IDS Face-to-Face Minutes
August 18, 2022

Meeting was called to order at approximately 10:00 am ET August 18, 2022.

Attendees –

Graydon Dodson	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Uli Wehner	Ricoh
Jimmy Wu	Microsoft
Steve Young	Canon

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2022-08-18-IDS-F2F v1.pdf.

- Minute Taker
  - Alan Sukert taking the minutes

2. Agenda:
   - Introductions, Agenda Review
   - Discuss results of latest Hardcopy Device international Technical Community (HCD iTC) Meetings and HCD collaborative Protection Profile (cPP)/Supporting Document (SD) v1.0 status
   - Cybersecurity Executive Order Status Update
   - HCD Security Guidelines v1.0 Status
   - Trusted Computing Group (TCG) / Internet Engineering Task Force (IETF) Liaison Reports
   - Wrap-Up / Next Steps
3. Alan went quickly through the PWG Antitrust and Intellectual Property and Patent policies.
4. Alan went through the current status of the HCD iTC and its efforts to develop HCD cPP v1.0 and HCD SD v1.0. Some of the key points from this discussion were:

   - Al continued presenting the new way of showing comments he started at the 8/19/2 IDS Face to Face of showing all the comments received to date across all the drafts to date.

     The key milestones reached since the 8/19/2 IDS Face to Face were that the Final Draft of the HCD cPP (Version 0.13 dated 7/25/22) was released for Public Review on 8/1/22, and the Final Draft of the HCD SD (Version 0.99 dated 7/29/22) was also released for Public Review on 8/1/22.

     Regarding the HCD cPP, specifically for the 2nd Public Draft there were 83 total comments submitted against the 2nd Public Draft, all of which have been. The tally for the 83 comments was:

     - 56 comments were ‘Accepted’ to be fixed for the Final Draft of the HCD cPP
     - 0 comments were ‘Accepted in Principle’ to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
     - 10 comment was ‘Deferred’ to be addressed a later time, possibly in a later version of the HCD cPP
     - 17 comments were either not accepted or rejected

Overall, for all the HCD cPP drafts to date the total comment tally has been:

- 287 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
- 3 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
- 27 comments were 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
- 42 comments were either not accepted or rejected

Al noted that that the positive trend for the HCD cPP of total comments going down for each successive draft noted earlier by Ira continued.

Specifically for the 2nd Public Draft of the HCD SD, there were 29 total comments submitted, all of which were adjudicated. The tally for the 29 comments was:

- 25 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
- 1 comment was 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
- 0 comments were 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
- 3 comments were either not accepted or rejected

Overall, for all the HCD SD drafts to date the total comment tally was:

- 106 comments were 'Accepted' to be fixed for the Final Draft of the HCD cPP
- 2 comments were 'Accepted in Principle' to be fixed eventually in the HCD cPP by the time the HCD cPP v1.0 is published
- 17 comment was 'Deferred' to be addressed a later time, possibly in a later version of the HCD cPP
- 6 comments were either not accepted or rejected

Al noted the HCD SD comments didn't follow the same positive declining pattern as the HCD cPP comments over time.

- Al then went thru the key issues resolved in the Final Drafts of both the HCD cPP and HCD SD. The two lists are shown at the end of these minutes. Some key points on each list:
- For the HCD cPP, the majority of the changes in the Final Draft revolved around four areas:
  - Implementation of the new FDP_UDU_EXT.1 User.DoC Unavailable SFR that replaced the former FDP_RIP.1/Overwrite SFR
  - Implementation of the new FPT_WIPE_EXT.1 Data Wiping SFR that replaced the former FDP_RIP.1/Purge SFR
  - Inclusion of Cryptographic Erase as a mandatory method for performing the "purge" function as defined in NIST SP 800-88r1
  - Allowing overwrite to apply to both wear-leveling and non-wear-leveling storage devices

  The other major issues resolved in the Final Draft of the HCD cPP were:

  - Modified SFRs FPT_SBT_EXT.1.5 and FPT_SBT_EXT.1.6 for Secure Boot to clarify that they apply only to Hardware Roots of Trust

  - Added a new table in Section 5.12 TOE Security Functional Requirements Rationale that maps OSPs to SFRs and provides the rationale for that mapping to comply with requirements in CC Part 1
  - Addressed 3 NIAP TDs - TD0642: FCS_CKM.1(a) Requirement; P-384 keysize moved to selection; TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH and TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server
- For the HCD SD, the major issues addressed in the Final Draft were:
  - The TSS, Guidance and Test Assurance Activities for the new FDP_UDU_EXT.1 User.DoC Unavailable and FPT_WIPE_EXT.1 Data Wiping SFRs
  - Revised the Test Assurance Activities for both SFR **FCS_COP.1/DataEncryption** and SFR **FCS_COP.1/StorageEncryption** to add testing of the key size of 192 bits
  - Broke up the Test Assurance Activities for SFR **FIA_PMG_EXT.1 Extended: Password Management** into two separate test cases to avoid confusion
  - Made several changes to the Vulnerability Analysis and Evaluation Activities for SARs sections to add missing information or to correct inaccurate information.
- Al indicated that at this point in time, other than working to address comments against the Final Drafts and work to get HCD cPP and HCD SD Version 1.0 published, the only outstanding issue is whether removal of support for:
  - TLS 1.1
  - SHA-1 support
  - Cipher suites with RSA Key Generation with keys < 2048 bits
  - All RSA and DHE Key Exchanges

  be in HCD cPP v1.0 or in a later version. The iTC still has to formally decide on that. Ira noted that FIPS 180 is deleting the definition of SHA-1.
- Al noted that the current “Parking Lot” issues that have been pushed to the next release of the HCD cPP/SD:
  - Addressing hardware-based Roots of Trust stored in mutable memory as well as immutable memory
  - Clarification that the Secure Boot SFR only requires verification of firmware/software that is stored in mutable memory at boot time and does not require verification of firmware/software stored in immutable memory
  - Comments that require implementation of TLS 1.3 to resolve
  - Support for NTP
  - Support for the CCUF Crypto Working Group SSH Package
  - Correcting TSS Assurance Activities for SFR FCS_CKM.4 Key Destruction
  - Clarification of TSS Assurance Activities for SFR FIA_X509_EXT.2 X.509 Certificate Authentication
- At this point all content for both documents is “locked down”. The only changes at this point that would necessitate new content and significant changes to existing content would be:
  - Request from JISEC or ITSCC or NIAP (or any other Scheme)

- Necessitated by any new NIAP TDs to either the HCD PP or any applicable SFRs in the ND & FDE cPPs/SDs

It is unlikely HCD iTC would accept Final Draft comments against either the HCD cPP or HCD SD from any other source other than the two above that would require substantive technical changes to the content of either document at tis point.

- Al then provided a status update on schedule that was just revised in August to reflect the work on publishing the Final Drafts of the HCD cPP and HCD SDl. The new "official;" schedule is as follows:
  - Publishing of Final Drafts of HCD cPP and HCD SD: Planned: 7/18; Actual: 8/1
  - Review Final Public Drafts of HCD cPP and HCD SD: Planned: 7/19/ – 8/22 Actual: 8/1 – 9/15
  - Review comments and update both documents: Planned: 8/23/22 – 9/6/22
  - Publish HCD cPP and HCD SD Version 1.0: Planned: 9/7/22

  Al indicated that we are already ~3 weeks behind schedule. If we get comments by 9/15 and there are no big technical issues, Al indicated that his best estimate was thar the HCD cPP and HCD SD Version 1.0 would likely end up being published sometime around the end of September or beginning of October.

- Al then listed these items as ones to consider for inclusion in the HCD cPP/SD Post-v1.0:

  <u>Will almost certainly be in next version</u>
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1. Ira noted that the current plan is that the ND iTC will put out ND cPP 3.0 for final public review Sep 14 with a planned late Nov 22 publishing date.
  - Inclusion of NTP
  - Inclusion of AVA_VAN and ALC_FLR.*
    - May require a PP Module to avoid duplicate certifications in EU

    Al noted that coordination between the CC and EUCC is gong to become a big issue in 2023.
  - Sync with key changes in ND cPP/SD v3.0 to be published in Oct 2022
    - Incorporate CCDB Crypto WG SSH Package
  - Changes due to HCD Integration Team (HIT) responses to comments/questions to HCD cPP/SD v1.0
  - Expand to address 3D printing
  - Changes due to requests from JISEC, ITSCC or NIAP
  - Update to ISO/IEC 15408/18045 to be published in Oct 2022
    - Adds new SFRs and pre-packaged PP and ST Assurance Activities in new Part 4

  <u>Potential for next or later versions</u>
  - Support for Wi-Fi and maybe Bluetooth
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs
  - CCDB Crypto WG, other CCUF Crypto WG Packages or NIAP TLS Package
  - Support for SNMPv3

- Support for NFC
- Support for new crypto algorithms
- Indirect updates based on new technologies or customer requests

Ira asked whether Al thought the next HCD cPP/SD version after 1.0 should be 1.1 or 2.0. Al's view is that the HCD iTC needed to get things like TLS 1.3 out sooner than later, with more timely minor versions say 6-9 months apart and major versions 2-3 years apart were better. Bottom Line – next version should be 1.1 in about 9 months at most after 1.0 is published.

- Al then spent some time talking about the HCD iTC Interpretation Team (HIT). The HIT will essentially take over maintenance of HCD cPP v1.0 and HCD SD v1.0 once they are published. The goal of the HIT is to provide timely responses to requests for interpretation (RFIs) from the CC community. The HIT has its own set of procedures based on the HCD iTC's Terms of Reference including rules for:
  - Determining what RFIs to review and how to process them
  - Voting and decision making
  - Membership and participation
  - What RFIs to pass on to the full iTC

  The general HIT process is:
  - HIT gets an RFI from a Scheme or vendor doing a certification using HCD cPP/SD or another source
  - HIT analyzes RFI to determine whether to accept RFI for some type of action
  - If rejects, indicates rationale for rejection
  - If accepts:
  - Prioritizes RFI
  - Determines Response
  - Generates either Technical Recommendation (TR), which goes to full iTC for approval, or a Technical Decision (TD) which does not need full iTC approval
  - Publishes TR or TD
- Next steps are pretty straightforward:
  - Address all the comments against the Final Drafts
  - Finalize "parking lot" issues for next and future versions of the HCD cPP/SD
  - Review and resolve all comments and update the HCD cPP and HCD SD drafts per the agreed schedule
  - Publish HCD cPP/SD v1.0 per the agreed schedule
  - Start planning for and implement the HCD iTC Interpretation Team (HIT) for maintaining HCD cPP/SD v1.0 and start planning for the next HCD cPP/SD update (whether it is v1.x or v2.0)
- Al finished the HCD iTC discussion with some more additions to the HCD iTC lessons learned he presented at the previous IDS Face-to-Face Meetings. These additional lessons learned were:
  - Being an Document Editor is hard work but they are the unsung heroes of any iTC and don't get the credit they deserve

- In 20-20 hindsight, the one thing the HCD iTC needs to do a better job of is handling major issues more efficiently – it took us way too long to reach agreement on the key areas of disagreement
- Having templates for the key documents an iTC must produce like the cPP and the SD was a big help in getting started
- A personal one – this being my third attempt at developing an HCD Protection Profile, you'd think it would get easier the third time around. But it doesn't because each time there are a different set of challenges and timelines.

- However, in the three tries we've done it faster – from 5 years to 3 years to 2 years, 7 months (assuming the cPP/SD are published in Sep 2022)

5. Al then gave a presentation on an updated to a presentation he gave at the 8/19/21 IDS Face to Face Meeting on the Cybersecurity Executive Order (EO 14028) of May 2021.

- Al started with a brief summary of what the key areas covered by EO 14028 were:
  - Policy – Federal Government must
    - Bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
    - Must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
    - Sharing Threat Information
    - Cyber Incident Reporting
    - Enhancing Software Supply Chain Security
    - Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incident
    - Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
    - Improving the federal government's investigative and remediation capabilities
  - Then Al summarized the main documents that NIST has produced to date that resulted from EO 14028:

    Software Security Practices documents (Released Feb 4, 2022)

    - Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and)
    - NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities (https://csrc.nist.gov/publications/detail/sp/800-218/final)

    Software Security Labeling documents (Released Feb 4, 2022)

    - Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products (https://doi.org/10.6028/NIST.CSWP.02042022-2)
    - Recommended Criteria for Cybersecurity Labeling of Consumer Software (https://doi.org/10.6028/NIST.CSWP.02042022-1)
    - Consumer Cybersecurity Labeling Pilots: The Approach and Feedback (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots)

Other Documents

- Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 - (https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eocritical-software-use-2) – Published Jul 9, 2021
- NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommendedminimum-standards-vendor-or) – Published Oct 2021
- 2nd Draft of NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-161r1-draft2) – Published Oct 2021

- Al then did a quick "deep dive" into one of the documents listed above - NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software.
  - The guidelines are meant to be minimum standards**,** not "best practices" of software verification by software producers. These Guidelines are based on assumption that there is no single software security verification standard that can encompass all types of software and be both specific and prescriptive while supporting efficient and effective verification, so they are designed for each software producers to use in creating their own processes which can be very specific and tailored to the software products, technology (e.g., language and platform), toolchain, and development lifecycle model.
  - The scope of these guidelines Includes "software source code" and software in general including binaries, bytecode, and executables, such as libraries and packages It does not include specialized testing regimes such as real-time software, firmware (microcode), embedded/cyberphysical software, machine learning (ML) or neural net code. It also excludes ancillary yet vital material such as configuration files, file or execution permissions, operational procedures, and hardware.
  - Al then quickly went through the list of the 11 steps the guidelines recommend as a minimum for development testing of software:
    - Do Threat Modeling - Threat modeling should be used early in order to identify design-level security issues and to focus verification and software needs should drive the threat modeling method(s) used.
    - Do Automated Testing – this is especially important for HCD certifications because a vendor can't do the required secure protocol and crypto testing per the HCD SD manually; it has to be done using automated tools
    - Code-Based, or Static, Analysis – This is your basic running of code standards checkers or now tools for checking for code vulnerabilities like buffer overflows
    - Review for Hardcoded Secrets – This is basically checking for any hardcoded passwords. Al noted the time a project at Xerox got skewered by a French security firm for finding several hardcoded passwords.
    - Run with Language-Provided Checks and Protection - Essentially this guideline is saying that if you have a compiler or interpreter or a software language that has options that enforce security or have built-in checks and protections both during development and in the software shipped, make sure you that you use them.
    - Black Box Test Cases – This is your classic requirements and functional testing at the integration and system levels.
    - Code-Based Test Cases – This is the traditional programmer unit testing where the goal is to test all paths or something similar.

- Historical Test Cases – This is essentially doing regression testing to make sure what previously worked still works
- Fuzzing – This is testing that involves providing invalid, unexpected, or random data as inputs to a computer program and see what gets found. It isn't particular mainstream these days, but Ira said it is used to test APIs with out of bound conditions to try to crash the system.
- Web Application Scanning – This pretty straightforward ; if your software has a web application (and most HCDs do) make sure you scan it for errors and vulnerabilities.
- Check Included Software Components – This just means to make sure to test all your OpenSource and 3rd Party components as well as your own software.

The general reaction to these guidelines was that it was basic common sense.

6. Ira then covered the latest status on the HCD Security Guidelines. Essentially nothing has changed since the February or August IDS Face to Faces – the version of the HCD Security Guidelines (Version 13.1 dated 8 February 2022) that can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208-rev.docx (Note: a "clean" version of the update can be found at https://ftp.pwg.org/pub/pwg/ids/wd/wd-idshcdsec10-20220208.docx) has not been updated.
7. For the final topic Ira presented his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). The key points from Ira's Liaison Report were:
   - Regarding TCG standards activities, some key items Ira stressed were:
     - Next TCG Members Meetings
       - **TCG Hybrid F2F (New Orleans, LA) – 25-27 October 2022 – Ira to call in**
       - **TCG Hybrid F2F (TBD location) – February 2022 – Ira to call in**
     - ***TCG Mobile Reference Architecture v2*** was rewritten for review in Q3 2022
     - ***TCG MARS 1.0 Mobile Profile*** – not looking at review any time soon
     - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work*** – looking at PR in Fall 2022
     - ***TCG DICE Endorsement Architecture for Devices*** – review completed. This is important for Attestation
   - Regarding IETF standards activities, some key items Ira stressed were:
     - **IETF 115 Hybrid F2F (London, UK) 7-11 November 2022 – Ira to call in**
     - **IETF 116 Hybrid F2F (Yokohama, Japan) – 27-31 March 2023 – Ira to call in**
     - Key TLS-related specs that have been recently published were:
     - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022**
     - **IETF Importing External Pre-Shared Keys (PSKs) for TLS 1.3 – RFC 9258 – July 2022**
     - **IETF Guidance for External Pre-Shared Key (PSK) Usage in TLS – RFC 9257 – July 2022**
     - Other TLS-related specs of note for the recent IETF 114 meeting:
       - **IETF Flags Extension for TLS 1.3 – draft-10 – July 2022** – is new technology

- **IETF Return Routability Check for DTLS 1.2/1.3 – draft-06 – July 2022** – is useful for IT devices
- **IETF Delegated Credentials for (D)TLS – draft-15 – June 2022 – IETF LC** – will be published before the end of 2022.

- Security Automation and Continuous Monitoring (SACM) wrapped up in December 2021 due to politics. However, the **IETF Concise Software Identifiers** spec is important to Remote ATtestation ProcedureS (RATS) and because it positively impacts runtime efficiency
- Regarding Concise Binary Object Representation **(**CBOR), some specs of note:
  - **IETF CBOR Tags for Time, Duration, and Period – draft-01 – July 2022** – this is moving along
  - **IETF Packed CBOR** – this work is at 100%
  - **IETF Notable CBOR Tags – draft-07 – July 2022** – this is new work
  - **IETF Feature Freezer for CDDL – draft-09 – December 2021** – this is new work
- Regarding Remote ATtestation ProcedureS (RATS):

  The following are now at the IETF Editors:
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-03 – July 2022**
  - **IETF Concise Reference Integrity Manifest – draft-03 – July 2022**
  - **IETF Direct Anonymous Attestation for RATS – draft-01 – July 2022**
- Finally, for the **IRTF Crypto Forum Research Group (CFRG):**

  This is where the IETF does all its cryptographic work
  - **IRTF Usage Limits on AEAD Algorithms – draft-05 – July 2022** – is a best practice that will allow usage of AEAD algorithms
  - **IRTF Hashing to Elliptic Curves – draft-16 – June 2022** – Contains recent elliptical curve algorithms

8. **Wrap Up**
   - Next IDS Working Group Meeting will be on September 8, 2022. Main topics of the meeting will be latest HCD iTC status.
   - Next IDS Face-to-Face Meeting will be during the November 2022 PWG Virtual Face-to-Face Meeting November 15-17, 2022.

   Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 11:58 am ET on August 18, 2022.

IDS Face-to-Face Minutes
August 18, 2022

MAJOR CHANGES INCLUDED IN FINAL PUBLIC DRAFT HCD cPP

1. **To include Cryptographic Erase into the HCD cPP and address concerns about** the fact that the FDP_RIP.1/* SFRs suggested to users that residual data is permanently removed from wear-leveling storage devices (e.g., SSDs), when in fact FDP_RIP.* can't be used for operations involving Cryptographic Erase (CE) because the actual data is still present in encrypted form, and future technologies might be capable of breaking the encryption the following was done:

   - **Replaced SFR FDP_RIP.1/Overwrite** Subset residual information protection with a new SFR FDP_UDU_EXT.1 User.DOC Unavailable **that (1) provides the option for Overwrite for the SFR to apply to both wear-levelling and non-wear-levelling storage devices and (2) to include destruction of cryptographic keys as well as overwrite to make USER.DOC unavailable.**
   - **Replaced SFR** FDP_RIP.1/Purge Subset residual information protection with a new SFR FPT_WIPE_EXT.1 Data Wiping that requires that customer-supplied D.USER and D.TSF data stored in non-volatile storage be made unavailable using Cryptographic Erase as a mandatory method and optionally using none or one or more of five other methods – overwrite, block erase, media specific eMMC method, media specific ATA erase method, or media specific NVMe method.
   - **Added or modified wording addressing Cryptographic Erase or destruction of cryptographic keys in the following Sections:**
     - **a. Section 1.4.2** USE CASE 2: Conditionally Mandatory Use Cases, Item 4. Nonvolatile Storage Devices
     - **b.** Section 1.4.3 USE CASE 3: Optional Use Cases, Item 2. Redeploying or Decommissioning the HCD
   - Added the following statement to the definition of O.STORAGE_ENCRYPTION in Section 3.5.4 Storage Encryption: "…and the TOE shall provide a function that an authorized administrator may destroy encryption keys or keying material if the TOE supports a function for removing the TOE from its Operational Environment".
   - Added the following note to Section 3.5.7 Wipe Data (optional): Note: Cryptographic erase which is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4 can be used as a method to remove some parts of User Data and TSF Data, but it cannot be a single method to remove User Data and TSF Data unless all the data are encrypted.
   - Because of the new FDP_UDU_EXT.1 SFR, modified Section 3.5.6 Image Overwrite (optional) to remove the statement "or by destroying its cryptographic key" in the last sentence since it was no longer necessary.
   - Changed the title of Section 3.5.7 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR
   - Changed the title of Section 4.1.13 from Purge Data (optional) to Wipe Data (optional) reflect the new FPT_WIPE_EXT.12 Data Wiping SFR
   - Changed the Organizational Security Policy (OSP) O.PURGE_DATE to O.WIPE_DATA to reflect the new FPT_WIPE_EXT.12 Data Wiping SFR
   - Modified the Application Note for the SFR FDP_DSK_EXT.1 Protection of Data on Disk to state that if additional data other than D.USER.DOC and D.TSF.CONF are encrypted, it will be purged by the cryptographic erase process
2. Modified SFRs FPT_SBT_EXT.1.5 and FPT_SBT_EXT.1.6 for Secure Boot to clarify that they apply only to Hardware Roots of Trust.

3. Removed the previous Software Functional Requirements table that was in Appendix H: SFR List, as well as the entire appendix, that mapped SFRs to OSPs. Replaced this table with a new table in Section 5.12 TOE Security Functional Requirements Rationale that maps OSPs to SFRs and provides the rationale for that mapping.
4. Moved SFR FCS_CKM.1/AKG Cryptographic Key Generation (for asymmetric keys) from a Conditionally Mandatory to an Optional requirement.
5. Added missing or incorrect SFR Mapping Information for several SFRs.
6. Removed the Consistency Rationale Appendix as being repetitive and no longer needed.
7. The term File Encryption Key (FEK) was incorrectly used in several places in the document; it was replaced by “BEV or DEK”. Also, is some instances “DEK” was missing when it should have been included, so in those instances “BEV” was changed to “BEV or DEK” also.
8. Corrected a typo in Section 5.4.2. FDP_ACF.1 Security attribute based access control, Table 5. D.USER.JOB Access Control SFP, where “log’ should have been “job”.
9. Addressed the following NIAP Technical Decisions:
    - TD0642: FCS_CKM.1(a) Requirement; P-384 keysize moved to selection
    - TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH
    - TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server
10. Fixed several grammatical and typographical errors in the document.

IDS Face-to-Face Minutes
August 18, 2022

MAJOR CHANGES INCLUDED IN FINAL DRAFT OF HCD SD

1. Added the Assurance Activities for the new SFRs **FDP_UDU_EXT.1 User.Doc Unavailable** and **FPT_WIPE_EXT.1 Data Wiping** that replaced the previous SFRs **FDP_RIP.1/Overwrite** and **FDP_RIP.1/Purge**, respectively.
2. Because of the inclusion of Cryptographic Erase due to the new SFRs **FDP_UDU_EXT.1 User.Doc Unavailable** and **FPT_WIPE_EXT.1 Data Wiping**, made the following changes to the Assurance Activities for SFR **FDP_DSK_EXT.1 Extended: Protection of Data on Disk**:
   - Added the following paragraph to the TSS Assurance Activities:

     If data (e.g., D.USER.JOB, D.TSF.PROT) other than D.USER.DOC and D.TSF.CONF are encrypted, the evaluator shall verify that TSS identifies all such data and states that no other customer-supplied data are encrypted
   - Added the following new tests to the Test Assurance Activities:

     Test 3. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) write the data to the storage device with operating TSFI which enforce write process of the data.

     Test 4. (If data other than D.USER.DOC and D.TSF.CONF are encrypted,) verify that the data written in Test 3 is not in plaintext form; and verify that the data can be decrypted by proper key and key material.
3. Updated the discussion in **Section 1.1. Technology Area and Scope of Supporting Document** to indicate that certifiers/certification bodies are users of this document.
4. Removed wording in **Section 1.2 Structure of the Document** that implied that Certifying Bodies (CB) could modify Evaluation Activities in the SD.
5. Removed wording in the preliminary paragraph in **Chapter 2. Evaluation Activities for SFRs** that suggested witnessing developer-generated tests vs. independently performing tests, because that would require CB approval.
6. Revised the Test Assurance Activities for both SFR **FCS_COP.1/DataEncryption** and SFR **FCS_COP.1/StorageEncryption** to add testing of the key size of 192 bits.
7. Broke up the Test Assurance Activities for SFR **FIA_PMG_EXT.1 Extended: Password Management** into two separate test cases to avoid confusion.
8. Revised **Section A.1.1. Type 1 Hypotheses - Public-Vulnerability-based** to add the missing information and to clarify the text from the previous versions of this document.
9. Revised Section **A.1.2. Type 2 Hypotheses - iTC-sourced** to indicate that there are currently are no iTC-sourced flaw hypotheses, but that a future revision of the HCD cPP may update this section for relevant findings made by evaluation laboratories.

10. Corrected and/or updated the Evaluation Activities for the following areas in **Chapter 6 Evaluation Activities for SARs:**

- **ADV_FSP.1-5 Evaluation Activity**
- **Operational User Guidance (AGD_OPE.1)**
- **Vulnerability Survey (AVA_VAN.1)**

11. Fixed some incorrect section references in the document as well as some typographical and grammatical errors.