IDS WG Meeting Minutes
July 27, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on July 27, 2023.

Attendees

Graydon Dobson	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD iTC and the HCD Interpretation Team (HIT)
   - An update on the EU Cybersecurity Act
   - Special Topic on the proposed update to NIST SP 800-171r3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
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 began discussing the results of the July 17th HCD iTC Meeting.

   There are four sets of reviews going on with respect to the HCD cPP v1.0 and HCD SD 1.0. NIAP is reviewing the HCD cPP and has submitted comments to the HIT that were discussed at a previous IDS WG Meeting. Also, Lexmark is certifying an HCD against HCD cPP/SD v1.0 using the Canadian Scheme, and as part of the Canadian Scheme's evaluation activities it reviewed the HCD cPP and submitted comments to the HIT. Kwangwoo Lee mentioned that several Schemes are reviewing the HCD cPP, so we may see more comments at some point. Finally, the Common Criteria Development Board (CCDB) is reviewing the HCD SD per the current iTC Development Process, so we may see some comments from that review also. The bottom line is that we may see several more comments from these Scheme reviews than we have received already.

   Kwangwoo mentioned that the next CCDB Meeting is at the end of October 2023 and we may see some more Endorsement Statements for the HCD cPP/SD v1.0 at that time; right now, only the Canadian Scheme has endorsed the HCD cPP/SD v1.0.

   Al then went into the issues that the HCD iTC has to face in the coming year in terms of what content might have to go into the next or future versions of the HCD cPP and HCD SD.

   a. The CCDB issued a draft Specification of Functional Requirements for Cryptography , Version 0.1 that went out for review and comment by July 31, 2023. This draft specification, which Al has denoted as the "Crypto Spec", contains versions of many key Crypto SFRs that are commonly used in PPs and cPPs. Some of the versions in the Crypto Spec are taken from CC:2022; some are taken from other sources.

      Al did a comparison between the SFRs in the Crypto Spec against the corresponding SFRs in the HCD cPP which he went through quickly at the meeting; this comparison can be found at Crypto Spec Differences Considered for HCD cPP Updates v2.pdf - ONLYOFFICE. Some of the key differences found were:

      - Many SFRs in the Crypto Spec added additional algorithms, key sizes and applicable standards not included in the HCD cPP versions of those SFRs

- The Crypto Spec used the FCS_CKM key management SFRs from CC:2022 which are different from the FCS_CKM key management SFRs in the HCD cPP. However, the Crypto Spec added to new key management SFRs - **FCS_CKM_EXT.7 Cryptographic Key Agreement** and **FCS_CKM_EXT.8 Password-Based Key Derivation** – that are not in CC:2022. The Crypto Spec SFR also made changes to the version of **FCS_CKM_EXT.3 Cryptographic Key Access** from CC:2022.
- The Crypto Spec took the **FCS_RBG** family from CC:2022, but interestingly the Crypto Spec changed SFR **FCS_RBG.1.1** from the version of that SFR in CC:2022.
- SFR **FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification** in the HCD cPP covered both Signal Generation and Signal Verification. I the Crypto Spec there were separate SFRs for Signal Generation (**FCS_COP.1/SigGen Cryptographic Operation (Signature Generation)**) and Signal Verification (**FCS_COP.1/SigVer Cryptographic Operation (Signature Verification)**).
- **FCS_COP.1/KeyWrap Cryptographic operation (Key Wrapping)** was a rare case where there were several algorithms in the HCD cPP version of the SFR that were not in the Crypto Spec version.
- The Crypto Spec version of SFR **FCS_KYC_EXT.1 Extended: Key Chaining** is completely different from the version of this SFR in the HCD cPP.

Al didn't point this out at the meeting, but it is interesting that the Crypto Spec took the FCD_RBG SFRs from CC:2022 but not the **FCS_RNG.1 Random number generation** SFR from CC:2022.

b. CC:2022 published in Nov 2022 does have differences from the prior version (CCv3.5R3) of the CC. The issue is that per the CCDB all PPs and cPPs have to be compliant to CC:2022 by Dec 31, 2025; after that date no certification against the previous version of the CC will be accepted by any of the countries who signed the CC Recognition Arrangement.

It's important to know what the differences in CC:2022 are. Al did a similar type of comparison of the SFRs in the new CC:2022 Part 2 against HCD cPP v1.0. This comparison can be found at CC2022 Differences Considered for HCD cPP Updates.pdf - ONLYOFFICE.

Some of the differences were hinted in the discussion of the Crypt Spec above. Summarizing the main differences in CC:2022:

- **FAU_GEN.1 Audit data generation** and some of the other audit-related SFRs changed from requiring "audit reports" to requiring "audit data".
- For **FAU_STG.1 Protected Audit Trail Storage**, SFRs **FAU_STG.1.1** and **FAU_STG.1.2** were combined into a single SFR **FAU_STG.1.1**
- **FCS_CKM.4 Cryptographic key destruction** was deprecated and replaced by a new SFR **FCS_CKM.6 Timing and event of cryptographic key destruction**
- In **FPT_TST_EXT.1 TSF Testing**, a new requirement "[assignment: *list of self-tests run by the TSF*]" was added
- In the SFR **FPT_STM.1 Time stamps**, a new SFR **FPT_STM.2.1 The TSF shall allow the [assignment: *user authorized by security policy*] to [assignment: *set the time, configure another time source*]].** was added
- Key new SFRs added were:
  - **FAU_STG.1 Audit data storage location**
  - **FCS_CKM.5 Cryptographic key derivation**
  - **FCS_RBG.1 Random bit generation**

    Note: there is a set of five other FCS_RBG SFRs in CC:2022 that provide additional requirements beyond basic Random Bit Generation
  - **FCS_RNG.1 Random number generation**
  - **FDP_IRC.1 Information retention control**

- **FDP_SDC.1 Stored data confidentiality**
- **FIA_API.1 Authentication proof of identity**
- **FTP_PRO.1 Trusted channel protocol**
- **FTP_PRO.2 Trusted channel establishment**
- **FTP_PRO.3 Trusted channel data protection**

c. A third concern the HCD iTC will have to deal with is the new content in Network Device (ND) cPP v3.0. ND cPP v3.0 was recently published, but after it was published NIAP submitted several serious technical comments mostly related to TLS 1.3 and DLTLS that the ND iTC has to address. The resolution of these comments will most likely result in publishing an Errata to ND cPP v3.0.

Nevertheless, the changes in ND cPP v3.0 because of how closely the HCD cPP is aligned with the content of the ND cPP. Al had done a comparison of the SFRs in the HCD cPP against the corresponding SFRs on ND cPP v3.0 which can be found at ND cPP v3.0 Differences Considered for HCD cPP Updates.pdf - ONLYOFFICE.

There were a lot of changes, many of which may be negated by the Crypto Spec. However, the two key changes are:

- ND cPP v3.0 now claims conformance to the NIAP Functional Package for SSH Version 1.for all SSH SFRs and associated Assurance Activities
- ND cPP v3.0 and ND SD v3.0 implements TLS 1.3.

d. The final issue that the HCD iTC has to consider for log range planning is Commercial National Security Algorithm (CNSA) 2.0. Currently all algorithms comply with CNSA 1.0. NSA wants algorithms to meet CNSA 2.0 to be quantum-resistant, especially for software and firmware signing, by 2035. However, the initial plan called for New software and firmware use CNSA 2.0 signing algorithms by 2025; Transitioning deployed software and firmware not CNSA 1.0 compliant to CNSA 2.0-compliant algorithms by 2025; and transitioning all deployed software and firmware to CNSA 2.0-compliant signatures by 2030.

That schedule was unrealistic, but NIAP is working on a plan for transitioning cPPs to CNSA 2.0. Once NIAP has developed this transition plan the HCD will work a plan for incorporating CNSA 2.0 algorithms into the HCD cPP and HCD SD.

Given these four issues, Kwangwoo decided that they needed to be prioritized. The priority, in order from high to low, is:

- Review the draft Specification of Functional Requirements for Cryptography
- Work on determining what CC:2022 changes should be incorporated into the HCD cPP/SD and when
- Work on determining what ND cPP/SD v3.0 changes should be incorporated into the HCD cPP/SD and when
- Implementing CNSA 2.0

4. Al next gave an update on the HIT.

- There are currently nine open HIT issues, including a new issue HCD-IT #10. Issue HCD-IT #10 is titled "**Mapping issue between Mandatory 'O.KEY_MATERIAL' objective and Cond. Mandatory 'FPT_KYP_EXT.1**". This issue came from the Canadian Scheme as part of its review of the HCD cPP in its evaluation role for the certification of a Lexmark HCD against HCD cPP/SD v1.0.

The issue is that the Organizational Security Policy (OSP) O.KEY_MATERIAL, which is defined as "The TOE shall protect from unauthorized access any cleartext keys, submasks, random numbers, or other values that contribute to the creation of encryption keys for storage of User Document Data or Confidential TSF Data in Nonvolatile Storage Devices; The TOE shall ensure that such key material is not stored in cleartext on the storage device that uses that material", is

mapped in Table 21 in Section I.9 in the HCD cPP to SFR **FPT_KYP_EXT.1** and also mapped to Use Case 2 I Section 1,4.2 which talks about protecting documents or confidential system information that may be present in Nonvolatile Storage Devices.

The problem is that **FPT_KYP_EXT.1** is a "Conditionally Mandatory" SFR, which would mean that OSP O.KEY_MATERIAL would only apply conditionally in cases where SFR **FPT_KYP_EXT.1** applied such as for HCDs that had hard disks. The concern was that O.KEY_MATERIAL would not apply to TSF data stored in wear-leveling devices such as SSDs, which does happen.

The HIT agreed that the best solution is to map OSP O.KEY_MATERIAL to an SFR such as **FPT_SKP_EXT.1 Extended: Protection of TSF Data** that is a mandatory SFR. This issue was assigned and is being worked.

- The Canadian Scheme had two additional comments that were the same type of comments as documented by NIAP in Issue HCD-IT #7 NIAP APE_REQ.2-7 Assessment of HCD cPP, so these two comments were included as comments under Issue HCD-IT #7 rather than created as a new issue.
- Work on the remaining open comments is progressing, although HCD-IT #2 is ready for the Technical Decision after the following process questions are addressed:
  - What indicates in GitHub that the solution has been accepted? Per the HIT Procedures the HIT must approve via vote the solution and then approval of the actual fix comes via the Pull Request that moves the file containing the fix from the Working branch into the Interpretation branch which requires approval of at least two additional HIT members besides the person who created the Pull Request.
  - Should the TD be approved by the full HCD iTC? Per the HIT Procedures only HIT approval is required
  - Should the TDs and TRs be published outside of the HCD iTC OnlyOffice site? We looked what the ND iTC did. They list all their NIAP-approved TDs and TRs on the NIAP portal under the NIAP approved ND cPPs. It would probably be an HCD iTC decision what HCD iTC documents get published on the CC and NIAP portals; no HIT recommendation on this topic has yet been made.

5. Al began updated the status of the EU Cybersecurity Act. The EU has a proposed 2023 Amendment to the 2019 EU Cybersecurity Act. Al had put together a presentation on this proposed amendment, which can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/EU Cybersecurity Act update.pdf. However, because of time constraint, Al just indicated that the main goal of the proposed amendment was to incorporate "managed security services" into the EU Cybersecurity Act to go along with ICT products, ICT services, ICT processes whenever those terms are mentioned in the Act.

   Smith ask how the Act defined the term "managed security services". In the proposal, "managed security services" is defined as "A service consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, including incident response, penetration testing, security audits and consultancy". Services, in this content, who be something provided by a third party or a person and not something provided by a computer program.

6. Al then presented his special topic for the day, which is a look at the Initial Public Draft of NIST Special Publication (SP) 800-171r3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The slides for this presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST SP 800-171R3 IPD.pdf.

   Because the time was getting short Al did not go through all the slides in the presentation but only hit a few key slides which are mentioned below (the full slide set is in the link above):

   - This Initial Public Draft was issued May 2023 so it is very recent
   - It is meant for protecting the *confidentiality* of CUI when the CUI is resident in a nonfederal system and organization, so unlike many NIST SPs this one is specifically design for organizations that do business with the Federal Government and not Federal Agencies.

- The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components
- Requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations 4
- **controlled unclassified information (CUI):** Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended

  CUI is basically any type of personal information such as Social Security Numbers or Patient Medical Information that must be protected due to of some federal regulation.
- The table below has the 23 security requirements categories that

Access Control	Maintenance	Security Assessment and Monitoring
Awareness and Training	Media Protection	System and Communications Protection
Audit and Accountability	Personnel Security	System and Information Integrity
Configuration Management	Physical Protection	Planning
Identification and Authentication	Risk Assessment	System and Services Acquisition
Incident Response	Supply Chain Risk Management	

- It turns out that Access Control has by far the greatest number of proposed “best practices” of all the categories – it took 7 slides in the presentation to cover all the subcategories and best practices for Access Control.
- Note how some of the best practices are written almost like Common Criteria requirements. For example, under Account Management the practice “Disable accounts of individuals within [*Assignment: organization-defined time period*] of discovery of [*Assignment: organization-defined significant risks*]”.

  Al Noted that there wasn’t anything unusual or unexpected under Access Control
- Under Audit and Accountability, Al noted there were not any best practices around audit storage
- Under Identification and Authentication, Al noted that the Password Management best practices in this new version are much less strict and more reasonable than in the original version. The “Store passwords using an approved salted key derivation function, preferably using a keyed hash” best practice is interesting in that it requires a “salted” key derivation function.
- Under Media Protection, for Media Sanitization the best practice is “Sanitize system media containing CUI prior to maintenance, disposal, release out of organizational control, or release for reuse”, where sanitization is defined as “Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means”.

- Under Systems and Communications Protection, Al found it interesting that the best practices for **Cryptographic Key Establishment** (Establish and manage cryptographic keys when cryptography is implemented in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*]) and **Management and Cryptographic Protection** (Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*]) are under this category and he noted how the best practices are defined.

  Al also noted here that nowhere in this document is there any best practice around protection of CUI stored in non-volatile storage.

7. **Actions:** None

Next Steps

The IDS Session at the August PWG Virtual Face-to-Face Meetings will be Thursday, August 10th, 2023 from 10A – 12N ET.

The next IDS WG Meeting will be July 13, 2023 at 3:00P ET / 12:00N PT, now that we are back on our normal cycle with IPP. Main topics will be the latest status of the HCD iTC and HIT, debrief of the IDS Session at the August PWG Virtual Face-to-Face Meetings and likely a special topic on a TBD topic