Hardcopy Devices TC Status

Kwangwoo Lee

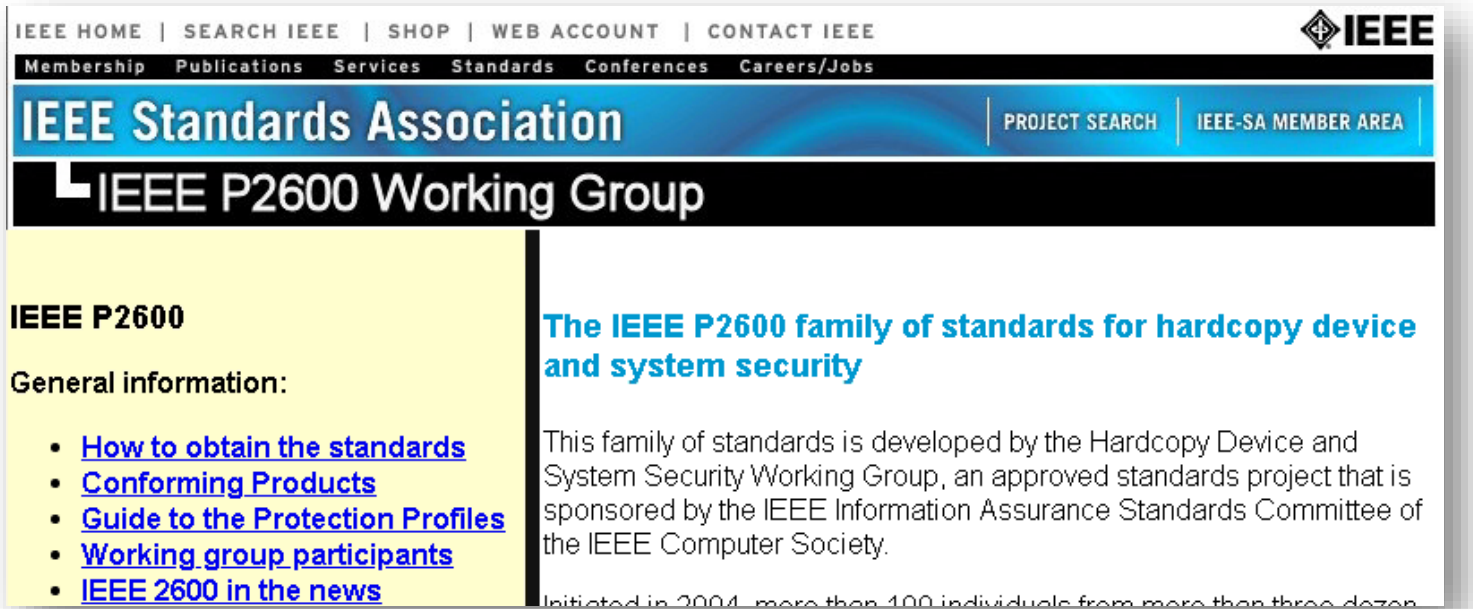
September 26, 2019

Overview

- **History of the Hardcopy Devices Protection Profiles**
  - IEEE 2600 PPs
  - HCD PP v1.0 (Protection Profile for Hardcopy Devices – V1.0)
  - Why didn't we just make the existing IEEE PPs conform to the new paradigm?
- **Challenges in Developing a new PP for HCDs**
  - Challenges during PP development
  - Challenges after PP publication
- **HCD iTC Status**
  - Essential Security Requirements
  - Terms of Reference
  - Key Person and affiliations
- **Lessons Learned**

IEEE 2600 PPs (1/2)

- Initiated in 2004, more than 100 individuals from more than three dozen organizations have participated in working group meetings, teleconferences, and email discussions.
- The IEEE P2600 Working Group developed IEEE Std. 2600™-2008 with security requirement and best practices for HCD vendors and customers in a variety of operational environments.



http://grouper.ieee.org/groups/2600/

IEEE 2600 PPs (2/2)

- The P2600 WG created Protection Profiles for two of those operational environments:
  - IEEE Std. 2600.1™-2009 at EAL3 was adopted as the US PP for HCDs, until NIAP changed its policy rejecting EAL4 and EAL3.
  - IEEE Std. 2600.2™-2009 at EAL2 was adopted as the new US PP for HCDs, adding additional functional requirements via NIAP Scheme Policy#20.

020	NIAP policy for the use of IEEE Multifunction Function Device Protection Profiles (IEEE 2600.1 and IEEE 2600.2)	2010.11.15

Published standards

- IEEE Std. 2600™-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security was published in June, 2008.
- IEEE Std. 2600.1™-2009, IEEE Standard for a Protection Profile in Operational Environment A was published in June, 2009. It is a NIAP-validated protection profile.
- IEEE Std. 2600.2™-2009, IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std. 2600™-2008 Operational Environment B was published in March 2010. It is a BSI-validated protection profile.

POLICY: NIAP will recognize the IEEE P2600.2 Protection Profile augmented with the changes outlined in Attachment A to this Policy as a U.S. Approved PP. The **IEEE 2600.1 PP will no longer be accepted for new evaluations under NIAP CCEVS** after the effective date of this policy. Products accepted into evaluation under NIAP CCEVS that claim conformance to the U.S. Approved IEEE 2600.2 PP may include additional functional requirements to those of Attachment A but **shall not** include any additional assurance requirements.

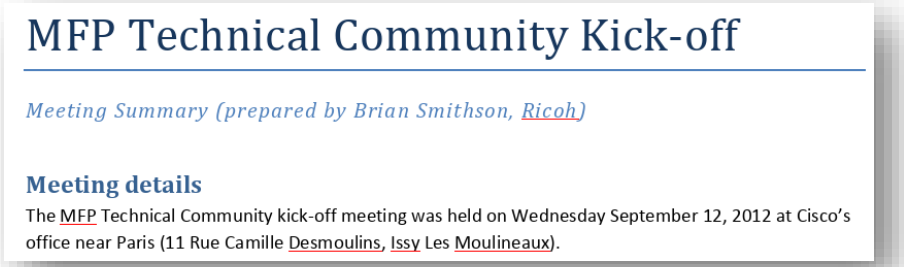
Usage as the US Government Approved Protection Profile for Hardcopy Devices

- IEEE Std 2600.2™-2009, with the addition of SFRs described in NIAP Policy #20, is the US Government Approved Protection Profile for Hardcopy Devices.
- IEEE Std 2600.1™-2009 fulfills all of the requirements of the US Government Approved Protection Profile for Hardcopy Devices. Refer to NIAP Policy #20 for details.

http://grouper.ieee.org/groups/2600/
https://www.niap-ccevs.org/Documents_and_Guidance/policy.cfm

HCD PP v1.0 (Protection Profile for Hardcopy Devices – V1.0)

- Developed by the MFP Technical Community
  - Effort was initiated by JISEC in 2012 to replace IEEE Std. 2600.2™
  - A working group was formed in May 2012 to create PP based on draft created by JBMIA, and an MFP TC had its kick-off meeting in September 2012



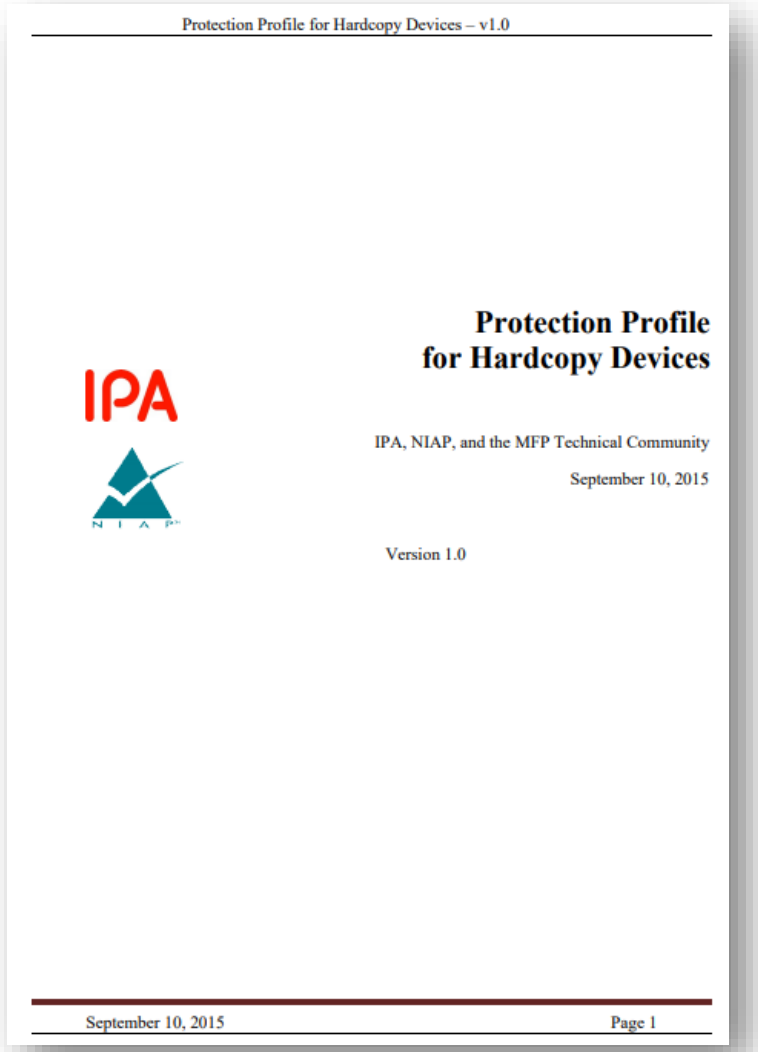
MFP Technical Community Kick-off

Meeting Summary (prepared by Brian Smithson, Ricoh)

Meeting details

The MFP Technical Community kick-off meeting was held on Wednesday September 12, 2012 at Cisco's office near Paris (11 Rue Camille Desmoulins, Issy Les Moulineaux).

  - After many drafts, a final version was published and approved by US and Japanese CC Schemes in September 2015
- HCD PP became effective immediately in the US; Japan gave vendors a two-year grace period
  - HCDs have been certified conforming to HCD PP in the US, Japan, Canada, and Sweden.



Protection Profile for Hardcopy Devices – v1.0

IPA

N I A P

Protection Profile for Hardcopy Devices

IPA, NIAP, and the MFP Technical Community

September 10, 2015

Version 1.0

September 10, 2015 Page 1

Why didn't we just make the existing IEEE PPs conform to the new paradigm?

- It may not be possible to add tailored assurance to an existing PP that was not designed to accommodate it.
  - Also, it is important to have some consistency with other new paradigm PPs, such as the Network Devices PP.

- Copyright to the existing PPs is owned by the *IEEE Standards Association*, so we can't just edit the existing PP as a starting point.

- We are making one collaborative PP that can be the basis for procurement for the governments of Japan and the US.

Challenges during PP development

- Some scheme policy changes were disruptive to vendors and confusing to customers:
  - Weeks after approving 2600.1, NIAP un-approved 2600.1, and instead, approved 2600.2 with NIAP policy #20.
    - It was difficult to explain this sudden change from EAL3 to EAL2.
  - Two weeks after DoD's DLA-Documents Services began requiring PP conformance, NIAP un-approved IEEE Std. 2600.2 as a US PP and archived Policy #20; DLA-DS rescinded.
  - In 2013, NIAP stopped accepting evaluations that do not conform to a NIAP-approved PP, but HCD PP was not published until two years later (Sep. 2015).
    - Vendors were forced to evaluate HCDs outside of the US.

Challenges after PP publication

- HCDPP does not claim conformance to an EAL, and it is not a cPP, so it does not adhere to CCRA mutual recognition rules.
  - For procurement, some nations recognize IEEE 2600.2, others recognize HCDPP, forcing vendors to certify to two PPs.
- NIAP's Scheme Policy#5 enforces cryptographic details that are not part of HCDPP. Certified products may or may not meet the requirement of Policy #5, distinguishable only by whether or not their certificates are listed on NIAP's PCL.
- NIAP certifies only HCDPP.
- Japan and Sweden certify HCD conformance to HCD PP, 2600.1, or 2600.2.
- Canada certifies HCDPP but treats 2600.2-conformant products as EAL2+ALC without PP conformance.
- Korea certifies HCD conformance to 2600.2.

Statistics of Hardcopy Devices

2584 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	55	81
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	68	140
Data Protection	78	99
Databases	31	53
Detection Devices and Systems	13	58
ICs, Smart Cards and Smart Card-Related Devices and Systems	1239	61
Key Management Systems	25	28
Mobility	31	33
Multi-Function Devices	211	197
Network and Network-Related Devices and Systems	267	260
Operating Systems	110	76
Other Devices and Systems	292	350
Products for Digital Signatures	111	8
Trusted Computing	50	0
Totals:	**2584**	**1444**
Grand Total:		**4028**

Categories	2008	2009	2010	2013	2014	2015	2016	2017	2018	2019	Total
IEEE 2600.1-2009					**8**	**4**	**3**	**3**			**18**
JP					8	3	1				12
SE						1	2	3			6
IEEE 2600.2-2009					**5**	**1**	**3**				**9**
DE					1						1
JP							2				2
SE					4	1	1				6
IEEE 2600.2-2009(US-Approved))					**3**	**13**	**17**	**32**	**15**	**4**	**84**
JP					2	8	15	31	15	4	75
KR					1	5	2	1			9
No PP	**1**	**2**	**1**	**2**	**3**	**15**	**23**	**1**	**5**	**4**	**57**
AU		1									1
CA					1	4	20				25
DE	1	1									2
JP			1	2	2	11	3	1	5		25
SE										4	4
PP_HCD_V1.0								**6**	**15**	**20**	**41**
CA									7	9	16
JP								4	7	5	16
SE									1	4	5
US								2		2	4
Total	**1**	**2**	**1**	**2**	**19**	**33**	**46**	**42**	**35**	**28**	**209**

https://www.commoncriteriaportal.org/products/stats/

HCD iTC Status

- CCDB at its Oct 2018 Meeting chartered a CCDB Working Group (WG) containing the Korean and Japanese schemes. Goal was formation of the HCD iTC at the April CCDB meeting in Rome
- HCD WG has created the following documents to be submitted to the CCDB for review at the April CCRA meeting:
  - Essential Security Requirements (ESR)
  - Terms of Reference (ToR)
- At the same time the HCD TC as creating its own versions of the same two documents plus a “Key Persons” document that will be referenced by the ToR
- Goal was to fold the HCD TC documents into the HCD WG versions that are submitted to the CCDB
- Currently, HCD TC is waiting the voting results from ~~CCDB/~~CCMC

HCD iTC Status – Essential Security Requirements

- [March 25, 2019] The HCD WG was aware of HCD TC works including the draft ESR done by the HCD TC since HCD TC provided the latest resolution of review comment as an input to support the HCD WG's works.
- [April 15, 2019] The HCD WG shared the HCD WG ESR v0.6 that agreed by CCDB HCD WG members. Note that US scheme provided their feedback as CC experts on this technology area.
- [April 15, 2019] Call for Comment
  - HCDTC members are encouraged to review the HCD WG draft ESR and submit comments on Causeway.
  - HCD WG mentioned that they welcome any improvement for the ESR if it is helpful to increase the security level of hardcopy devices.
  - HCD TC created the Gap Analysis between HCD_TC_ESR_v0.61 and HCD_WG_ESR_v0.6
    - Alan provide the comparison by section of the latest draft ESR created by the HCD TC to the latest draft ESR provided by the HCD Working Group.
- [June 3, 2019] Review comment for the HCD_WG_ESR_v0.6
  - HCD TC received 9 comments for the HCD _WG_ESR_v0.6 by May 24th, 2019 from HCD TC members. After that, HCD TC members reviewed the comments during the HCD TC monthly teleconference meeting.
- [June 15, 2019] HCD TC submit the review comments for the HCD_WG_ESR_v0.6 and shared the updated HCD ESR to HCD WG (ITSCC, JISEC).
  - HCD WG (ITSCC) responded that they will review the updated ESR and review comments from mid of July if there was no negative opinion or objection from CCDB members during the CCDB ToR approval voting process. It will be discussed by HCD WG members before the HCD iTC creation.

HCD iTC Status – Terms of Reference

- HCD TC shared the draft version of HCD iTC ToR to HCD WG (ITSCC, JISEC).
- [March 8, 2019] HCD WG reviewed the draft ToR that was provided by HCD TC. HCD WG provided the review comment based on HCD WG's agreement. Based on HCD review comment, HCD TC revised the voting text.
- [March 28, 2019] HCD TC shared the draft version of HCD iTC ToR - v0.5.docx to HCD WG (ITSCC, JISEC).
- [April 12, 2019] HCD WG shared the CCRA voting process and tentative schedule of HCD iTC establishment during 15th CCUF Workshop in Rome
- [April 17, 2019] HCD WG submitted the ToR to CCDB.
- [May 13, 2019] HCD TC checked the CCDB voting progress thru HCD WG (ITSCC). They mentioned that the CCDB ToR voting is not initiated yet.
- [June 3, 2019] HCD WG shared that CCDB HCD iTC ToR approval voting is started in May.
- [July 7, 2019] HCD WG shared that they didn't hear any negative sound/opinion and objection from CCDB chair yet.
- [Aug 19, 2019] HCD WG shared that HCD iTC ToR approval voting is completed without negative sound/opinion and objection from CCDB (Aug 12). Also, CCDB chair requested next process to CCMC Chair.

HCD iTC Status – Key Person and affiliations

- HCD TC requested several HCD stakeholders to invite the SME(s) list of HCD iTC
  - According to the feedbacks of each organization, HCD TC have created the draft Hardcopy Device International Technical Community – Key persons and affiliations.

- The Status of Subject Matter Experts (v0.8) – 62 members 33 organization
  - Industry SMEs: 34 members 14 organizations
  - Lab SMEs: 19 members 10 organizations
  - Certification Body SMEs: 4 members 3 schemes (KR, JP, SE)
  - Other SMEs: 5 members (IEEE-ISTO PWG experts/Biometric iTC expert/JBMIA)

HCD cPP 1.0 consideration

- TLS 1.3, deprecation of TLS 1.1 and inputs from TLS TC
- Internationally-friendly crypto requirements that don’t rely on FIPS
- Management of Crypto keys
- Additional IPSec requirements
- Protection of authentication passwords
- Inclusion of Wi-Fi (especially with development of WPA3)
- Addition of requirements for support of SNMPv3
- Audit Log Server Requirements
- Inclusion of TPMs and SSDs
- Incorporation of GDPR and privacy implications
- Password policies
- Continued syncing with NDcPP and FDE cPPs
- HCD iTC need to consider the new templates that was provided by Tool WG.

Lessons Learned (2)

- It takes a core group of very dedicated people to get a PP created or updated.

Sep. 2015, CCUF MFP TC, Windsor, UK

April 2017, CCUF MFP TC, Amsterdam, NL

April2018, CCUF HCD TC, Trondheim, Norway

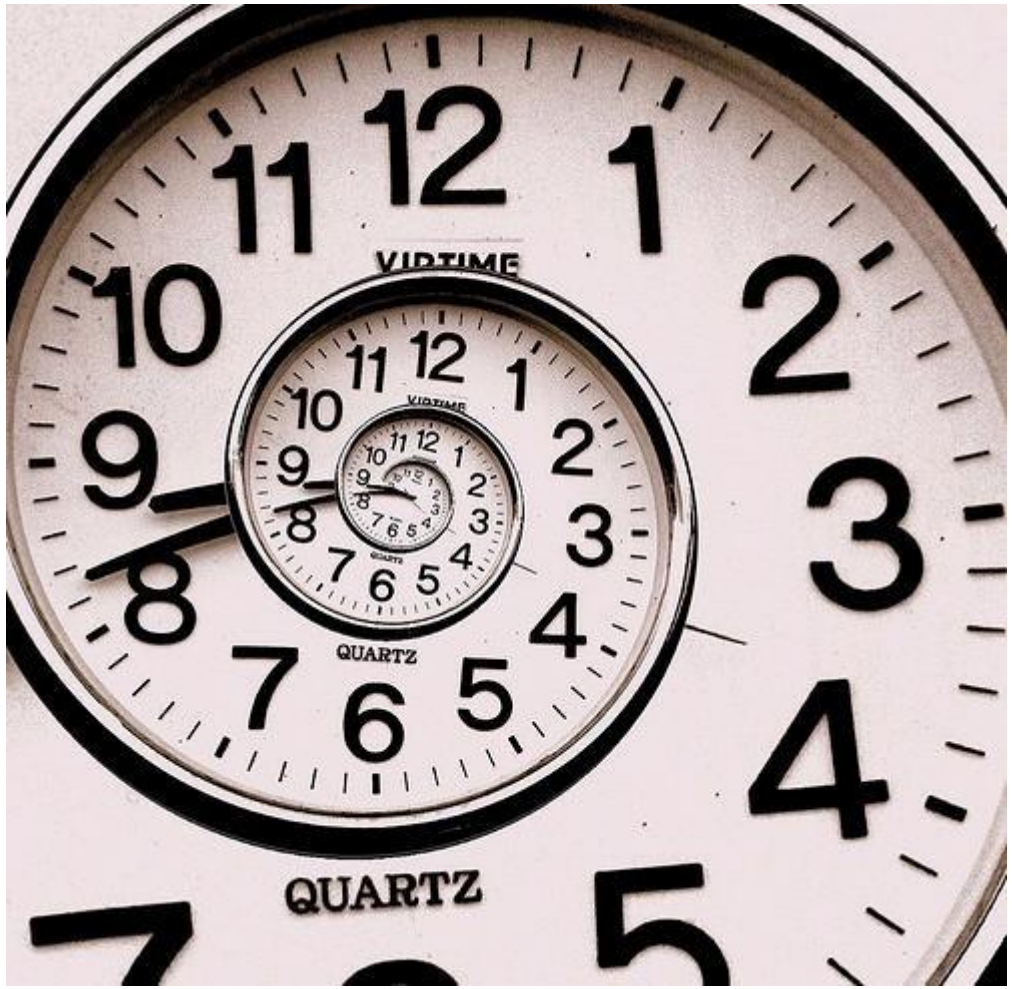
April 2019, CCUF HCD TC, Rome, Italy

Oct. 2017 CCUF MFP TC, Berlin, Germany

Oct. 2018, CCUF HCD TC, Amsterdam, NL

Lessons Learned (1)

- It took much longer than we expected or planned to create or update the HCD PP, so don't expect a new or update PP to be developed quickly either.



Special Thanks

- Alan Sukert, Xerox & Brian Smithson, Ricoh USA
- Eunkyung Yi, IT Security Certification Center (ITSCC)
- HCD WG (ITSCC, JISEC)
- HCD TC
- HCD pre-ITC Subject Matter Experts
- PWG
- JBMIA
- ND iTC
- FDE iTC
- CCUF
- CCDB
- CCMC
- ISO/IEC SC27 WG3

- The 15th CCUF Workshop, September 25-30, 2019, Pan Pacific, Singapore.
- The 14th CCUF Workshop, October 24-29, 2018: Amsterdam, Netherlands.
- The 13th CCUF Workshop, April 2018, Trondheim, Norway.
- The 12th CCUF Workshop, October 2017, Berlin, Germany.
- The 11th CCUF Workshop, April 2017, Amsterdam, Netherlands.
- The 10th CCUF Workshop, November 2016, Reading, UK.
- The 9th CCUF Workshop, April 2016, Seoul, Korea.
- The 8th CCUF Workshop, September 2015, London, UK.
- The 7th CCUF Workshop, April 2015, Canberra, Australia.
- The 6th CCUF Workshop, September 2014, New Delhi, India.
- The 5th CCUF Workshop, March 17 - 20, 2014, Istanbul, Turkey.
- The 4th CCUF Workshop, September 4 - 9, 2013, Orlando, US.
- The 3rd CCUF Workshop, May 13 - 17, 2013.
- CCUF General Membership Meeting, February 25, 2013.
- The 2nd CCUF Workshop, September 11 - 13, 2012, Paris, France.
- The 1st CCUF Workshops, 2012, Cannes, France and Tokyo, Japan.

Lessons Learned (3)

- The Schemes that sponsor an PP or cPP need to commit the necessary resources support from the beginning to the TC/iTC to address questions/concerns/issues as they come up.

- If you pull in requirements into a PP from other PPs or cPPs, ensure these requirements are assessed to make sure they apply to the PP they are being inserted into or modify them so they apply.

Lessons Learned (4)

- Have a plan and process in place from the beginning for updating a PP once it is approved, because updates will be needed.
- Make sure you get the involvement from vendors, consultants, and CCTLs as well as the Schemes in developing the requirements that are to go into a PP.
- Make sure assurance activities are consistent with their corresponding requirements and can be performed by vendors and CCTLs
- Have a process in place from the beginning to obtain interpretations and questions on requirements or assurance activities as the PP is being created, and more importantly, as the PP is being implemented.

HCD TC to HCD iTC Transition

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - Leadership
    - Probably the most important question now -- who will take on the following roles defined in the ToR:
      - iTC Chair
      - Record Manager (aka “Secretary”)
      - Technical Editor(s)
    - How do we determine who takes each role and when will that occur
      - How long the terms of office will be for each of these roles
      - The original thought was that theses roles would be “voluntary” in terms of how they are assigned and the term would be for as long as the volunteers wanted to serve in that role. Do we (or should we) make this more formal?

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - What iTC or TC, if any, should we pattern the formation and processes of the HCD iTC after –
    - Network Device
    - Full Drive Encryption
    - OS
    - Some other TC
    - None of the above
  - Should the HCD iTC implement some type of “NIT” process like the ND iTC has where a small team develops any interpretations needed? If so, how soon after formation of the iTC

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - How should we handle comments against the cPP drafts?
  - How often should the HCD iTC meet
    - We have the Spring and Fall Face-to-Face Meetings as part of the CCUF now; do we need additional Face-to-Face Meetings beyond these two
      - If so, where would we hold them
    - Should we have monthly Conference Calls, and if so how often
  - iTC participation
    - Should we have some type of minimum participation requirement on the part of a voting entity to allow that entity to vote
    - How do we get as many vendors, labs and schemes as possible to participate in the iTC

HCD TC → HCD iTC Transition

- Questions that need to be addressed:
  - How often should we update the ToR
  - How often should we issue updates to the HCD cPP
    - Major version update (e.g., 1.0 → 2.0) once 1-2 years and minor updates at least once every six months
    - Some other cadence
  - Other questions I haven't thought about

Question?