NCCAs, peer assessments of the CABs and strict requirements for vulnerability assessment. One goal is to harmonize on crypto evaluation procedures, although there is no plan to do certifications specific to cryptography.
  - As stated at the CCUF Workshop, the EU is struggling with the Implementations Act for EUCC. The guidance document for EUCC has been submitted for review. The EU is shooting for 1Q 2023 for adoption of the EUCC Implementation Act.
  - The plan is that 1 year after certification of the EUCC for High Assurance, evaluations against EUCC will start.
  - High Assurance in EUCC translates to vulnerability assessment per VAN.4 and VAN.5; Substantial Assurance in EUCC translates to vulnerability assessment per VAN.1 and VAN.2

  - Work on EUCC is now focused on developing (1) the Implementation Act, (2) the maintenance strategy for EUCC and (3) a catalogue of National CABs.
  - ENISA has a web site dedicated to EUCC
  - The new regulations like CRA will put the following requirements on vendors:
    - STs must have AVA_VAN, AKLC_FLR and ATE_IND
    - Existing SOG/IS technical domains will be kept once SOG/IS is sunset
    - Will have to provide a description of their vulnerability handling resolution process
    - There will be no substitution from the certificate version
  - Just like for CC, EUCC certificates will have a 5-year limit
  - EU is working on establishing mutual recognition with 3rd countries
  - CABs will be accredited per ISO/IEC 17065; ITSEFs will be accredited per ISO/IEC 17025 and ISO/IEC 23532-1 and will be good for 3 years.
- There were several other interesting presentations that Al attended, but because of time constraints at this meeting he didn't go into detail on any of them. However, there were a couple of presentations dealing with Quantum Crypto and Post Quantum Cryptography (PQC) which is becoming a big topic thanks to the CNSA 2.0 announcement which Al covered as a special topic at this meeting.

  PQC will affect all products and any PP or cPP that depends on TLS and crypto, The CCRA will have to determine how PQC will impact CC and issues like requirements for TLS session key generation. For example, PQC algorithms need more quality entropy bits that conventional crypto algorithms. NIST is working on standards for PQC algorithms that cannot be compromised by quantum computers.

5. Al then presented this week's special topic on Commercial National Security Algorithm (CNSA) Suite 2.0. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CNSA 2.0.pdf.

   The main items covered in the presentation were:

- CNSA 2.0 was released by NSA in Sep 2022. The purpose of this release was to address the future deployment of a cryptanalytically relevant quantum computers (CRQCs) would break public-key systems used today. The time frame for when this could happen varies with the person making the prediction, but most exports feel this could happen within the next 15 years. So, NSA needs to plan, prepare, and budget now for an effective transition to quantum-resistant (QR) algorithms to assure continued protection of National Security Systems (NSS) and related assets.
- CNSA 2.0 Is an update to CNSA 1.0 Algorithms and applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified National Security Systems (NSS). In addition, per CNSSP 11, software and hardware providing cryptographic services require NIAP or NSA validation in addition to meeting the requirements of the appropriate version of CNSA.
- The current CNSA 1.0 algorithms supported by NSA are in the table below:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256-bit keys to protect up to TOP SECRET

Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

- The algorithms that are part of CNSA 2.0 are as follows”
  - For Software and Firmware Signing, NSA chose separate algorithms because:
    - NIST has standardized these algorithms already, while other post-quantum signatures are not yet standardized,
    - This signature use-case is more urgent, and
    - This selection places algorithms with the most substantial history of cryptanalysis in a use case where their potential performance issues have minimal impact.

  The algorithms chosen for software- and firmware-signing are those specified in NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes and are:

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.

Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

NSA originally recommended LMS but now indicates that both algorithms are equally effective

- For Symmetric Keys the chosen algorithms are:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

- For General-use Public Key algorithms, the selected algorithms are:

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.

It was noted that neither of these algorithms have final standards nor Federal Information Processing Standard (FIPS)-validated implementations available at this time, but were selected now so vendors could begin building toward these requirements, and so acquisition officials and NSS owners and operators will know what the requirements are.

It was also noted that this effectively deprecates the use of RSA, Diffie-Hellman (DH), and elliptic curve cryptography (ECDH and ECDSA) when mandated, which will have a significant affect on any PP or cPP that requires any of these three cryptographies (such as the HCD cPP).

- The transition plan noted in the CNSA 2.0 announcement for the algorithms above is:
  - The timing of the transition depends on the proliferation of standards-based implementations
  - NSA expects the transition to QR algorithms for NSS to be complete by 2035 in line with NSM-10. NSA urges vendors and NSS owners and operators to make every effort to meet this deadline.
  - Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period.

    - When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases

  - NIAP's general transition plan for CNSA 2.0 is:

    - NIAP will release protection profiles specifying that products support CNSA 2.0 algorithms in accordance with NIST and other standards

    - All new equipment must meet the requirement at its next protection profile requirements update to remain NIAP; older compliant

    - Using CNSA 2.0 algorithms as the preferred configuration option will begin as soon as validated and tested solutions are available and implemented in CAVP

    - NIAP Protection Profile requirements and NSM-10 technology refresh requirements will determine the removal of legacy algorithm support

    - At that point, legacy equipment and software not refreshed regularly will require a waiver and a plan to bring it into compliance

    Al noted that he had attended a meeting earlier in the week where NIAP laid out in more detail its transition plan. The main parts of the plan are:

    - CNSA 1.0 algorithms must be include in all NIAP approved PPs (i.e., PPs that are developed under the auspices of NIAP; this is not refer to cPPs developed by iTCs and approved by NIAP). NIAP PPs can not include any crypto algorithms below CNSA 1.0.

    - SHA-512 requirements will be added to all NIAP PPs

    - Eventually the requirement will be changed to requiring either CNSA 1.0 or CNSA 2.0 algorithms

    - NIAP's implementation plan for the two Software and Firmware Signing algorithms are (1) LMS in 1st half of 2023 and (2) XMSS in the 2nd Half of 2023.

    - Regarding asymmetric algorithms, CNSA 2.0 key establishment algorithms will be mandated in all NIAP PPs as soon as they are standardized, adequate Assurance Activities have been developed and CAVP has been appropriately updated.

    - NIAP will eventually deprecate CNSA 1.0, but that isn't likely to happen until the 2030 – 2033 timeframe. NIAP currently has no timeline for making CNSA 1.0 mandatory in NIAP PPs.

    - At some point (no timeline was given) NIAP will engage iTCs on rolling CNSA 2.0 into NISP-approved cPPs. NIAP is also in discussions with the CCRA on how to integrate CNSA 2.0 into cPPs. Finally, NIAP will work with vendors to try to meet the NSA schedule for transition to CNSA 2.0, although they admitted it is likely the NSA schedule will probably have to be stretched out.

    - NIAP did indicate that at some point (again no timeline was provided) cPPs and PPs will have to have CNSA 2.0 algorithms as requirements to be on the Product Compliant List (PCL).

- Al then provided some NSA guidelines on how vendors, labs, etc. can prepare for CNSA 2.0:

  - AES-256, SHA-384, SHA-512, and the NIST hash-based signatures listed in NIST SP 800-208 are considered safe against attack by a large quantum computer

  - Should begin implementing other quantum-resistant algorithms NIST and NSA chose as soon as possible and provide feedback about any issues they discover

  - CNSA 1.0 Suite continues to represent the interim strategy as the commercial space transitions to the algorithms in CNSA 2.0

  - NSA encourages vendors to use CNSA 2.0 approved hash-based signatures for software- and firmware-signing
  - NSA does not approve using pre-standardized or non FIPS-validated CNSA 2.0 algorithms (even in hybrid modes) for NSS missions
  - NSA recommends limited use of pre-standardized or non-FIPS-validated CNSA 2.0 algorithms and modules in research settings to prepare for the transition
  - NSA requests vendors begin preparing to implement CNSA 2.0 algorithms so they are primed to provide products soon after NIST completes standardization and development of the applicable Assurance Activities
- The complete list of CNSA 2.0 algorithms is below:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

6. Round Table:

Some upcoming events in 2023:

- **ISO/IEC 19790 Cryptographic Module Day 2023**
27 March | Brussels Hotel Marriott Grand Place
www.CryptoMod.org
- **The International Conference on the EU Cybersecurity Act 2023**
28-29 March | Brussels Hotel Marriott Grand Place
www.EUCyberAct.org

- **Post-Quantum Cybersecurity Day 2023**
  May 15 | Westin Arlington Gateway
  www.PQCyber.org
- **Cybersecurity Maturity Model Certification (CMMC) Day 2023**
  May 15 | Westin Arlington Gateway
  www.CMMCDay.org
- **CSfC Conference 2023**
  May 16 | Westin Arlington Gateway
  www.CertInfoSec.org
- **The International Cryptographic Module Conference 2023**
  September 14-16 | Shaw Centre, Ottawa, Ontario, Canada
  www.ICMConference.org
- **The International Common Criteria Conference 2023**
  October 31-November 2 | Marriott Metro Center, Washington DC
  www.ICCConference.org

7. **Actions:** None

Next Steps

- The next IDS WG Meeting will be December 15, 2022 at 3:00P ET / 12:00N PT. Main topic will be a special topic (likely the EU Cyber Resiliency Act). It will be the last meeting in 2022.
- The next PWG Face to Face Meetings will be February 7-9, 2023. The IDS Session will likely be on February 9th from 10A – 12N ET.