IDS Face-to-Face Minutes
August 10, 2023

Meeting was called to order at approximately 10:00 am ET August 10, 2023.

Attendees –

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

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2023-08-10-IDS-F2F v1.pdf.

- Minute Taker
  - Alan Sukert taking the minutes.

2. Agenda:
   - Introductions, Agenda Review
   - Discuss status of the Hardcopy Device international Technical Community (HCD iTC), the HCD Interpretation Team (HIT and plans for future HCD collaborative Protection Profile (cPP) / HCD Supporting Document (SD) releases since the publishing of v1.0
   - Special Topic on AI Cybersecurity in the EU and US
   - 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, Intellectual Property and Patent policies.

4. Alan went through the current status of the HCD iTC, the HIT and potential content of the next releases of the HCD cPP and HCD SD. Some of the key points from this discussion were:

   - At the current time the HCD iTC is meeting once a month for mostly status on issues. Al the iTC will soon start going to at least meetings every 2 weeks to start looking at some of the potential content for a v1.1, especially given the various issues the HCD iTC is facing (see Slide 18).

     The HCD iTC is currently awaiting Endorsements7 from NIAP (US), ITSCC (Korea) and JISEC (Japan). NIAP is reviewing the HCD cPP as part of a potential certification of the HCD cPP (see the HIT discussion below).

     The CCDB is currently reviewing HCD SD v1.0 as part of the iTC Development process for the HCD iTC. Also, some other (unknown) Schemes may be reviewing the HCD cPP.

     The Canadian Scheme submitted an Endorsement in February 2023. A vendor (Lexmark) is almost ready to begin certification of an HCD against the HCD cPP / HCD SD v1.0 using the Canadian Scheme.

     Kwangwoo Lee (Chair of the HCD iTC) thinks that we may get additional Endorsements at the Fall 2023 CCDB Meeting in Washington DC the end of October.

   - Al then gave the status of the HCD Interpretation Team.as follows:

- The HIT currently has 10 members, which is the desired maximum of 10 members number of HIT members. The current makeup of the HIT is five from HCD vendors, two from Evaluation Labs, one Consultant (AL), and two from Schemes (1 from NIAP and 1 from the Canadian Scheme).
- HIT procedures v1.0 have been finalized and approved by the HIT members and the HD iTC, and the necessary infrastructure was set up by Al. The HIT will be using GitHub for documenting Requests for Interpretation (RfIs) and for creating and tracking the changes to HCD cPP v1.0 and HCD SD v1.0 for approved RFIs. To help Al created a new HCD-IT repository and a new Integration baseline where all the HIT approved changes will be placed and used to create any new v1.0 related releases.
- The HIT had five meetings at the time of this presentation. During these five meetings the HIT processed the following eleven RfIs:

Issue #	Title	Issue
HCD-IT #1	The FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption) SFR in HCD cPP v1.0 is inconsistent with TPM 2.0 Architecture specification section 26.6 “Sensitive Area Encryption**"**	FCS_COP.1/KeyEnc SFR - Case: AES algorithm • AES used in [[selection: CBC, GCM] mode] TPM 2.0 Architecture specification Section 26.6 (Page 172) - "All symmetric encryption of the sensitive area uses Cipher Feedback (CFB) mode." CFB is the only AES mode allowed by the TPM 2.0 specification **No change in status since the last F2F Meeting – Still under review**
HCD-IT #2	Clarification is needed about algorithm verification of Root of Trust in the Test Assurance activities for the Secure Boot SFR	HCD SD Section 2.6.1 FPT_SBT_EXT.1 Extended: Secure Boot, 2.6.1.3 Tests, pg. 59: Add a note in this section saying that the algorithm verification for Root of Trust should be avoided, because authenticity check in Root of Trust should be performed by some kind of immutable code, so the algorithm verification tests should be difficult to perform. **Solution has been developed; Technical Decision being prepared.**
HCD-IT #3	Extraneous "selection" in SFR FCS_CKM.4 Cryptographic key destruction in HCD cPP v1.0	Section 5.3.5, FCS_CKM.4 Cryptographic key destruction on page 33: in FCS_CKM.4.1 the last line of the SFR states "] that meets the following: [selection: no standard]." Since the selection has already been made in the cPP, the "selection:" should be deleted. **Was a duplicate so Issue was Closed**

Issue #	Title	Issue
HCD-IT #4	NIAP APE_ECD.1-5 Evaluation Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_ECD.1-5, The evaluator shall examine the extended components definition to determine that each extended functional component uses the existing CC Part 2 components as a model for presentation. – Gave several example **No change in status since the last F2F Meeting – Starting to make changes**
HCD-IT #5	NIAP APE_REQ.2-5 Evaluation Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-5, The evaluator shall examine the statement of security requirements to determine that all assignment operations are performed correctly. – provides several examples **No change in status since the last F2F Meeting – Starting to make changes**
HCD-IT #6	NIAP APE_REQ.2-8 Assessment Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-8, The evaluator shall examine the statement of security requirements to determine that all refinement operations are performed correctly. -- general inconsistency as to whether an SFR with a refinement in it starts with "Refinement:" or not – several examples noted **No change in status since the last F2F Meeting – Starting to make changes**
HCD-IT #7	NIAP APE_REQ.2-7 Assessment of HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-7, The evaluator shall examine the statement of security

Issue #	Title	Issue
		requirements to determine that all selection operations are performed correctly. -- General inconsistency with regards to whether or not "selection:" prompt is bolded Examples are provided **No change in status since the last F2F Meeting – Starting to make changes**
HCD-IT #8	Update of Application Notes in SFR FPT_KYP_EXT.1 Needed in HCD cPP v1.0 to Clarify Key Storage Conditions	In the discussions by the HIT of Issue HCD-IT #1, one proposed solution to the issue was to use the provisions of SFR FPT_KYP_EXT.1 Extended: Protection of Key and Key Material to address the concern expressed in HCD-IT #1. However, during the discussion it was pointed out that one deficiency of the FPT_KYP_EXT.1 in HCD cPP v1.0 is that the Application Notes for this SFR d not adequately explain what all the conditions in SFR FPT_KYP_EXT.1.1 that pertain to the storage of keys are. This issue is to request that the Application Notes in SFR FPT_KYP_EXT.1 be modified to more clearly explain what each of the conditions for key storage mean in SFR FPT_KYP_EXT.1.1. **Awaiting Review – Working on the exact wording of the revised Application Notes for SFR FPT_KYP_EXT.1 and what condition really applies here.**
HCD-IT #9	Modification proposal : tests for FDP_DSK_EXT.1.	This SFR should be satisfied and certified if encryption of any confidential data will not depend on a user electing to protect that data. However current test description is limited to perform writing to the storage device with “operating TSFI“ which enforce write process of User documents and Confidential TSF data. Therefore, a functionality which does not have such TSFI and the data cannot be tested and certified even if the TOE function is satisfied with the SFR. This situation should be corrected. For more detail, SWAP and Core dump etc., are written User documents and Confidential TSF data to storage device

Issue #	Title	Issue
		by system (OS) at any timing as necessary. SWAP and Core dump etc., doesn't write any User documents and Confidential TSF data when TSFI is operated. **Awaiting Review – this was a legacy issue. The issue is in Section 3.1.3.4 of the SD; specifically Test 1 for FDP_DSK_EXT.1which explicitly requires an operating TSFI, but encryption of data stored on a storage device needs to be done without user intervention, meaning there is no TSFI involved.** **Working to modify the tests in Section 3.1.3.4 to remove the references to TSFIs in verifying the written data is properly encrypted**
HCD-IT #10	Mapping issue between Mandatory 'O.KEY_MATERIAL' objective and Cond. Mandatory FPT_KYP_EXT.1	[APE_REQ.2-11] According to HCD cPP I.6, "O.KEY_MATERIAL" is defined as a mandatory objective. I.9 maps "O.KEY_MATERIAL" only to "FPT_KYP_EXT.1" which is a conditionally mandatory SFR. This creates scenarios where mandatory "O.KEY_MATERIAL" security objective cannot be satisfied when FPT_KYP_EXT.1 is not claimed as per conditions are not met (Section 1.4.2 "USE CASE 2: Conditionally Mandatory Use Cases"). Additional details: I reviewed the following GitHub issue on cPP Draft where I believe the decision was made to remove O.KEY_MATERIAL from being "conditionally mandatory". However, no information is found on how this change affects the mapping: HCD-iTC/HCD-iTC-Template#238 **Awaiting Review – This came from the Canadian Scheme's review of HCD cPP v1.0. Issue is that OSP O.KEY_MATERIAL is mapped to SFR FPT_KYP_EXT.1 which is a "Conditionally Mandatory" SFR. Means that OSP O.KEY_MATERIAL would only apply conditionally in cases where , for example, an HCD had hard disks and would not apply to TSF data stored in wear-leveling devices such as SSDs.**

Issue #	Title	Issue
		Best solution is to map O.KEY_MATERIAL to a mandatory SFR like FPT_SKP_EXT.1 Extended: Protection of TSF Data.
HCD-IT #11	In FCS_CKM.4 Cryptographic key destruction, clarification needed whether encrypted keys stored in non-volatile memory are within the scope of key destruction	**Awaiting Review – This issue was submitted by Shin-ichi Inoue of Ecsec Laboratory** **For Section 5.3.5 FCS_CKM.4 Cryptographic key destruction in the HCD cPP, it is not clear that encrypted keys stored in non-volatile memory is within the scope of key destruction. Suggested change is to describe in an Application Note whether encrypted keys stored in non-volatile memory are within the scope of key destruction or not.** **The key to the issue is the word "encrypted" in the Issue statement. This Issue is also linked to Section 5.3.4, SFR FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction and SFR 5.3.4.1 which states "FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed." The central question of this issue – should we be destroying all keys or just plaintext keys. The HIT is divided on the answer to this question**

- HCD-IT #`1 – HCD-IT #7 were covered in detail at the 5/19/23 IDS Face-to-Face Session.

  For HIT-IT #8, this issue came about from the discussion of HCD-IT #1, where it became apparent that it was not clear what the various cases in SFR FPT_KYP_EXT.1 meant. So, the HIT agreed that the Application Notes for this SFR should be updated to provide this necessary clarification.

  Two HIT members have been working on this issue. One of the two members working on this issue feels that the HCD iTC changed the intent of **FPT_KYP_EXT.1** from what it originally was when it was taken from the FDE EE cPP. As a result, the two situations - a key in protected storage already and a key from a TPM protecting another set of keys are the same scenario.

  The other member, who originally make the proposal that resulted in **FPT_KYP_EXT.1** in its current form in the HCD cPP, showed that the two conditions are actually different - Condition A is where "the Application encrypts or decrypts initial value of key chain by TPM-owned key (another key) (i.e., the key is unsealed by the TPM)"; Condition B is where "the Application stores or loads the initial value of the key chain in protected storage area" (i.e., the key is protected by the TPM).

  The two members are still working on the wording for the Application Notes.

- For HIT-IT #9, this was a legacy issue. The issue is in Section 3.1.3.4 of the HCD SD for SFR **FDP_DSK_EXT.1**; specifically Test 1 which reads:

  Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data.

  The issue is that this test explicitly requires an operating TSFI, but encryption of stored on a storage device needs to be done without user intervention, meaning there is no TSFI involved..

  The suggestion is just to modify the tests in Section 3.1.3.4 to remove the references to TSFIs in verifying the written data is properly encrypted; a proposed change is being worked.

- HIT-IT #10 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.

  FPT_KYP_EXT.1 is a “Conditionally Mandatory” SFR, which would mean that OSP O.KEY_MATERIAL would only apply conditionally in cases where **FPT_KYP_EXT.1** applied such as 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 general consensus was that the best solution was to map O.KEY_MATERIAL to a mandatory SFR like **FPT_SKP_EXT.1 Extended: Protection of TSF Data**. This issue being reviewed for a potential solution.

- HIT-IT #11 - The key to the issue is the word “encrypted” in the Issue statement. This Issue is also linked to SFR **FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction** and SFR 5.3.4.1 which states “**FCS_CKM_EXT.4.1** The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.”

  SFRs **FCS_CKM_EXT.4** and **FCS_CKM.4** were taken from the ND cPP v2.2e originally; The original idea for **FCS_CKM.4** was that it applies to all keys, including encrypted keys, and not just plaintext keys. However, since **FCS_CKM_EXT.4** only applies to “plaintext secret and private cryptographic keys and cryptographic critical security parameters”, someone looking at the HCD cPP could imply that **FCS_CKM.4** only applies to plaintext keys also.

  On the other hand, although **FCS_CKM.4** does not explicitly state that it applies to encrypted keys it could be interpreted to apply to non-volatile memory and to encrypted keys. There was even a suggestion of defining via an Application Note that a “cryptographic key” is.

  Therefore, the central question of this issue – should we be destroying all keys or just plaintext keys. The HIT is divided on the answer and further discussion s are on-going. Al noted at the meeting this could be the first Issue that could require a vote by the HIT to resolve.

- As far as HIT-related releases, there will definitely need to be an Errata release for HCD cPP v1.0 and HCD SD v1.0 address the NIAP and Canadian Scheme evaluation comments (at a minimum) and possibly fixes for any completed Issues.
- As far as additional standalone HCD cPP or HCD SD v1.0.x releases after the initial Errata release. if there will be any such releases and how many of these releases will occur likely depend on comments we get from:
  - The review of the HCD SD from the CCDB
  - The review of the HCD cPP from the other Schemes and
  - The current Lexmark certification and future certifications against HCD cPP or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme

  Note: The nature and severity of the comments will probably determine whether comments against HCD cPP or HCD SD v1.0 get fixed in a v1.0 release or get fixed in a later version
- The "Post v1,0 Release Plan" slide was changed this time to reflect that there are four key issues that will likely drive what content will go into the next and future releases of the HCD cPP and HCD SD, These four issues, in order of priority from high to low, are:
  - CCDB Specification of Functional Requirements for Cryptography
  - CC:2022 Compliance
  - Syncing with ND cPP / SD v3.0
  - Commercial National Security Algorithm (CNSA) 2.0

  The next few slides provided details on these four issues.
- The draft CCDB Specification of Functional Requirements for Cryptography was issued the beginning of July 2023 with comments due Juy 31, 2023. It is a draft Specification from the Common Criteria Development Board (CCDB) Crypto Working Group of key cryptographic SFRs that are commonly used in cPPs. Al indicated that it appears from his examination of the draft document that the text of the SFRs in the draft Specification either:
  - Came from the CC:2022 FCS Class SFRs, **although interestingly some of them were changed**; (Al emphasized this later point at the meeting which is why it is bolded in these notes)
  - Were created by the CCDB Crypto Working Group; or
  - May have come from the modified text of crypto SFRs in various cPPs

  Some of the review comments from the HCD iTC against the draft Specification were:
  - Are all of the SFRs in the Specification mandatory or can an iTC pick the ones they need like we can do in CC:2022 Part 2?
  - Is "Exact Conformance" to the SFRs in the Specification required or can an iTC add additional requirements to the SFRs?
  - If a PP or cPP already has a version of one of the SFRs that is in the Specification that is different from the version in the Specification, are the iTCs required to use the version in the specification?
  - Will the necessary Assurance Activities for each of the SFRs in the Specification be provided? Al indicated the SFRs in the Spec really can't be adequately assessed without knowing how the SFRs will be evaluated
  - What is the transition plan for the SFRs in the Specification when published? Al indicated this is the key question for the HCD iTC – when will we have to switch to the SFRs in the Spec to get of a certified HCD on the NIAP Product Compliant List for example.

  Al had looked at the SFRs in the draft Spec and did a comparison with the corresponding SFRs in HCD cPP v1.0. The keys differences he found were:

- Many SFRs in the draft Spec added additional algorithms, key sizes and applicable standards not included in the HCD cPP versions of those SFRs
- The draft Spec uses the FCS_CKM key management SFRs from CC:2022 which are different from the FCS_CKM key management SFRs in the HCD cPP. However:
  - Draft Spec added two 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
  - Draft Spec SFR made changes to the version of **FCS_CKM_EXT.3 Cryptographic Key Access** from CC:2022
- The draft Spec took the **FCS_RBG** family from CC:2022, but 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; the draft Spec has separate SFRs for Signal Generation (**FCS_COP.1/SigGen Cryptographic Operation (Signature Generation)**) and Signal Verification (**FCS_COP.1/SigVer Cryptographic Operation (Signature Verification)**)
- The draft Spec version of SFR **FCS_KYC_EXT.1 Extended: Key Chaining** is completely different from the version of this SFR in the HCD cPP

The differences Al found most interesting were the changes the draft Spec made to the CC:2022 SFRs and the splitting of **FCS_COP/1/SigGen** into separate SFRs for Signal Generation and Signal Verification.

- Slide 21 presented the rules for transitioning from CCv3.1R5 to CC:2022 in terms of certifications against PPs/CPPs. The one rule Al discussed was the key rule that will drive the HCD iTC:
  - Product certifications based on CC v3.1 R5 against a PP or PP configuration claiming exact conformance may be started until 31st of December 2025

  This means that any certification against an “exact conformance” PP like the HCD cPP after Jan 1, 2026 must be against CC:2022. So, by Jan 1, 2026 the HCD cPP must be CC:2022 compliant.

  Al looked at some of the key changes in the CC:2022 Part 2 SFRs, and they were:
  - **FAU_GEN.1 Audit data generation** and some of the other FAU Class SFRs changed from requiring “audit reports” to requiring “audit data”. This is not a subtle change, depending on how CC:2022 defines “audit data”.
  - **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 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:
    - **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_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

Al will look into the other CC:2022 parts to see what differences there might impact the HCD iTC.

- Al then looked at some of the key new content that was included in the published ND cPP v3.0, based on a comparison between ND cPP v3.0 and ND cPP v1.0, that the H CD cPP should look at for potential inclusion in the next update of the HCD cPP (and by extension the HCD SD for the associated Assurance Activities):
  - Claim conformance to NIAP Functional Package for SSH
  - Updates to TLS and DTLS SFRs to incorporate TLS 1.3 and removal of TLS 1.1
  - Inclusion of new SFRs under SFRs **FAU_STG_EXT.1 External Audit Trail Storage, FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication, FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication, FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication, FCS_DTLSC_EXT.2 DTLS Client Support for Mutual Authentication** and **FPT_STM.1 Reliable Time Stamps**
  - Inclusion of new SFRs **FCS_TLSC_EXT.3 TLS Client Support for secure renegotiation (TLSv1.2 only)** and **FCS_TLSS_EXT.3 TLS Server Support for secure renegotiation**
  - Inclusion of Optional Security Assurance Requirements for Flaw Remediation (ALC_FLR)
  - Added additional requirements to several crypto SFRs like FCS_CKM.4 Cryptographic Key Destruction and FCS_RBG_EXT.1 Random Bit Generation

  Although all of these are important, the key ones are the updates to include TLS 1.3 and remove TLS 1.1, updating the SSH SFRs from the NIAP Functional Package for SSH SFRs (which are very different from the existing SSH SFRs in the HCD cPP) so the HCD cPP can claim conformance to that package, and the inclusion of the optional ALC_FLR assurance activities which are being added to mesh with the EUCC requirements which makes ALC_FLR mandatory.

  As a side note, Ira indicated that the ND iTC TLS Subcommittee was meeting with NIAP SMEs to try to address the multiple NIAP comments (mostly against TLS and DTLS) against ND cPP v3.0,

- Regarding CNSA 2.0, Al just pointed to the chart below that showed the CNSA 2.0 algorithms:

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

- Slide 25 showed the original NIAP transition plan for CNSA 2.0, which had LMSS integrated into NIAP PPs by 1H 2023. That, of course, has not happened. The HCD iTC will wait until NIAP comes up with its new CNSA 2.0 transition plan for how iTCs will integrate CNSA 2.0 algorithms into cPPs before taking any action.
- Al then listed, based on the above discussions, his view of the likely potential content for the next update to the HCD cPP/SD, whe6her it be a v1.1 or v2.0:
  - Incorporation of the SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
    - We don‘t know what either the CCDB or the various Schemes are going to require with respect to the “Crypto Spec” yet
  - Updates for the relevant changes in CC:2022
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1, including updates to TLS and DTLS and other relevant changes per ND cPP/SD 3.0
  - Incorporate the NIAP Functional Package for SSH so can claim conformance to it
  - Inclusion of AVA_VAN and ALC_FLR.*
  - Initial implementation of CNSA 2.0 algorithms
    - Inclusion of SHA-384 and SHA-512 and possible inclusion of LMS as an option likely first steps
  - Changes due to any approved RfIs (Issues) to HCD cPP/SD v1.0
    - Will have to decide if only include changes approved by NIAP
  - Inclusion of NTP (Al thinks we have to include this because the industry uses NTP to set time on HCDs)
  - Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes
- The list of changes that could go in future releases likely beyond the next update to the HCD cPP/SD is essentially the same as it was for the May 18th IDS Face-to-Face Meeting, but some new items were added (the items in bold are the ones AL feels should be the higher priority items on the list):
  - **Full implementation of CNSA 2.0**
  - **Support for any new crypto algorithms**
  - **NIAP IPsec Package or other new NIAP Packages**
  - **Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs**
  - **Updates to Address 3D printing and the Digital Thread to Additive Manufacturing**
  - **Support for Cloud Printing**
  - **Support for Artificial Intelligence**
  - **Support for Wi-Fi**
  - **Any new CCDB Crypto WG or CCUF Crypto WG Packages or Specifications**
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Support for SNMPv3
  - Support for NFC
  - Updates based on new technologies, customer requests or government mandates

- Syncing with newer updates to ND and FDE cPPs/SDs

- Next steps for the HCD iTC are:
  - Continue HIT activities for maintaining HCD cPP/SD v1.0 and issue the necessary TDs/TRs and Errata to address all documented RfIs
  - Determine HCD cPP/HCD SD release plan for both v1.0 and updated versions
  - Determine the content for and then create the next HCD cPP/SD releases for both v1.0 and v1.1 or V2.0, whichever is next
  - Fully engage the HCD iTC to work on the next update to the HCD cPP and HCD SD
  - Engage in long-range planning to determine what content will be needed in the HCD cPP/SD in the 3-5 year range and beyond. This last bullet is new and reflects Al's view that the HCD iTC has to start thinking about what will be this necessary content 3-5 years from now, especially given CNSA 2.0 and its 2030 deadline.

- The set of "Lessons Learned" was spawned by a comment Smith made at the last IDS WG Meeting and reflects Al's thoughts on his 19+ years working on developing PPs and cPPs:
  - You really have to love this type of work (or be a little crazy) to do it well, because it is very time consuming, very exhausting and very frustrating work
  - It is also a long-term time commitment that one has to be willing to make
  - Patient is a definite virtue in working on a Technical Community developing PPs/cPPs because nothing happens as quickly as you want it to happen or as smoothly as you want it to happen
  - Common Criteria (CC) is very complex, so you need to focus on those parts of the CC that support what you are trying to accomplish – I am still learning things about CC even after 19 years of working with it
  - Biggest lesson I learned on the HCD iTC – establish and agree on your procedures and then follow them even when it hurts; every time you don't you get yourself into self-inflicted trouble

5. Al then went through his special topic on AI Cybersecurity in the EU and US. The topic consisted of two parts - a look at the EU Artificial Intelligence (AI) Act and a look at US AI-Related Legislation.

   EU Artificial Intelligence (AI) Act

   - The slides for this portion of the special topic were taken from a presentation Al gave at the 1/26/23 IDS WG Meeting. The slides for that presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/AI Act.pdf.

     Al noted that the EU AI Act still has not formally become law in the EU yet, but as of the middle of 2023 the EU has finalized its negotiating position which is a big step towards becoming a law.

   - The scope of the EU AI Act is:
     - Providers placing on the market or putting into service AI systems in the Union, irrespective of Providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country
     - Users of AI systems located within the Union
     - Providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union
     - Not apply to AI systems developed or used exclusively for military purposes
     - Not apply to public authorities in a third country nor to international organizations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organizations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States

     The key here is that this Act is meant to apply to the providers and users of AI systems.

- The EU AI Act prohibits the following:
  - The placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm
  - The placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behavior of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm
  - The placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behavior or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:
    - Detrimental or unfavorable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
    - Detrimental or unfavorable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behavior or its gravity

  Note that the emphasis here is on preventing AI systems from having a behavioral impact on users.

- The main focus of the EU AI Act is on Hi-Risk AI Systems, which are defined as AI Systems that meet both of the following conditions:
    - The AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonization legislation listed in Annex I of the EU AI Act (Note: Annex ! addresses "AI Techniques and Approaches")
    - The product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonization legislation listed in Annex II of the EU AI Act (Note: Annex !I is a list of EU Regulations that the EU AI Act must harmonize with – it is two full pages of EU Regulations which shows how big the issue of harmonization is within the EU).

  AI Systems can be added to the list of Hi-Risk AI Systems if they meet both of the following conditions:
    - The AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III
    - The AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III

  The following are types of Hi-Risk AI Systems:
  - Biometric identification and categorization of natural persons:
    - AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons
  - Management and operation of critical infrastructure
    - AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity
  - Education and vocational training:
    - AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions

    - AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions
  - Employment, workers management and access to self-employment:
    - AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests
    - AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships
  - Access to and enjoyment of essential private services and public services and benefits:
    - AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services
    - AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use
    - AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid
  - Law enforcement:
    - AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences
    - AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person
    - AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in this regulation
    - AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences

  You can see that in general Hi-Risk AI Systems deal with areas involving biometrics, educational, public service and law enforcement uses of AI.
- Requirements paced on Hi-Risk AI Systems by the EU AI Act involve several areas:,
  - The requirements for testing of a Hi-Risk AI System are typical test requirements. Specifically, High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria:
    - Training, validation and testing data sets shall be subject to appropriate data governance and management practices
    - Training, validation and testing data sets shall be relevant, representative, free of errors and complete
    - Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioral or functional setting within which the high risk AI system is intended to be used
    - Appropriate data governance and management practices shall apply for the development of high-risk AI systems
  - There are also requirements (see Slide 38) for technical documentation of a Hi-Risk AI system to be drawn up before that system is placed on the market or put into service and be kept up-to date and for record-keeping in the form of logs – it is not clear whether this is

referring to paper logs, audit logs, or some other type of “log”. The record-keeping requirements include enablement of automatic recording of events while the high-risk AI systems is operating.

Record-keeping is required to collect, as a minimum:

- Recording of the period of each use of the system (start date and time and end date and time of each use)
- The reference database against which input data has been checked by the system
- Input data for which the search has led to a match
- Identification of the natural persons involved in the verification of the results

- Slides 39 and 40 list other requirements for Hi-Risk AI systems that are related to human oversight and design and development of high-risk AI systems. A couple of key ones are:
  - High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system’s output and use it appropriately
  - High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users
  - Human oversight shall aim at preventing or minimizing the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse
  - High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems
  - High-risk AI systems shall be resilient as regards attempts by unauthorized third parties to alter their use or performance by exploiting the system vulnerabilities

  Ira commented that resiliency of AI systems hasn’t been achieved yet because the issue of poisoning of input data sets for AI systems still hasn’t been solved.

- Slides 41 and 42 provide a list of requirements for the providers Hi-Risk AI systems. Many of these requirements are what would be expected - like “Put a quality management system in place that ensures compliance with this Regulation” or “Immediately take the necessary corrective actions if non-conformities are found to bring that system into conformity, to withdraw it or to recall it, as appropriate”. A few of the more interesting beyond these expected ones are:
  - Implementation of written policies, procedures and instructions shall be proportionate to the size of the provider’s organization
  - Affix the marking to their high-risk AI systems to indicate the conformity with the AI Act
  - Upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with requirements
  - That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions and shall be proportionate to the size of the provider’s organization
  - Ensure that their systems undergo the relevant conformity assessment procedure in accordance with the AI Act prior to their placing on the market or putting into service
  - Logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law
  - Inform the distributors of the high-risk AI system in question and, where applicable, the authorized representative and importers accordingly

- Users of Hi-Risk AI Systems also have requirements per the EU AI Act. These requirements are:
  - Use such systems in accordance with the instructions of use accompanying the systems
  - To the extent the user exercises control over the input data, ensure that input data is relevant in view of the intended purpose of the high-risk AI system
  - Monitor the operation of the high-risk AI system on the basis of the instructions of use
  - When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of AI Act, inform the provider or distributor and suspend the use of the system
  - Inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of the AI Act and interrupt the use of the AI system
  - Keep the logs automatically generated by that high-risk AI system, to the extent such logs are under their control
  - Use the information provided under the AI Act to comply with their obligation to carry out a data protection impact assessment

  Al indicated there were nothing unique in these user requirements.

US AI-Related Legislation

The slides for the first four topics came from a presentation given at the 6/22/23 IDS WG Meeting and can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/US AI Legislation.pdf. The slides for the NIST AI Risk Management Framework came from a presentation given at the 1/26/23 IDS WG Meeting and can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST AI Risk Management Framework v2.pdf

a. AI in Government Act of 2020

- This was not a standalone law; it was actually Division U of the Consolidated Appropriations Act, 2021. Its purpose was to create the AI Center of Excellence (AI CoE) to:
  - Facilitate the adoption of artificial intelligence technologies in the Federal Government; and
  - Improve cohesion and competency in the adoption and use of artificial intelligence within the Federal Government
- The duties of the AI CoE were to be:
  - Regularly convening individuals from agencies, industry, Federal laboratories, nonprofit organizations, institutions of higher education, and other entities to discuss recent developments in artificial intelligence;
  - Collecting, aggregating, and publishing on a publicly available website information regarding programs, pilots, and other initiatives led by other agencies and any other information determined appropriate by the Administrator;
  - Advising the Administrator, the Director, and agencies on the acquisition and use of artificial intelligence through technical insight and expertise, as needed;
  - Assist agencies in applying Federal policies regarding the management and use of data in applications of artificial intelligence;
  - Consulting with agencies, including the Department of Defense, the Department of Commerce, the Department of Energy, the Department of Homeland Security, the Office of Management and Budget, the Office of the Director of National Intelligence, and the National Science Foundation, that operate programs, create standards and guidelines, or otherwise fund internal projects or coordinate between the public and private sectors relating to artificial intelligence;

- Advising the Director on developing policy related to the use of artificial intelligence by agencies
- Advising the Director of the Office of Science and Technology Policy on developing policy related to research and national investment in artificial intelligence

- The law includes the following requirement with respect to providing guidance to Federal Agency use of AI:

  No later than 270 days after enactment of this act the Director of the Office of Management and Budget (OMB) shall issue a memorandum to the head of each agency that shall—

  - Inform the development of policies regarding Federal acquisition and use by agencies regarding technologies that are empowered or enabled by artificial intelligence, including an identification of the responsibilities of agency officials managing the use of such technology;
  - Recommend approaches to remove barriers for use by agencies of artificial intelligence technologies in order to promote the innovative application of those technologies while protecting civil liberties, civil rights, and economic and national security;
  - Identify best practices for identifying, assessing, and mitigating any discriminatory impact or bias on the basis of any classification protected under Federal nondiscrimination laws, or any unintended consequence of the use of artificial intelligence, including policies to identify data used to train artificial intelligence algorithms as well as the data analyzed by artificial intelligence used by the agencies; and
  - Provide a template of the required contents of the agency plans
- Another requirement in the law was that not later than 180 days after the date on which the Director of the OMB issues the memorandum required under subsection (a) or an update to the memorandum required under subsection (d), the head of each agency shall submit to the Director and post on a publicly available page on the website of the agency:
  - (1) a plan to achieve consistency with the memorandum; or
  - (2) a written determination that the agency does not use and does not anticipate using artificial intelligence.
  - UPDATES.—Not later than 2 years after the date on which the Director of the OMB issues the memorandum required under subsection (a), and every 2 years thereafter for 10 years, the Director of the OMB shall issue updates to the memorandum

Al noted that this law applied only to the Federal Government only and these duties had no impact on AI activities or issues for activities performed outside of the Federal Government. This is true of all of the legislation and Executive Orders, which is different from the scope of the EU AI Act.

b. National Artificial Intelligence Initiative Act of 2020

The National Artificial Intelligence Initiative Act of 2020 was also not a standalone act; it was Division E, Section 5001 of the “WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021”.

One of the interesting things in this law was how it “defined” Artificial Intelligence - ‘‘artificial intelligence’’ means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action. It is definitely not the definition we are used to seeing for AI.

The stated purposes of this law were to:

- Ensure continued United States leadership in artificial intelligence research and development;

- Lead the world in the development and use of trustworthy artificial intelligence systems in the public and private sectors;
- Prepare the present and future United States workforce for the integration of artificial intelligence systems across all sectors of the economy and society; and
- Coordinate ongoing artificial intelligence research, development, and demonstration activities among the civilian agencies, the Department of Defense and the Intelligence Community to ensure that each informs the work of the others

The National Artificial Intelligence Initiative that this law created was to perform the following activities:

- Sustained and consistent support for artificial intelligence research and development through grants, cooperative agreements, testbeds, and access to data and computing resources
- Support for K-12 education and postsecondary educational programs, including workforce training and career and technical education programs, and informal education programs
- Support for interdisciplinary research, education, and workforce training programs for students and researchers that promote learning in the methods and systems used in artificial intelligence and foster interdisciplinary perspectives and collaborations among subject matter experts in relevant fields
- Interagency planning and coordination of Federal artificial intelligence research, development, demonstration, standards engagement, and other activities under the Initiative, as appropriate
- Outreach to diverse stakeholders, including citizen groups, industry, and civil rights and disability rights organizations
- Leveraging existing Federal investments to advance objectives of the Initiative
- Support for a network of interdisciplinary artificial intelligence research institutes
- Support opportunities for international cooperation with strategic allies, as appropriate, on the research and development, assessment, and resources for trustworthy artificial intelligence systems

The law established roles for three National AI Research Institutes – the National Institute of Standards and Technology (NIST), the National Oceanic and Atmospheric Administration Artificial Intelligence Center and the National Science Foundation (NSF).

- For NIST, there were several key roles mentioned in the law (see the details in Slide 54, but the two that are most relevant are:
  - Support and strategically engage in the development of voluntary consensus standards, including international standards, through open, transparent, and consensus-based processes
  - RISK MANAGEMENT FRAMEWORK.—Not later than 2 years after the date of the enactment of this Act, the Director shall work to develop, and periodically update, in collaboration with other public and private sector organizations, including the National Science Foundation and the Department of Energy, a voluntary risk management framework for trustworthy artificial intelligence systems

  This law explicitly required NIST to create the AI Risk Management Framework that will be discussed later in this special topic.
- The National Oceanic and Atmospheric Administration Artificial Intelligence Center is under the National Oceanic and Atmospheric Administration (NAOA) and is responsible for tasks such as:
  - (1) coordinate and facilitate artificial intelligence research and innovation, tools, systems, and capabilities across the National Oceanic and Atmospheric Administration;

- (2) establish data standards and develop and maintain a central repository for agency-wide artificial intelligence applications; and
- (3) accelerate the transition of artificial intelligence research to applications in support of the mission of the National Oceanic and Atmospheric Administration

See Slide 55 for more details. Al noted he was surprised NAOA was involved in AI research and development, but was reminded that NAOA deals with things such as long-range weather forecasting where AI can be very useful.

- Some of the AI-related tasks the NSF is responsible for are:
  - (1) support research, including interdisciplinary research, on artificial intelligence systems and related areas;
  - (2) use the existing programs of the National Science Foundation, in collaboration with other Federal departments and agencies, as appropriate to — (A) improve the teaching and learning of topics related to artificial intelligence systems in K-12 education and postsecondary educational programs; and (B) increase participation in artificial intelligence related fields;
  - (3) support partnerships among institutions of higher education, Federal laboratories, nonprofit organizations, State, local, and Tribal governments, industry, and potential users of artificial intelligence systems that facilitate collaborative research, personnel exchanges, and workforce development;
  - (4) ensure adequate access to research and education infrastructure with respect to artificial intelligence systems.

  See Slide 56 for more details.

c. Executive Order 13859 Maintaining American Leadership in Artificial Intelligence

This Executive Order (EO) was issued February 11, 2019.

A couple of definitions that were included in this EO were:

- ‘artificial intelligence’’ means the full extent of Federal investments in AI, to include: R&D of core AI techniques and technologies; AI prototype systems; application and adaptation of AI techniques; architectural and systems support for AI; and cyberinfrastructure, data sets, and standards for AI; and
- ‘‘open data’’ shall, in accordance with OMB Circular A– 130 and memorandum M–13–13, mean ‘‘publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.

Note that the artificial intelligence definition is really not a definition.

The principle of this EO were to:

- Drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies
- Train current and future generations of American workers with the skills to develop and apply AI technologies
- Foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application
- Promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations

The objectives of this EO include:

- Promote sustained investment in AI R&D in collaboration with industry, academia, international partners and allies, and other non-Federal entities

- Enhance access to high-quality and fully traceable Federal data, models, and computing resources to increase the value of such resources for AI R&D, while maintaining safety, security, privacy, and confidentiality protections consistent with applicable laws and policies
- Reduce barriers to the use of AI technologies to promote their innovative application while protecting American technology, economic and national security, civil liberties, privacy, and values
- Ensure that technical standards minimize vulnerability to attacks from malicious actors and reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies; and develop international standards to promote and protect those priorities
- Train the next generation of American AI researchers and users through apprenticeships; skills programs; and education in science, technology, engineering, and mathematics (STEM), with an emphasis on computer science, to ensure that American workers, including Federal workers, are capable of taking full advantage of the opportunities of AI
- Develop and implement an action plan to protect the advantage of the United States in AI and technology critical to United States economic and national security interests against strategic competitors and foreign adversaries

The Initiative was to be coordinated through the National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence (Select Committee); any actions were to be implemented by agencies that conduct foundational AI R&D, develop and deploy applications of AI technologies, provide educational grants, and regulate and provide guidance for applications of AI technologies

Heads of all agencies were to review their Federal data and models to identify opportunities to increase access and use by the greater non-Federal AI research community in a manner that benefits that community, while protecting safety, security, privacy, and confidentiality. In identifying data and models for consideration for increased public access, agencies were to consider issues such as:

- Privacy and civil liberty protections for individuals who may be affected by increased access and use, as well as confidentiality protections for individuals and other data providers; and
- Safety and security concerns, including those related to the association or compilation of data and models

Finally, Heads of implementing agencies that also provide educational grants were to, to the extent consistent with applicable law, consider AI as a priority area within existing Federal fellowship and service programs. Eligible programs for prioritization were to give preference to American citizens, to the extent permitted by law, and were to include:

- High school, undergraduate, and graduate fellowship; alternative education; and training programs;
- Programs to recognize and fund early-career university faculty who conduct AI R&D, including through Presidential awards and recognitions;
- Scholarship for service programs;
- Direct commissioning programs of the United States Armed Forces; and
- Programs that support the development of instructional programs and curricula that encourage the integration of AI technologies into courses in order to facilitate personalized and adaptive learning experiences for formal and informal education and training

d. Executive Order 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government

This EO was issued on December 3, 2020, and was intended to::

- Promote the innovation and use of AI, where appropriate, to improve Government operations and services in a manner that fosters public trust, builds confidence in AI, protects our

Nation's values, and remains consistent with all applicable laws, including those related to privacy, civil rights, and civil liberties

- Ensure that responsible agencies shall, when considering the design, development, acquisition, and use of AI in Government, be guided by the common set of Principles which are designed to foster public trust and confidence in the use of AI, protect our Nation's values, and ensure that the use of AI remains consistent with all applicable laws, including those related to privacy, civil rights, and civil liberties

The main objective of this EO was that when designing, developing, acquiring, and using AI in the Federal Government, agencies shall adhere to the following Principles:

- Lawful and respectful of our Nation's values (including those addressing privacy, civil rights, and civil liberties)
- Purposeful and performance-driven (where the benefits of developing AI significantly outweigh the risks, and the risks can be assessed and managed)
- Accurate, reliable, and effective (the application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective)
- Safe, secure, and resilient
- Understandable (the operations and outcomes of their AI applications are sufficiently understandable by subject matter experts, users, and others, as appropriate)
- Responsible and traceable (that human roles and responsibilities are clearly defined, understood, and appropriately assigned for the design, development, acquisition, and use of AI)
- Regularly monitored (AI applications are regularly tested against the Principles of this EO)
- Transparent (Agencies shall be transparent in disclosing relevant information regarding their use of AI to appropriate stakeholders)
- Accountable (Agencies shall be accountable for implementing and enforcing appropriate safeguards for the proper use and functioning of their applications of AI)

In terms of the scope of this EO:

- The Principles and implementation guidance in this order shall apply to AI designed, developed, acquired, or used specifically to advance the execution of agencies' missions, enhance decision making, or provide the public with a specified benefit
- This order applies to both existing and new uses of AI; both standalone AI and AI embedded within other systems or applications; AI developed both by the agency or by third parties on behalf of agencies for the fulfilment of specific agency missions, including relevant data inputs used to train AI and outputs used in support of decision making; and agencies' procurement of AI applications
- This order does not apply to:
    - AI used in defense or national security systems, in whole or in part, although agencies shall adhere to other applicable guidelines and principles for defense and national security purposes, such as those adopted by the Department of Defense and the Office of the Director of National Intelligence;
    - AI embedded within common commercial products, such as word processors or map navigation systems, while noting that Government use of such products must nevertheless comply with applicable law and policy to assure the protection of safety, security, privacy, civil rights, civil liberties, and American values; and
    - AI research and development (R&D) activities, although the Principles and OMB implementation guidance should inform any R&D directed at potential future applications of AI in the Federal Government

Ira noted that wording of the bullet that states this does not apply to commercial products actually says it does apply to commercial products because it says the Government uses these products

and the first bullet states that "shall apply to AI designed, developed, **acquired, or use**d specifically to advance the execution of agencies' missions, enhance decision making, or provide the public with a specified benefit".

e. NIST AI 100.1 NIST AI Risk Management Framework (AI RMF 1.0)

Because of time constraints this was a very brief look at the NIST AI Risk Management Framework.

NIST AI 100.1 was published in January 2023. Its main goals of the NIST AI Risk Management Framework (RMF) were to:

- Offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems.
- Be ***voluntary***, rights-preserving, non-sector-specific, and use-case agnostic, providing flexibility to organizations of all sizes and in all sectors and throughout society to implement the approaches in the Framework
- Be practical, to adapt to the AI landscape as AI technologies continue to develop, and to be operationalized by organizations in varying degrees and capacities so society can benefit from AI while also being protected from its potential harms
- Be flexible and to augment existing risk practices which should align with applicable laws, regulations, and norms
- Designed to equip organizations and individuals – referred to here as *AI actors* – with approaches that increase the trustworthiness of AI systems, and to help foster the responsible design, development, deployment, and use of AI systems over time
- Offer approaches to minimize anticipated negative impacts of AI systems *and* identify opportunities to maximize positive impacts
- Designed to address new risks as they emerge

Note that unlike the various AI legislation, the NIST AI Risk Management Framework (RMF) is design for all organizations within and outside of the Federal Government.

Probably the main theme of the NIST AI RMF is the concept of "trustworthiness", which in the context of the NIST AI RMF is defined in terms of 7 characteristics - valid and reliable, safe, fair with harmful bias managed, secure and resilient, accountable and transparent, explainable and interpretable, and privacy-enhanced. These are shown pictorially in Slide 70.

The four "Core Functions" of the NIST AI RMF, shown pictorially in Slide 71, are:

- **Govern**: Cultivate and implement a culture of risk management within organizations developing, deploying, or acquiring AI systems
- **Map**: Establish the context to frame risks related to an AI system
- **Measure**: Employ quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor AI risk and related impacts

  Note: Just like the EU AI Act, measurement and metrics is an important aspect of the NIST AI RMF.
- **Manage**: Entails allocating risk management resources to mapped and measured risks on a regular basis and as defined by the Govern function

Each "Core Function" is comprised of a set of categories and subcategories that define the tasks that can be performed to meet each Core Function.

Finally, the NIST AI RMT does mention the following set of AI-specific risks:

- The data used for building an AI system may not be a true or appropriate representation of the context or intended use of the AI system, and the ground truth may either not exist or not be available

- Harmful bias and other data quality issues can affect AI system trustworthiness, which could lead to negative impacts
- AI system dependency and reliance on data for training tasks, combined with increased volume and complexity typically associated with such data
- Intentional or unintentional changes during training may fundamentally alter AI system performance
- Datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to deployment context
- AI system scale and complexity (many systems contain billions or even trillions of decision points) housed within more traditional software applications
- Use of pre-trained models that can advance research and improve performance can also increase levels of statistical uncertainty and cause issues with bias management, scientific validity, and reproducibility.
- Higher degree of difficulty in predicting failure modes for emergent properties of large-scale pre-trained models
- Privacy risk due to enhanced data aggregation capability for AI systems
- AI systems may require more frequent maintenance and triggers for conducting corrective maintenance due to data, model, or concept drift
- Increased opacity and concerns about reproducibility
- Underdeveloped software testing standards and inability to document AI-based practices to the standard expected of traditionally engineered software for all but the simplest of cases.
- Difficulty in performing regular AI-based software testing, or determining what to test, since AI systems are not subject to the same controls as traditional code development
- Computational costs for developing AI systems and their impact on the environment and planet
- Inability to predict or detect the side effects of AI-based systems beyond statistical measures

AI noted that these are all essentially “technical-related” AI risks and really don’t get at the real concerns today concerning AI – e.g., the potential use of AI to put out misinformation or journalistic concerns about use of AI in creating articles with false or incorrect information. o AI added the following bullet to the AI-Risks slide - **Social and ethical impact of the use of AI systems.**

6. Ira indicated that nothing had been done on the HCD Security Guidelines since the last IDS Face-to-Face Meeting, so this topic was skipped for this session..
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 mentioned were:
        - Last TCG Members F2F Meetings was in Berlin Germany on 27-29 June 2023; next one will be 24-26 Oct 2023 in Kirkland WA. Both will be hybrid meetings and Ira did or will call into both.
        - For **Mobile Platform (MPWG)**:
            - ***TCG Runtime Integrity Preservation for Mobile Devices*** - is a very good document
            - Global Platform and collaborated on the ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore*** specs. The provide a single programing model. All three have been prototyped and ***Entity Attestation Protocol / COSE Keystore*** are both in public review.

- For **Recent Specs**
  - ***TCG Mobile Reference Architecture v2 – publication approved by TC July 2023***
  - ***TCG PC Client Platform Firmware Profile v1.06 – public review July 2023***
  - ***TCG Algorithm Registry v1.34 – public review June 2023***
  - ***TCG Component Class Registry v1r14 – published May 2023*** – is a list of components
  - ***TCG MARS API v1 – published May 2023*** – is a MARS library
  - ***TCG Measurement and Attestation RootS (MARS) Library*** – Is hardware in a CPU or co-processor

- Regarding IETF standards activities, some key items Ira stressed were:
  - **IETF 117 F2F** was in San Francisco CA on 24-28 July 2023 (Ira called in); **IETF 118 F2F** will be in Prague, Czech Republic) on 6-10 November 2023 and IETF 119 Hybrid F2F will be in Brisbane, Australia) on 18-22 March 2024. Both will be Hybrid meetings and Ira will call in.
  - For TLS:
    - **IETF Delegated Credentials for (D)TLS – draft-15** will be of interest to IPP
    - **IETF Exported Authenticators in TLS – RFC 9261** is binding at the API level to prevent man-in-the-middle attacks
    - **IETF SSLKEYLOGFILE Format for TLS – draft-01** provides useful information
    - **IETF Flags Extension for TLS 1.3 – draft-12** provides headers
    - **IETF TLS 1.3 – draft-09** will be in IETF Last Call in a month
    - **IETF Abridged Compression for WebPKI Certificates** deals with the explosion in the size of certificates
    - **IETF TLS 1.2 is Frozen – draft-01** Will provide for no more extensions to TLS 1.2
    - **IETF Post-quantum hybrid ECDHE-Kyber Key Agreement for TLSv1.3 – draft-01** is a hybrid for key exchange
  - For **Security Automation and Continuous Monitoring (SACM)**
    - **IETF Concise Software Identifiers – RFC 9393** was finally published in June 2023. .
  - **Concise Binary Object Representation (CBOR)**
    - CDDL is the only IETF approved language for ISON and CBOR messages
    - **IETF Updates to the CDDL grammar of RFC 8610 – draft-00** is an Errata
    - **IETF CDDL Module Structure – draft-00** involves import and export structures
    - **IETF App-Oriented Literals in CBOR Ext Diag Notation – draft-02** is for debugging
  - Regarding **Remote ATtestation ProcedureS (RATS)**:
    - **IETF RATS Architecture – RFC 9334** was published in January 2023
    - **IETF EAT Media Types – draft-04** in IETF Last Call
    - **IETF RATS Endorsements – draft-02** is being worked on
    - **IETF EAT Attestation Results – draft-01** is a pretty good document

- **IETF Concise Reference Integrity Manifest (CoRIM) – draft-02** is a means to verify attestation

- Finally, for the **IRTF Crypto Forum Research Group (CFRG):**
  - **IRTF Hybrid Public Key Encryption – RFC 9180** – team is arguing over how to use this feature so spec is being revisited
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106** is an update
  - **IRTF AEGIS family of authenticated encryption algorithms – draft-04** is the next generation of authenticated encryption algorithms
  - **IRTF Merkle Tree Ladder Mode (MTL) Signatures – draft-00** is applicable to update signatures
  - **IRTF BBS Signature Scheme – draft-03** is a signature scheme for BBS
  - **IRTF Guidelines for Writing Cryptography Specifications – draft-00** is a good document. Ira suggested that the HCD iTC should read it.
  - **IRTF Two-Round Threshold Schnorr Sigs with FROST – draft-14** is in late IETF Last Call. It will impact Post-Quantum resistant algorithms
  - **IRTF Deterministic Nonce-less Hybrid Public Key Encryption – draft-01** is a hot topic

8. **Wrap Up**

- The next IDS Working Group Meeting will be on August 24, 2023. Main topics of the meeting will be updated status of the HCD iTC and HIT, debrief of this IDS Face-to-face, probably a special topic that currently is TBD.
- Next IDS Face-to-Face Meeting will be during the November 2023 PWG Virtual Face-to-Face Meeting November 14-16, 2023 (likely on Nov 16, 2023).

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 N ET on August 10, 2023.