IDS Face-to-Face Minutes
May 19, 2023

Meeting was called to order at approximately 10:00 am ET May 18, 2023.

Attendees –

Amin Bandali	
Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Paul Tykodi	Tykodi Consulting
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/2023-05-18-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 US Cybersecurity Strategy and Plans
   - 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 thinks the iTC will have to 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 new content in ND cPP v3.0 (see Slide 17 discussion).

   - The HCD iTC is currently awaiting Position Statements 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 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.

At the International Common Criteria Conference during his talk Al was asked if there was a document that indicated that changes in the HCD cPP from the HCD PP. Al put together two documents that indicate the major changes of the HCD cPP and HCD SD, respectively, from the HCD PP; these documents are posted on the HCD iTC OnlyOffice site. Along the way Al found a few minor grammatical errors that will need to be corrected in am errata.

- Al then gave the status of the HCD Interpretation Team.as follows:
  - The HIT currently has 7 members. The goal is to have a maximum of 10 members on the HIT, but 7 is a good number to start with. We have designated a HIT Lead (Al) and a HIT Deputy Lead (Jerry Colunga). The current membership is from HCD vendors, two Evaluation Labs, and a NIAP representative from NSA.
  - HIT procedures v1.0 were finalized and approved by the HIT members 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 three meetings at the time of this presentation. During these three meetings the HIT processed the following seven 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
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.
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.

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
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
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
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 requirements to determine that all selection operations are performed correctly. -- General inconsistency with regards to whether or not "selection:" prompt is bolded

Issue #	Title	Issue
		Examples are provided

- For HIT-IT #1, this issue was because Lexmark was using a TPM to generate a key that was to be stored in flash memory, not in the TPM. The Key Encryption SFR FCS_COP.1/KeyEnc in the HCD cPP for the AES algorithm only allows CBC and GCM mode, but TPM 2.0 Architecture specification Section 26.6 (Page 172) indicates that TPMs require CFB mode. The proposed solution was to add 'CFB' as an allowable mode,

  However, a HIT member argued that the Key Protection SFR FPT_KYP_EXT.1 in HCD cPP covered the Lexmark case. Specifically, the fact that Lexmark was not storing the key in a TPM fell under the case in FPT_KYP_EXT.1.1 where a key is protected by another key that is not part of the key chain. The HIT members are analyzing both options to determining which is the better one before proceeding.

- For HIT-IT #2, this is a case of an issue that had been raised as a comment for the Final Draft of the HCD SD, the resolution was approved by the HCD iTC but the fix did not get done in time to make the Final Draft and thus did not get into Version 1.0. The HIT members agreed that already agreed-upon fix should go into the very next v1.0 release (see discussion below), and Jerry Colunga the HCD SD author was directed to create a Technical Decision for this issue with the agreed-upon fix.

- HIT-IT #3 was essentially a grammatical issue involving the SFR style conventions listed in Section 5.1 of the HCD cPP. In SFR FCS_CKM.4 Cryptographic key destruction the last line of the SFR states "] that meets the following: [selection: no standard]."; the selection is not necessary and should be deleted.

  Turns out this comment is included in one of the examples in HCD-IT #7, so the HIT agreed to reject this issue as a duplicate and close it out.

- HIT-IT #4 – HIT-it #7 are four issues representing comments from NIAP from its evaluation of the HCD cPP against the PP evaluation requirements in CC Part 1 as part of HCD cPP v1.0. These four sets of comments represent inconsistencies in how the HCD cPP met the SFR style conventions in HCD cPP Section 5.1.

  The SFR style conventions in the HCD cPP were the SFR style conventions in the 2015 HCD PP with some minor changes to reflect the difference between a PP and a cPP. Al wasn't sure where the HCD the HCD TC got the SFR style conventions used in the HCD PP, because Al found that there are no SFR style conventions mentioned anywhere in Parts 1-3 in CCv3.1R5. The NIAP position, however, is that is doesn't matter where the conventions come from; whatever style conventions are in your cPP you are expected to meet consistently and the comments reflect the fact didn't do that in HCD cPP 1.0.

  Specifically:

  - HCD-IT #4 was comments related to not consistently ensuring each extended functional component definition in Appendix D used the corresponding existing CC Part 2 component as a model for its presentation.
  - HCD-IT #5 was comments related to not consistently ensuring that all assignment operations are documented correctly

- HCD-IT #6 was comments related to not consistently an SFR with a refinement in it starts with "Refinement:" or not that an SFR with a refinement in it starts with "Refinement:" or not
- HCD-IT #6 was comments related to not consistently ensuring that for SFRs that contain a “selection, the "selection:" prompt is bolded

The cPP author Brian Volkoff is currently working on resolving these 4 issues. The NIAP rep on the HIT noted that there will likely be more comments coming from the NIAP assessment of HCD cPP v1.0.

- Slide 13 summarized an interesting discussion that occurred at the last HIT Meeting. Al asked the question “What should be the scope of the HIT – i.e., what are the types of issues that the HIT should be addressing and what are they types of issues that the HIT should be forwarding on to the full HCD iTC. After some back-and-forth, we agreed with the NIAP rep that theoretically the HIT should be able to address any issue, so all issues are in scope.
  After further discussion the HIT realized the real question was “what issues can the HIT resolve by itself and what issues does the HIT have to let the full HCD iTC resolve”. The consensus of the HIT members present at the meeting was that:
  - The HIT should be able to resolve any issue that involves a clarification of existing requirements in either HCD cPP v1.0 or HCD SD v1.0
  - For any issue that involves new content to either the HCD cPP or HCD SD, the HIT should make a recommendation to the full HCD iTC. That recommendation could be for change to v1.0 only, a change to a future release only, a change to both v1.0 and a future release, or for no change at all.

  The HIT will have to codify these guidelines a little to further define what constitutes a “clarification” vs “new content”.
- As far as HIT-related releases, there will probably need to be an Errata release (likely v1.0a) to address the NIAP evaluation comments at a minimum) and at least one update (likely v1.0.1) to v1.0 for both the HCD cPP and HCD SD with fixes from the various RfIs that come in. The Errata release will almost certainly be the first v1.0 update to be published as soon as possible after receipt of all NIAP cPP evaluation comments. We still need to plan for the v1.0.1 releases of both the HCD cPP and HCD SD in terms of both content and time frame – depending on number of RfIs received Al thought we might be talking maybe 9 -12 months from now.
- The “Post v1,0 Release Plan” slide (Slide 15) is essentially the same slide as Al showed at the February 8, 2023 Face-to-Face IDS Session. The HCD iTC is still working on a release plan for v1.1 and future releases of the HCD cPP and HCD SD. We talked to other iTCs about what their release strategy is, and they have told us that basically they have no specific rules for the timeframe of their releases. A couple of things the HCD iTC has agreed on:
  - We will have major and minor releases
  - The first update to the HCD cPP and HCD SD will likely be “Errata” releases (see HIT release discussion above)

  The rest of the questions about the HCD iTC release planning are described in Slide 15.
- Al then presented the following rules for transitioning from CCv3.1R5 to CC:2022 in terms of certifications against PPs/CPPs:
  - CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024
  - Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 will be accepted up to the 31st of December 2027
  - After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date
  - New initial certifications based on CC v3.1 R5 may be started until 30th of June 2024

    - **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**
    - PP authors must update the PP or PP configuration to CC:2022 as soon as possible, and any new or updated PPs or PP configurations published after 30th of June 2024 must be based on CC:2022
  - After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date

  Since the HCD cPP is an "Exact Conformance" PP, the key rule in this list is the bolded one above – any certification against an "exact conformance" PP like the HCD cPP after Jan 1, 2026 must be against CC:2022. That means that by Jan 1, 2026 the HCD cPP must be CC:2022 compliant. We will have to determine exactly what that means and what, if any, changes we may have to make in the HCD cPP or HCD SD between now and 12/31/2025.

- Al then looked at some of the key new content that was included in ND cPP v3.0, based on a comparison he between ND cPP v3.0 and ND cPP v2.2e that the H CD cPP should look at for potential inclusion in the net major or minor update of the HCD cPP (and be 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, the reference to the NIAP Functional Package for SSH for all SSH-related SFRs (which are very different from the existing SSH SFRs in the HCD cPP), 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.

- In terms of likely potential content for the next (v1.1) update to the HCD cPP/SD, Al's view is pretty much the same as it was at the Feb 8th IDS Face-to-Face Meeting:
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Inclusion of NTP
  - Inclusion of AVA_VAN and ALC_FLR.*
  - Incorporate NIAP Functional Package for SSH
  - 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 to HCD cPP/SD v1.0
    - Will have to decide if only include changes approved by NIAP
  - Updates to CC:2022 published in November 2022
  - Comparison of CC:2022 Part 2 to CC v3.1R5 revealed several changes that should be looked at by the HCD iTC for inclusion

- Changes due to requests from JISEC, ITSCC, NIAP and Canada

The only "new" item in the list was the inclusion of Canadian the last bullet since Canada has endorsed the HCD cPP v1.0 and there will (hopefully) at least one certification in Canada against the HCD cPP/SD v1.0 in the near future.

- 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 Feb 8th IDS Face-to-Face Meeting (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**
  - **Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs**
  - **Expand to address 3D printing**
  - **Support for Wi-Fi** and maybe Bluetooth
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Any new CCDB Crypto WG or CCUF Crypto WG Packages
  - Support for SNMPv3
  - Support for NFC
  - Indirect updates based on new technologies, customer requests or government mandates
  - Syncing with newer versions of ND and FDE cPPs/SDs
- Next steps for the HCD iTC are:
  - Continue HIT activities for maintaining HCD cPP/SD v1.0
  - Agree on the 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 an updated version
  - Ensure that the HCD iTC continues to be fully engaged now that HCD cPP v1.0 and HCD SD v1.0 have been published
- The first set of "Lessons Learned" from the initiation of the HIT are:
  - Starting from scratch, it is important to have someone with experience to learn from; otherwise, all you do is flounder around
  - "Learning by doing" is the only real way to learn
  - When you take a leadership role, you often surprise yourself in the things that you do well and in the things that you don't do so well – Ira indicated he could relate to this one
  - When you are starting up a team, make sure you have a plan. However, make sure the plan is flexible because invariably things will not go as planned
  - Maybe my #1 lesson learned so far, if you are the team lead make sure you have a very good vice-lead, because you never know what can happen

5. Al then went through his special topic on Cybersecurity in the US. The topic consisted of two parts - a look at the new National Cybersecurity Strategy and a look at CISA's (Cybersecurity and Infrastructure Security Agency) 2023-2025 Cybersecurity Plan.

National Cybersecurity Strategy

- The new National Cybersecurity Strategy was published March 1, 2023 and can be found at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

  It turns out that the Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which we have talked about at previous IDS WG Meetings, and the

work performed and reports created in response to that Executive Order laid the groundwork for this National Cybersecurity Strategy.

The main goal of the National Cybersecurity Strategy is to explain how the US will:

- Defend the homeland by protecting networks, systems, functions, and data;
- Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
- Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
- Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet

These are the typical types of goals one would expect from a national strategy like this and are your basic “motherhood and apple pie” type goals for a strategy of this kind.

- Slides 25 and 26 describe the current landscape that the National Cybersecurity Strategy was built around. The key conditions that Al emphasized were:
  - Rise of the open internet has allowed US competitors and advisories to engage in pernicious economic espionage and malicious cyber activities such as cyber-attacks, cyber-enabled economic espionage and trillions of dollars of intellectual property theft , causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world – in fact the open internet is a key thread throughout the strategy
  - Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities

  As a result, the strategy must recognize that:

  - Purely technocratic approach to cyberspace is insufficient to address the nature of these new problems
  - Must impose costs if it hopes to deter malicious cyber actors and prevent further escalation – making sure malicious actors pay for their actions is a critical element of any cybersecurity strategy
  - Must retain the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies
  - The US is vulnerable to peacetime cyber-attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber-attacks against the United States during a crisis short of war – vulnerability of infrastructure is another theme throughout the strategy
  - These adversaries are continually developing new and more effective cyber weapons – our enemies are continually getting better so we have to get better as stopping them
- The National Cybersecurity Strategy is made up of four Pillars:
  - **Protect the American People, the Homeland, and the American Way of Life**

    Will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime
  - **Promote American Prosperity**

    Need to demonstrate a coherent and comprehensive approach to address challenges that threaten our national security in this increasingly digitized world – the key here is the fact that the strategy has to apply to “a digitized world”
  - **Preserve Peace through Strength**

Need to issue transformative policies that reflect today's new reality where Cyberspace is no longer treated as a separate category of policy or activity disjointed from other elements of national power

- **Advance American Influence**

  Need to maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace

Each Pillar has a set of high-level Steps, methods and tasks for achieving those pillars that the remaining slides described and which will be summarized below. Al picked one representative task from each method to keep the number of slides down so the presentation could fit in the allowed time slot.

a. Pillar I: **Protect the American People, the Homeland, and the American Way of Life**

   The objective of Pillar 1 is to manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems. Pillar has 3 Steps as follows:

   - Step 1 - **Secure Federal Networks and Information** by**:**
     - **FURTHER CENTRALIZE MANAGEMENT AND OVERSIGHT OF FEDERAL CIVILIAN CYBERSECURITY** through
       - Deploying centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies, standards, and directives

         Al noted that standards and best practices is a common task that appears throughout the strategy. That means that the work that the IDS is doing in supporting the HCD cPP and the standards work that Ira will talk about in his Liaison Report fits right into this strategy.
     - **ALIGN RISK MANAGEMENT AND INFORMATION TECHNOLOGY ACTIVITIES** through
       - The Administration, through OMB and DHS, guiding and directing risk management actions across Federal civilian departments and agencies, and CIOs will be empowered to take a proactive leadership role in assuring IT procurement decisions assign the proper priority to securing networks and data - risk management is another theme that goes across the entire strategy
     - **IMPROVE FEDERAL SUPPLY CHAIN RISK MANAGEMENT** through
       - Integrating supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices

       Al noted the importance that the strategy covers supply chain risk management.
     - **STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY** through
       - Ensuring, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information

       Al noted that it was good that as part of the strategy it involved sharing threat intelligence with Federal contractors who are often the targets of cyberattacks.
     - **ENSURE THE GOVERNMENT LEADS IN BEST AND INNOVATIVE PRACTICES through**
       - Being a leader in developing and implementing standards and best practices in new and emerging areas such as quantum computing

       Again, the stress on implementing standards, but here the emphasis on quantum computing and new emerging areas..

- **Step 2 - Support Critical Infrastructure** by**:**
  - **REFINE ROLES AND RESPONSIBILITIES** through
    - Identify and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination

      Identifying and bridging gaps is an important step.
  - **PRIORITIZE ACTIONS ACCORDING TO IDENTIFIED NATIONAL RISKS** through
    - Prioritizing risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation

    The seven key areas listed are key areas that have all been in the news recently, which solidifies why they were chosen as areas that should be emphasized for risk-reduction.
  - **LEVERAGE INFORMATION AND COMMUNICATIONS TECHNOLOGY PROVIDERS AS CYBERSECURITY ENABLERS** through
    - Promoting an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards

    Again.\, the stress on the important of a secure supply chain based on best practices and standards
  - **PROTECT OUR DEMOCRACY** through
    - Coordinating the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system

    Interesting the push on the use of standards and guidance to help safeguard election security.
  - **INCENTIVIZE CYBERSECURITY INVESTMENTS** through
    - Working with private and public sector entities to promote understanding of cybersecurity risk so they make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments

    Cooperation with public sector has been a key strategy throughout the Biden Administration.
  - **PRIORITIZE NATIONAL RESEARCH AND DEVELOPMENT INVESTMENTS** through
    - Aligning investments to the priorities, which will focus on building new cybersecurity approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies, and building resilience to large-scale or long-duration disruptions

    It just makes sense to align investments with priorities
  - **IMPROVE TRANSPORTATION AND MARITIME CYBERSECURITY** through
    - Clarifying maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure

    We too often forget the importance of shipping and maritime cybersecurity.

- **IMPROVE SPACE CYBERSECURITY** through
  - Enhancing efforts to protect our space assets and support infrastructure from evolving cyber threats

  The strategy even has to account for any future space involvement.

- **Step 3 - Combat Cybercrime and Improve Incident Reporting** by**:**
  - **IMPROVE INCIDENT REPORTING AND RESPONSE** through
    - Encouraging reporting of intrusions and theft of data by all victims, especially critical infrastructure partners
  - **MODERNIZE ELECTRONIC SURVEILLANCE AND COMPUTER CRIME LAWS** through
    - Working with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors

    This is an area that has been in the news a lot lately and one law enforcement wants badly.
  - **REDUCE THREATS FROM TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE** through
    - Advocating for law enforcement to have effective legal tools to investigate and prosecute transnational criminal groups and modernized organized crime statutes for use against computer hacking
  - **IMPROVE APPREHENSION OF CRIMINALS LOCATED ABROAD** through
    - Identify gaps and potential mechanisms for bringing foreign based cyber criminals to justice

    All of the above for Step 3 are reasonable things to do.
  - **STRENGTHEN PARTNER NATIONS' LAW ENFORCEMENT CAPACITY TO COMBAT CRIMINAL CYBER ACTIVITY** through
    - Continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation

    Working with our international partners is another long-standing strategy of the Biden Administration.

b. Pillar II: **Promote American Prosperity**

The objective of Pillar II is to preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency. Pillar II has 3 Steps as follows:

- Step 1 - **Secure Federal Networks and Information** by**:**
  - **Foster a Vibrant and Resilient Digital Economy** through
    - Collaborating with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges

    We see the common themes for Pillar I here also.

- **PRIORITIZE INNOVATION**
  - Promoting implementation and continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem

  More emphasis on standards and best practices.

- **INVEST IN NEXT GENERATION INFRASTRUCTURE**
  - Facilitating the accelerated development and rollout of next-generation telecommunications and information communications infrastructure in the US
  - Examining the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application

  Note the references here to AI and quantum computing which are becoming big areas of importance. Some commented that given the latest concerns about AI, they wondered if this strategy might have to be revised.

- **PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS**
  - Continuing to work with international counterparts to promote open, industry driven standards, innovative products, and risk-based approaches that permit global innovation and the free flow of data

  Maybe one of the key central themes of the entire strategy is here – ensure the free flow of information and ideas across borders

- **MAINTAIN UNITED STATES LEADERSHIP IN EMERGING TECHNOLOGIES**
  - Making a concerted effort to protect cutting edge technologies, including from theft by our adversaries, support those technologies' maturation, and, where possible, reduce United States companies' barriers to market entry

  Al feels this is a key task that needs more emphasis than it will probably get because we are losing our technology leadership to China and we cannot allow that to happen.

- **PROMOTE FULL-LIFECYCLE CYBERSECURITY**
  - Promoting full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery

  It was nice to see the strategy place importance of promoting a secure lifecycle. The idea of default security settings spawned a lively discussion of why US and Japanese HCD vendors by-and-large do not do that in their HCD devices.

- **Step 2. Foster and Protect United States Ingenuity** by**:**
  - **UPDATE MECHANISMS TO REVIEW FOREIGN INVESTMENT AND OPERATION IN THE UNITED STATES**
    - Formalizing and streamlining the review of Federal Communications Commission referrals for telecommunications licenses
  - **MAINTAIN A STRONG AND BALANCED INTELLECTUAL PROPERTY PROTECTION SYSTEM**
    - Continuing to help foster a global intellectual property rights system that provides incentives for innovation through the protection and enforcement of intellectual property rights

    Just like we do for the PWG, IP protection is very important in maintaining our technological leadership..

- **PROTECT THE CONFIDENTIALITY AND INTEGRITY OF AMERICAN IDEAS**
  - Working against the illicit appropriation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate

- **Step 3. Develop a Superior Cybersecurity Workforce** by**:**
  - **BUILD AND SUSTAIN THE TALENT PIPELINE**
    - Continuing to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education

    It is very important to ensure we don't stop the "brain drain" to China and other countries. Maintaining our educational advantage is critical to maintaining our technical superiority.
  - **EXPAND RE-SKILLING AND EDUCATIONAL OPPORTUNITIES FOR AMERICA'S WORKERS**
    - Working with the Congress to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce
  - **ENHANCE THE FEDERAL CYBERSECURITY WORKFORCE**
    - Continuing to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce
  - **USE EXECUTIVE AUTHORITY TO HIGHLIGHT AND REWARD TALENT**
    - Implementing actions to prepare, grow, and sustain a workforce that can defend and bolster America's critical infrastructure and innovation base

    All four of these tasks under Step 3 and their methods are what one would expect to be proposed to build a cybersecurity workforce within the US.

c. Pillar III: **Preserve Peace Through Strength**

The objective of Pillar III is to identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace. Pillar III has 2 steps as follows:

- Step 1 - **Enhance Cyber Stability through Norms of Responsible State Behavior** by**:**
  - **ENCOURAGE UNIVERSAL ADHERENCE TO CYBER NORMS**
    - Encouraging other nations to publicly affirm International law and voluntary non-binding norms of responsible state behavior in cyberspace) through enhanced outreach and engagement in multilateral fora

      More "alliance-building" which as stated earlier is a core of this strategy.

Step 2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE**
  - Leading the world in the use of all-source cyber intelligence to drive the identification and attribution of malicious cyber activity that threatens United States national interests

  Again, emphasized the themes of collaboration and sharing of intelligence
- **IMPOSE CONSEQUENCES**
  - Developing swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior

Emphasizes that a key to a good cybersecurity strategy is having strong consequences to any malicious actor that even attempts to perform a cybersecurity attack against the US.

- **BUILD A CYBER DETERRENCE INITIATIVE**
  - Launching an international Cyber Deterrence Initiative to build broader coalition of like-minded states and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior

  More coalition-building.

- **COUNTER MALIGN CYBER INFLUENCE AND INFORMATION OPERATIONS**
  - Using all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation

  Al was glad to see that the strategy included a task to fight misinformation.

d. Pillar IV: **Advance American Influence**

The objective of Pillar IV is to preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests. Pillar IV has 2 steps as follows:

- Step 1 - **Promote an Open, Interoperable, Reliable, and Secure Internet** by**:**
  - **PROTECT AND PROMOTE INTERNET FREEDOM**
    - Encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member

      Note: 'Internet Freedom' in this context is defined as online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium. By extension, Internet freedom also supports the free flow of information online that enhances international trade and commerce, fosters innovation, and strengthens both national and international security

      Note the definition of Internet Freedom in this context revolves around .human rights and freedoms; not explicitly on open internet from a technical perspective
  - **WORK WITH LIKE-MINDED COUNTRIES, INDUSTRY, ACADEMIA, AND CIVIL SOCIETY**
    - Continue to work with like-minded countries, industry, civil society, and other stakeholders to advance human rights and Internet freedom globally and to counter authoritarian efforts to censor and influence Internet development

    Human rights are another cornerstone of this strategy.
  - **PROMOTE A MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE**
    - Continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance (characterized by transparent, bottom-up, consensus-driven processes) prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet

    Multi-stakeholder model is an interesting new concept.
  - **PROMOTE INTEROPERABLE AND RELIABLE COMMUNICATIONS INFRASTRUCTURE AND INTERNET CONNECTIVITY**

- Promote communications infrastructure and Internet connectivity that is open, interoperable, reliable, and secure

Just reinforcing the open internet plank of the strategy.

- **PROMOTE AND MAINTAIN MARKETS FOR UNITED STATES INGENUITY WORLDWIDE**
  - Advise on infrastructure deployments, innovation, risk management, policy, and standards to further the global Internet's reach and to ensure interoperability, security, and stability

Another instance of pushing standards and best practices as part of the strategy.

- **Step 2. Build International Cyber Capacity** by**:**
  - **ENHANCE CYBER CAPACITY BUILDING EFFORTS**
    - Aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchanges

Al liked the idea of sharing ".actionable cyber threat information"

CISA's 2023 – 2025 Cybersecurity Plan

The CISA 2023 – 2025 Cybersecurity Plan can be found at https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf. The purpose of this plan is to:

- Communicate the Cybersecurity and Infrastructure Security Agency's (CISA) mission and vision
- Promote unity of effort across the agency and our partners, and defines success for CISA as an agency
- Describe the stakeholder, policy, and operational context in which CISA must perform and present the strategic changes CISA will make to better execute our vital mission over the next three years
- Build on and align with the *United States Department of Homeland Security Strategic Plan for Fiscal Years 2020 – 2024*

The CISA core values that this plan aligns with are the following:

- **Collaboration** - We will approach every engagement as an opportunity to build trust with our teammates, our partners, and our customers
- **Innovation** - We must move with creativity and agility at the speed of ideas to stay ahead of threats to our nation and our way of life, and we must be grounded in the strength of our resilience
- **Service** - Our commitment is a calling to protect and defend the infrastructure Americans rely on every hour of every day
- **Accountability** - We will model the behavior we want to see in others; we will hold ourselves and our teammates responsible for our actions; and we will empower our workforce through trust, transparency, and radical honesty

The goals of this cybersecurity plan are to:

- **Cyber Defense** - SPEARHEAD THE NATIONAL EFFORT TO ENSURE DEFENSE AND RESILIENCE OF CYBERSPACE
- **Risk Reduction and Resilience** - REDUCE RISKS TO, AND STRENGTHEN RESILIENCE OF, AMERICA'S CRITICAL INFRASTRUCTURE
- **Operational Collaboration** - STRENGTHEN WHOLE- OF-NATION OPERATIONAL COLL ABORATION AND INFORMATION SHARING

- **Agency Unification** - UNIFY AS ONE CISA THROUGH INTEGRATED FUNCTIONS, CAPABILITIES, AND WORKFORCE

Each of these goals has multiple objectives with one or more tasks associated with each objectives. Al noted that some of the objective in this plan are similar to the objectives in the National Cybersecurity Strategy,. However, in response to a question Al indicated that this plan was not developed as a response to the National Cybersecurity Strategy; it was developed totally independent of the strategy.

The various objectives and tasks for each goal are as follows (Note: Just as was done for the National Cybersecurity Strategy above, only one representative task was listed for each of the objectives):

a. Goal 1 - **Cyber Defense**

Objective 1.1 ENHANCE THE ABILITY OF FEDERAL SYSTEMS TO WITHSTAND CYBERATTACKS AND INCIDENTS

Driving and facilitating the adoption of modern, secure, and resilient technologies

Objective 1.2 INCREASE CISA'S ABILITY TO ACTIVELY DETECT CYBER THREATS TARGETING AMERICA'S CRITICAL INFRASTRUCTURE AND CRITICAL NETWORKS

Will advance our capability to actively detect threats across federal and SLTT networks while working with industry partners to enhance our understanding of threats targeting private networks

Objective 1.3 DRIVE THE DISCLOSURE AND MITIGATION OF CRITICAL CYBER VULNERABILITIES

Along with our partners, will enable timely and coordinated vulnerability disclosure, provide recommendations, and amplify appropriate mitigation countermeasures using relevant channels and mechanisms

Objective 1.4 ADVANCE THE CYBERSPACE ECOSYSTEM TO DRIVE SECURITY-BY-DEFAULT

Foster the development and adoption of state-of-the-art network defense and cyber operations tools, services, and capabilities to drive security-by-default in the technology ecosystem

Al emphasized that here like in the National Cybersecurity Strategy there is the emphasis on "security by default"

b. Goal 2 - **Risk Reduction and Resilience**

Objective 2.1 EXPAND VISIBILITY OF RISKS TO INFRASTRUCTURE, SYSTEMS, AND NETWORKS

Need to deepen our insights into the nation's cyber and physical critical infrastructure assets and systems, as well as identifying the potential and future sources of risk that could impact that infrastructure

Objective 2.2 ADVANCE CISA'S RISK ANALYTIC CAPABILITIES AND METHODOLOGIES

Must mature CISA's risk analysis capabilities and methodologies to promote in-depth understanding of the risks we face

Objective 2.3 ENHANCE CISA'S SECURITY AND RISK MITIGATION GUIDANCE AND IMPACT

Will issue authoritative guidance to drive effective IT network risk management

Objective 2.4 BUILD GREATER STAKEHOLDER CAPACITY IN INFRASTRUCTURE AND NETWORK SECURITY AND RESILIENCE

Will deliver impactful capabilities and services to meet our stakeholders' most pressing and evolving physical security challenges, which include insider threats, active shooter preparedness, bombing prevention, and security in public gathering places

Objective 2.5 INCREASE CISA'S ABILITY TO RESPOND TO THREATS AND INCIDENTS

Must bolster and expand our headquarters and regional capacity to support our stakeholders and interagency partners following physical threats and incidents

Objective 2.6 SUPPORT RISK MANAGEMENT ACTIVITIES FOR ELECTION INFRASTRUCTURE

Be the federal government's hub for understanding and characterizing risks to election infrastructure and ensuring election officials and their private sector partners have the information they need to manage risk to their systems

c. Goal 3 - **Operational Collaboration**

Objective 3.1 OPTIMIZE COLLABORATIVE PLANNING AND IMPLEMENTATION OF STAKEHOLDER ENGAGEMENTS AND PARTNERSHIP ACTIVITIES

Must plan, prioritize, and coordinate stakeholder engagements within our agency, SRMAs, and across the broader stakeholder community

Objective 3.2 FULLY INTEGRATE REGIONAL OFFICES INTO CISA'S OPERATIONAL COORDINATION

Will establish processes for coordinating engagement activities between HQ divisions and regions and mutually support operational relationship management

Objective 3.3 STREAMLINE STAKEHOLDER ACCESS TO AND USE OF APPROPRIATE CISA PROGRAMS, PRODUCTS, AND SERVICES

Wherever possible and suitable, will offer our customers tailored product information, access, and delivery, based on their specific needs and circumstances; to this end, our catalog of resources will be consistently available, accurate, tailorable, engaging, and easy to access

Objective 3.4 ENHANCE INFORMATION SHARING WITH CISA'S PARTNERSHIP BASE

Must enhance multidirectional communications with external partners, including timely incident reporting and the sharing of threats and vulnerabilities, intelligence and intelligence requirements, as well as other information and data

Objective 3.5 INCREASE INTEGRATION OF STAKEHOLDER INSIGHTS TO INFORM CISA PRODUCT DEVELOPMENT AND MISSION DELIVERY

Will increase integration of stakeholder insights, information, and data to assist in decision making and the prioritization, development, modification, and tailoring of our products, services, and areas of focus

d. Goal 4 - **Agency Unification**

Objective 4.1 STRENGTHEN AND INTEGRATE CISA GOVERNANCE, MANAGEMENT, AND PRIORITIZATION

Will work to delineate lines of effort and assign organizational and/or individual responsibility to drive collective decision making, and document and integrate processes to ensure standardization and utilization of best practices

Objective 4.2 OPTIMIZE CISA BUSINESS OPERATIONS TO BE MUTUALLY SUPPORTIVE ACROSS ALL DIVISIONS

Will streamline existing operations and adopt agile, new technologies that will enable customer service and improved timely, modern, and secure services

Objective 4.3 CULTIVATE AND GROW CISA'S HIGH-PERFORMING WORKFORCE

Will implement a world-class talent ecosystem that spans recruiting, hiring, training, recognition, advancement, retention, and succession planning

Objective 4.4 ADVANCE CISA'S CULTURE OF EXCELLENCE

Our culture will be incorporated in our day-to-day tasks, mission-enabling functions, service to our partners and stakeholders, and in our everyday behaviors

Note that because it was getting towards the end of the allotted time slot for this special topic presentation, Al mostly just read through the CISA Plan objectives and task with little comment. Al did note the similarities between the National Strategy and the CISA Plan in areas like Risk Management, information sharing and threat response.

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:
     - Next TCG Members F2F Meetings will be 27-29 June 2023 in Berlin Germany and 24-26 Oct 2023 in Kirkland WA. Both will be hybrid meetings and Ira will call into both.
     - For **Mobile Platform (MPWG)**:
       - ***TCG Mobile Reference Architecture v2*** went to public review end of April 2023.
       - ***TCG TPM 2.0 Mobile Common Profile*** has been delayed due to editorial and technical comments until Q3/Q4 2023.
       - ***TCG MARS 1.0 Mobile Profile*** is delayed until Q4 2023
     - For **Recent Specs**
       - ***TCG MARS FAQ*** was published in Feb 023. MARS is microcode for MCUs.
       - ***TCG MARS API*** v1 was published May 2023
       - ***TCG DICE Protection Environment*** went to public review April 2023
       - ***TCG EK (Endorsement Key) Credential Profile for TPM 2.0*** was published March 2023
       - A TCG Mobile Ecosystem Security Guidelines (similar to our HS|D Security Guidelines) will be completed in Fall 023.
   - Regarding IETF standards activities, some key items Ira stressed were:
     - **IETF 117 F2F** will be in San Francisco CA on 24-28 July 2023 and **IETF 118 F2F** will be in Prague, Czech Republic) on 6-10 November 2023. Both will be Hybrid meetings and Ira to call in.
     - For TLS:
       - Are no new RFCs
       - **IETF IANA Registry Updates for TLS/DTLS** went to WG Last Call in Mar 2023; should be in IETF LC by this summer
       - **IETF TLS 1.3** went to WG Last Call in March 2023
       - **IETF Compact TLS 1.3** fixed a lot of issues and should be in WG Last Call by this Fall
       - **IETF Delegated Credentials for (D)TLS – draft-15** is a major extension for (D)TLS and is now to the RFC Editor
     - For **Security Automation and Continuous Monitoring (SACM)**

- **IETF Concise Software Identifiers – draft-24 – February 2023** is now to the RFC Editor. .

- **Concise Binary Object Representation (CBOR**
  - No new RFCs
  - **IETF Gordian dCBOR: Deterministic CBOR – draft-01** and **IETF Envelope Structured Data Format – draft-02** both involve cybercurrencies
  - **IETF CBOR Tags for Time, Duration, and Period** is now in WG Last Call and should be in IETF Last Call in June
  - **IETF App-Oriented Literals in CBOR Ext Diag Notation – draft-02 – March 2023** involves development and support
  - **IETF CDDL 2.0 -- a draft plan - draft-02 - March 2023** is the first draft of CDDL 2.0
  - **IETF CDDL Module Structure – draft-00 – March 2023** introduces new features for CDDL 2.0
  - **IETF Packed CBOR – draft-08 – January 2023** is now in WG Last Call
- Regarding **Remote ATtestation ProcedureS (RATS)**:

  Some new specs in RATS are:
  - **IETF Proximate Location Claim – draft-00 – March 2023**
  - **IETF Epoch Markers – draft-04 – March 2023**
  - **IETF Concise Reference Integrity Manifest (CoRIM) – draft-01 – March 2023**
  - **IETF RATS Endorsements: CORIM vs EAT – draft-00 – March 2023**

  Other specs of interest:
  - **IETF EAT Media Types – draft-02 – March 2023** – is a registry f EAT media types
  - **IETF Attestation Event Stream Subscription – draft-03 – March 2023** has been published
  - **IETF Reference Interaction Models for RATS – draft-07 – March 2023** complements the **IETF RATS Architecture** and is in WG Last Call
  - **IETF CoRIM Profile for ARM PSA – draft-02 – March 2023** is a concise reference integrity measure
  - **IETF RATS Conceptual Messages Wrapper – draft-02 – March 2023** is a set of potential new wrappers
  - **IETF Attestation Results for Secure Interactions – draft-04 – March 2023** specifies enhancements to the RATS architecture
- Finally, for the **IRTF Crypto Forum Research Group (CFRG):**
  - **IRTF Hybrid Public Key Encryption – RFC 9180 – February 2022** has been recognized by the EU but not by NIST

  The following specs are to the IRTF Chair for review:
  - **IRTF Two-Round Threshold Schnorr Sigs with FROST – draft-13 – May 2023**
  - **IRTF Ristretto255 and Decaf448 Groups – draft-07 – April 2023**
  - **IRTF RSA Blind Signatures - draft-12 - April 2023**

  The following specs are to the RFC Editor for review:

- **IRTF Oblivious Pseudorandom Functions (OPRFs) – February 2023**
- **IRTF Verifiable Random Functions (VRFs) – draft-15 – August 2022**
- **IRTF Hashing to Elliptic Curves – draft-16 – June 2022**
- **IRTF SPAKE2, a PAKE – draft-26 – February 2022**

8. **Wrap Up**

   - At the time of this meeting, the next IDS Working Group Meeting was scheduled to be on Jun 1, 2023. However, subsequent to this meeting AL and the chairs of the IPP WG agree to swap meeting dates in June due to scheduling conflicts, so the next IDS WG Meeting will now be June 8, 2023.

     Main topics of the meeting will be updated status of the HCD HIT. debrief of this IDS Face-to-face, and if Ira attends the meeting a discussion on how we can help get development of the HCD Security Guidelines moving again. .

   - Next IDS Face-to-Face Meeting will be during the August 2023 PWG Virtual Face-to-Face Meeting Aug 8-10, 2023 (likely on Aug 10, 2023).

   Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 N ET on May 19, 2023.