IDS Face-to-Face Minutes
May 8, 2024

Meeting was called to order at approximately 10:00 am ET May 8, 2024.

Attendees –

Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC
Uli Wehner	Ricoh
Michael Ziler	Microsoft

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2024-05-08-IDS-F2F v1.pdf.

- Minute Taker
  - Alan Sukert taking the minutes.

2. Agenda:
   - Introductions, Agenda Review
   - Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
   - EUCC Implementing Regulation
   - 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 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 the HCD iTC Status discussion were:

   - The Errata – HCD cPP v1.0e and HCD SD v1.0e – was finally published on March 4, 2024. It contained fixes for the following issues:
     - HCD-IT #2
     - HCD-IT #4 – HCD-IT #7
     - HCD-IT #9
     - HCD-IT#12
     - HCD-IT #16
     - HCD-IT #18 – HCD-IT #19
     - HCD-IT #21 & HCD-IT #22

     Slides 13 and 13 provide more detail on these issues.
   - The HCD iTC has now received Endorsement Statements for the HCD cPP v1.0/v1.0e from the Canadian and Korean Schemes and from NIAP. However, NIAP's endorsement came with the following important caveat:

NIAP's endorsement is a formal statement that products successfully evaluated against the HCD cPP V1.0E that demonstrate exact conformance to the cPP, meeting the below identified conditions, and in compliance with all NIAP policies, will be placed on the NIAP Product Compliant List:

- Each applicable cryptographic support security functional requirement (FCS_) must include at least one selection conforming to Commercial National Security Algorithm (CNSA) Suite V1.0 or V2.0
- SHA-256 may be selected in FCS_PCC_EXT.1 and may be included in FCS_COP.1/Hash and FCS_COP.1/KeyedHash for that function; and
- **SHA-1 may not be selected**

This version succeeds the HCD PP V1.0 **which will sunset effective 23 October 2024**

Slides 9 and 10 provides the list of algorithms that comprise CNSA Suite v1.0 and v2.0.

- From a HCD Interpretation Team (HIT) perspective, now that the Errata has been published the priorities, in order, are:
  - Resolving the remaining Priority 1 Issues
  - Resolving any remaining Priority 2 Issues
  - Assigning priorities to issues with no priority assigned
  - Addressing any new issues that are raised against the Errata

  Slides 15-18 provide a list of the current open Priority 1 issues, open Priority 2 issues and open issues with no assigned priority that the BHIT must resolve.

- The other main topic the HIT will have to decide is whether the HIT will issue any more standalone HCD cPP or HCD SD v1.0.x releases after the Errata release to address the Priority 1 issues at least (or do we pass them on the HCD iTC to include in the next full release of the HCD cPP and HCD SD)

  If the HIT does decide to do standalone releases, how many of these releases will occur likely depends on the comments we get from:
  - The review of the HCD cPP from the other Schemes and
  - Future certifications against HCD cPP v1.0 or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme

- For the HCD iTC itself, the priorities for 2024 (and probably 2025), in order, are:
  a. CC:2022 Transition Policy – Ensuring the HCD cPP and HCD SD are compliant with CC:2022 by Dec 31, 2025 (CCDB deadline for certifications against prior CC version)
  b. Syncing with Network Device cPP/SD v3.0
  c. Syncing with the output from the CCDB Crypto Working Group – SFR Catalog planned for release by end of 2024
  d. Implementing HIT Technical Decisions
  e. Implementing AVA_VAN requirements to sync with EUCC
  f. NIAP PQC Requirements (CNSA 2.0) – currently on hold by NIAP
  g. Parking Lot Issues
  h. Any New Issue

- In terms of HCD cPP/SD release planning, the current plan is for the following releases:
  - V2.0 – 2026:
    - Will contain the results from the CCDB Crypto WG's SFR Catalog, Syncing with ND cPP/SD 3.0, and CC:2022 Compliant efforts
  - V3.0 - 2027 – 2028:

- Will likely contain some CNSA 2.0 components and content from the other priorities

A question was asked whether there was any plan for an interim v1.1 release in the 2025 time frame that might include some on the content planned for v2.0. Al responded that at the current time there are no plans for a v1.1 release but he would bring it up at a future HCD iTC meeting.

- Al then listed, based on the above HCD-iTC priorities, what Al thought would be definitive content of v2.0:
  - Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
  - Updates for the relevant changes in CC:2022
  - Update for the relevant changes in ND cPP v3.0e
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Standardizing on ND 3.0 Implementation for now
  - Incorporate the NIAP Functional Package for SSH so can claim conformance to it
  - Inclusion of AVA_VAN to sync with EUCC
  - Priority 1 Issues to HCD cPP/SD v1.0
  - Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes due to on-going certifications against HCD cPP/SD v1.0e
- The list of changes that could go in V3.0 or later releases is essentially the same as shown in previous sessions with some differences and additions:
  - NTP
  - Full implementation of CNSA 2.0
  - Support for Cloud Printing
  - Incorporate NIAP Functional Package for X.509 when it becomes available
  - Support for post quantum and other new crypto algorithms
  - Any 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 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 Other iTCs such as DSC iTC and FDE iTC
  - Syncing with newer versions of ND cPP/SD
- Key next steps for the HCD iTC are:
  - Continue HIT activities for maintaining HCD cPP/SD v1.0e and issue the necessary TDs/TRs and Errata to address all documented RfIs
  - Complete HCD cPP/SD v1.0e certification by Canadian Scheme
  - Fully engage the HCD iTC to work on HCD cPP v2.0 and HCD SD v2.0
  - Start planning for HCD cPP/SD v3.0 and beyond

5. Al then went through the special topic – the recently enacted EUCC Implementation Regulation. The slides presented for this special topic are extracted from a much longer presentation Al plans to give at the next IDS Working Group Meeting. The key points presented at the session were:

   - The final EUCC Implementation Regulation, which was published on 31 Jan 2024 and will go into full force on 27 January 2025, is significantly different from the final draft EUCC Implementation Regulation that was made available in the fall of 2023. The goals of this regulation are:
     - It should specify the roles, rules, and obligations, as well as the structure of the European **Common Criteria- based** cybersecurity certification scheme (EUCC) in accordance with the European cybersecurity certification framework set out in Regulation (EU) 2019/881
     - The scheme should be based on established international standards such as the Common Criteria. The Common Criteria is accompanied by the Common Evaluation Methodology.
     - The EUCC uses the Common Criteria's vulnerability assessment family (AVA_VAN), components 1 to 5. The applicant for an EUCC certificate should provide the documentation related to the intended use of the ICT product and the analysis of the levels of risks associated with such usage to enable the conformity assessment body to evaluate the suitability of the assurance level selected. Where the evaluation and certification activities are performed by the same conformity assessment body, the applicant should submit the requested information only once

     The keys here are the use of the Common Criteria and the heavy reliance on the use of the Vulnerability Assessment family to provide the security assurance.

   - The new scope of the EUCC Implementation Regulation has been simplified to now be:
     - This Regulation sets out the European Common Criteria-based cybersecurity certification scheme (EUCC)
     - This Regulation applies to all information and communication technologies ('ICT') products, including their documentation, which are submitted for certification under the EUCC, and to all protection profiles which are submitted for certification as part of the ICT process leading to the certification of ICT products
   - The standards that the EUCC will be based on have been boiled down to just two – the Common Criteria standard (ISO/IEC 15408, Common Criteria for Information Technology Security Evaluation) and the CEM (ISO/IEC 18045, Common Methodology for Information Technology Security Evaluation).
   - In terms of Assurance Levels:
     - Certification bodies shall issue EUCC certificates at assurance level 'substantial' or 'high.'
     - EUCC certificates at assurance level 'substantial' shall correspond to certificates that cover AVA_VAN level 1 or 2.
     - EUCC certificates at assurance level 'high' shall correspond to certificates that cover AVA_VAN level 3, 4 or 5.
     - The assurance level confirmed in a EUCC certificate shall distinguish between the conformant and augmented use of the assurance components as specified in the Common Criteria in accordance with Annex VIII.
     - Conformity assessment bodies shall apply those assurance components on which the selected AVA_VAN level depends in accordance with the Common Criteria and CEM standards

       Note that the EUCC assurance levels are defined in terms of the Vulnerability Assessment (AVA_VAN) levels
   - In terms of certifying ICT Products:

     a. Certification of an ICT product shall be carried out against its security target:

- as defined by the applicant; or
- incorporating a certified protection profile as part of the ICT process, where the ICT product falls in the ICT product category covered by that protection profile

b. An ICT product submitted for certification shall, as a minimum, be evaluated in accordance with the following:
   - The applicable elements of the Common Criteria (CC) and CEM standards
   - The security assurance requirements classes for vulnerability assessment and independent functional testing, as set out in the evaluation standards referred to in the CC and CEM
   - The level of risk associated with the intended use of the ICT products concerned and their security functions that support the security objectives
   - The applicable state-of-the-art documents listed in Annex I (See Slides 47 and 48); and the applicable certified protection profiles listed in Annex II (these were included as part of this presentation)
   - In the case of an ICT product undergoing a composite product evaluation in accordance with the relevant state-of- the-art documents, the ITSEF (this is the Evaluation Lab) that carried out the evaluation of the underlying ICT product shall share the relevant information with the ITSEF performing the evaluation of the composite ICT product.

c. The certification bodies shall issue an EUCC certificate where **all** of the following conditions are met:
   - The category of ICT product falls within the scope of the accreditation, and where applicable of the authorisation, of the certification body and the ITSEF involved in the certification;
   - The applicant for certification has signed a statement undertaking all commitments listed in this section;
   - The ITSEF has concluded the evaluation without objection in accordance with the evaluation standards, criteria and methods referred to in this Regulation;
   - The certification body has concluded the review of the evaluation results without objection;
   - The certification body has verified that the evaluation technical reports provided by the ITSEF are consistent with the provided evidence and that the evaluation standards, criteria and methods have been correctly applied

d. The certification body shall set a period of validity for each EUCC certificate issued, taking into account the characteristics of the certified ICT product.

   The period of validity of the EUCC certificate **shall not exceed 5 years**. (Note: means each certifying body can set its own period of validity)

   By derogation from paragraph 2 that period may exceed 5 years, subject to the prior approval of the national cybersecurity certification authority. The national cybersecurity certification authority shall notify the European Cybersecurity Certification Group of the granted approval without undue delay (Note – the ability to get permission to extend the period of validity is something the CCRA currently does not allow)

- In terms of certifying Protection Profiles:

  a. Protection profiles shall be certified for the sole purpose of the certification of ICT products falling in the specific category of ICT products covered by the protection profile

  b. A protection profile shall be evaluated, as a minimum, in accordance with the following:
     - The applicable elements of the CC and CEM standards;

- The level of risk associated with the intended use of the ICT products concerned pursuant to Article 52 of Regulation (EU) 2019/881 and their security functions that support the security objectives set out in Article 51 of that regulation (note the difference in the text for PPs from the corresponding requirement for ICT products); and
- The applicable state-of-the-art documents listed in Annex I. A protection profile covered by a technical domain shall be certified against the requirements set out in that technical domain

c. Conditions for issuance of a EUCC certificate for a PP are:
   - The applicant for certification shall provide the certification body and the ITSEF with all the necessary complete and correct information.
   - Conditions for issuance of an EUCC certificate for and ICT product and certificate content/format requirements shall apply mutatis mutandis (whatever that means).
   - The ITSEF shall evaluate whether a protection profile is complete, consistent, technically sound, and effective for the intended use and the security objectives of the ICT product's category covered by that protection profile.
   - A protection profile shall be certified solely by:
     - a national cybersecurity certification authority or another public body accredited as certification body; or
     - a certification body, upon prior approval by the national cybersecurity certification authority for each individual protection profile.

d. The certification body shall set a period of validity for each EUCC certificate.

   The period of validity may be up to the lifetime of the protection profile concerned (but it can be a finite period also)

- The Vulnerability Management Procedures in the issued regulation were changed significantly from those in previous drafts. A summary of the Vulnerability Management Procedures is:
  - The holder of an EUCC certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules laid down in this Section and, where necessary, supplemented by the procedures set out in EN ISO/IEC 30111
  - The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers
  - Where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record it and carry out a vulnerability impact analysis
  - When a potential vulnerability impacts a composite product, the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability
  - In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body
  - The Vulnerability Management Procedures include procedures for a Vulnerability Impact Analysis:
    - The Vulnerability Impact Analysis shall refer to the target of evaluation and the assurance statements contained in the certificate. Vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT product
    - Where applicable, an attack potential calculation shall be performed in accordance with the relevant methodology included in the CC and CEM and the relevant state-of-the-art documents listed in Annex I, to determine the exploitability of the vulnerability. The AVA_VAN level of the EUCC certificate shall be taken into account

- In addition, the Vulnerability Management Procedures include procedures for a Vulnerability Impact Analysis Report:
  - Where the vulnerability impact analysis report determines that the vulnerability is not residual within the meaning of CC and CEM, and that it can be remedied, Vulnerability Remediation shall apply
  - Where the vulnerability impact analysis report determines that the vulnerability is not residual and that it cannot be remedied, the EUCC certificate shall be withdrawn in accordance with requirements for Withdrawal of an EUCC Certificate
  - The holder of the EUCC certificate shall monitor any residual vulnerabilities to ensure that it cannot be exploited in case of the changes in the operational environment
- Regarding Vulnerability Remediation, the procedures state that the holder of an EUCC certificate shall submit a proposal for an appropriate remedial action to the certification body. Certification body shall review the certificate. The scope of the review shall be determined by the proposed remediation of the vulnerability. It is interesting that these procedures only cover the proposed remedial action and not the performance of the remedial action.
- For Vulnerability Disclosures, the procedures in the Regulation involve:
  - The information provided by the certification body to the national cybersecurity certification authority shall include all elements necessary for the national cybersecurity certification authority to understand the impact of the vulnerability, the changes to be made to the ICT product and, where available, any information from the certification body on the broader implications of the vulnerability for other certified ICT products
  - The information provided in accordance with above paragraph shall not contain details of the means of exploitation of the vulnerability
  - The national cybersecurity certification authority shall share the relevant information received with other national cybersecurity certification authorities and ENISA.
  - Other national cybersecurity certification authorities may decide to further analyse the vulnerability or, after informing the holder of the EUCC certificate, request the relevant certification bodies to assess whether the vulnerability may affect other certified ICT products.
  - Upon withdrawal of a certificate, the holder of the EUCC certificate shall disclose and register any publicly known and remediated vulnerability in the ICT product on the European vulnerability database

  These procedures are more detailed that what is currently required per the CC. It will be interesting to see if the CCDB adopts some of EUCC's more rigorous approach to Vulnerability Management requirements.

- This next part of the Regulation – Mutual Recognition Agreements with Third Countries - is an area that will likely cause the biggest issues for the CCRA, the member Schemes and vendors that want to certify their products such s HCDs in EU-member countries. Al went through the slides (43 – 45) carefully during his presentation.

  a. Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a mutual recognition agreement with the Union.

     The mutual recognition agreement shall cover the applicable assurance levels for certified ICT products and, where applicable, protection profiles.

     Mutual recognition agreements may only be concluded with third countries that meet the following conditions:

     - Have an authority that:
       - Is a public body, independent of the entities it supervises and monitors in terms of organisational and legal structure, financial funding and decision making;

- Has appropriate monitoring and supervising powers to carry out investigations and is empowered to take appropriate corrective measures to ensure compliance
- Has an effective, proportionate and dissuasive penalty system to ensure compliance;

Note: Most Schemes under the CCRA do not currently have any type of investigative or enforcement powers; these last two requirements will be very difficult for CCRA member countries to meet

- Agrees to collaborate with the European Cybersecurity Certification Group and ENISA to exchange best practice and relevant developments in the field of cybersecurity certification and to work towards a uniform interpretation of the currently applicable evaluation criteria and methods, amongst others, by applying harmonised documentation that is equivalent to the state-of-the-art documents listed in Annex I Note: This is a good requirement
- Have an independent accreditation body performing accreditations using equivalent standards to those referred to in Regulation (EC) No 765/2008; Note: Would have to see this EU Regulation to determine if this would be an impediment or not
- Commit that the evaluation and certification processes and procedures will be carried out in a duly professional manner, taking into account compliance with the CC and CEM;
- Have the capacity to report previously undetected vulnerabilities and an established, adequate vulnerability management and disclosure procedure in place. Note: See the comments above under Vulnerability Management Procedures

b. Mutual recognition agreements may only be concluded with third countries that meet the following conditions:

- Have an authority that:
  - Have established procedures that enable it to effectively lodge and handle complaints and provide effective legal remedy for the complainant;
  - Establishing a mechanism for cooperation with other Union and Member States' bodies relevant to the cybersecurity certification under this Regulation

CC:2022 really does have any specific procedures that address complaints, but such procedures could be developed by the CCDB; the other mechanism "requirement: is what the CCRA is trying to establish with ENISA with respect to EUCC.

In addition to the conditions set out above, a mutual recognition agreement referred to in covering assurance level "high" may only be concluded with third countries where also the following conditions are met:

- The third country has an independent and public cybersecurity certification authority performing or delegating evaluation activities necessary to allow certification under assurance level 'high' that are equivalent to the requirements and procedures laid down for national cybersecurity authorities in this Regulation and in Regulation (EU) 2019/881 - this would be the various Schemes under CC;
- The mutual recognition agreement establishes a joint mechanism equivalent to the peer assessment for EUCC certification to enhance the exchange of practices and jointly solve issues in the area of evaluation and certification. **Note that there currently is not any type of peer review included in either CC:2022 or the CEM**

There were lots of comments about the Mutual Recognition requirements. The consensus was that it will be very difficult for the member nations in the CCRA or the CCRA itself to meet the requirements stated above to be able to establish Mutual Recognition Agreements with the EU to be able to certify products in the EU under EUCC. For example, requirements around monitoring, enforcement and establishing penalties will be very hard to establish on either a CCRA or a member nation level.

- Slide 46 just showed a list of some of the other topics covered by the EUCC Implementation Regulation. Al just quickly showed the slide during his presentation.
- Slides 47 and 48, as stated earlier, list the “State-of-the-Art” documents included in Annex I of the EUCC Implementation Regulation.
- The remainder of the presentation discussed what is in Annex IV – Assurance Continuity and Certificate Review - in the EUCC Implementation Regulation. The key items in Annex IV are:

  a. Scope of Assurance Continuity

     The following requirements for assurance continuity apply to the maintenance activities related to the following:

     - a re-assessment if an unchanged certified ICT product still meets its security requirements;
     - an evaluation of the impacts of changes to a certified ICT product on its certification;
     - if included in the certification, the application of patches in accordance with an assessed patch management process;
     - if included, the review of the certificate holder’s lifecycle management or production processes.

     This is like Assurance Continuity used by Schemes such as NIAP.

     The holder of an EUCC certificate may request the review of the certificate in the following cases:

     - the EUCC certificate is due to expire within nine months; Note: Not sure if 9 months is the time frame for CC; might be up to each Scheme
     - there has been a change either in the certified ICT product or in another factor which could impact its security functionality;
     - the holder of the certificate demands that the vulnerability assessment is carried out again to reconfirm the EUCC certificate’s assurance associated with the ICT product’s resistance against present cyberattacks. Note: This requirement may be something the CCDB might introduce into the CC for consistency with EUCC.

  b. Reassessment

     - Where there is a need to assess the impact of changes in the threat environment of an unchanged certified ICT product, a re-assessment request shall be submitted to the certification body.
     - The re-assessment shall be carried out by the same ITSEF that was involved in the previous evaluation by reusing all its results that still apply. The evaluation shall focus on assurance activities which are potentially impacted by the changed threat environment of the certified ICT product, in particular the relevant AVA_VAN family and in addition the assurance lifecycle (ALC) family where sufficient evidence about the maintenance of the development environment shall be collected again.
     - The ITSEF shall describe the changes and detail the results of the re-assessment with an update of the previous evaluation technical report.
     - The certification body shall review the updated evaluation technical report and establish a re-assessment report. The status of the initial certificate shall then be modified in accordance with requirements for Renewal of an EUCC Certificate.
     - The re-assessment report and updated certificate shall be provided to the national cybersecurity certification authority and ENISA for publication on its cybersecurity certification website

Note the reliance on Vulnerability Assessment. Also, the CC does not specifically discuss “reassessment” in this context like the EUCC Implementation Regulation does

c. Changes to a Certified ICT Product

I. Where a certified ICT product has been subject to changes, the holder of the certificate wishing to maintain the certificate shall provide to the certification body an impact analysis report.

Note: This and the following procedures for changes to an ICT product are much more detailed than required in the CC. Each country Scheme would probably have its own change procedures rather than having a centralized procedure applying to all CCRA countries.

The impact analysis report shall provide the following elements:

- an introduction containing necessary information to identify the impact analysis report and the target of evaluation subject to changes;
- a description of the changes to the product;
- the identification of affected developer evidence;
- a description of the developer evidence modifications;
- the findings and the conclusions on the impact on assurance for each change.

The certification body shall examine the changes described in the impact analysis report to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the impact analysis report.

Following the examination, the certification body determines the scale of a change as minor or major in correspondence to its impact.

II. Where the changes have been confirmed by the certification body to be minor, a new certificate shall be issued for the modified ICT product and a maintenance report to the initial certification report shall be established, under following conditions:

- The maintenance report shall be included as a subset of the impact analysis report, containing following sections:
  - introduction;
  - description of changes;
  - affected developer evidence;
- The validity date of the new certificate shall not exceed the date of the initial certificate. Note: This is different than, for instance NIAP, where Assurance Continuity can extend the validity of a certificate.

II. The new certificate including the maintenance report shall be provided to ENISA for publication on its cybersecurity certification website.

III. Where the changes have been confirmed to be major, a re-evaluation shall be carried out in the context of the previous evaluation and by reusing any results from the previous evaluation that still apply. Note: It is interesting that the regulation does not define what is a “major” change; leaves it open to interpretation and subjectivity

IV. After completion of the evaluation of the changed target of evaluation, the ITSEF shall establish a new evaluation technical report. The certification body shall review the updated evaluation technical report and, where applicable, establish a new certificate with a new certification report.

V. The new certificate and certification report shall be provided to ENISA for publication.

For the most part these procedures are like what most Schemes under CC do for Assurance Continuity

d. Patch Management

These procedures encompass an area where in Al's view CC and most Schemes under the CCRA are very deficient. The CCDB should adapt what is in this regulation for Patch Management to Common Criteria.

I. A patch management procedure provides for a structured process of updating a certified ICT product. The patch management procedure including the mechanism as implemented into the ICT product by the applicant for certification can be used after the certification of the ICT product under the responsibility of the conformity assessment body.

The applicant for certification may include into the certification of the ICT product a patch mechanism as part of a certified management procedure implemented into the ICT product under one of the following conditions:

- the functionalities affected by the patch reside outside the target of evaluation of the certified ICT product;
- the patch relates to a predetermined minor change to the certified ICT product;
- the patch relates to a confirmed vulnerability with critical effects on the security of the certified ICT product.

II. If the patch relates to a major change to the target of evaluation of the certified ICT product in relation to a previously undetected vulnerability having no critical effects to the security of the ICT product, the provisions for Renewal of an EUCC Certificate apply.

III. The patch management procedure for an ICT product will be composed of the following elements:

- the process for the development and release of the patch for the ICT product;
- the technical mechanism and functions for the adoption of the patch into the ICT product;
- a set of evaluation activities related to the effectiveness and performance of the technical mechanism.

IV. During the certification of the ICT product:

- the applicant for certification of the ICT product shall provide the description of the patch management procedure;
- the ITSEF shall verify the following elements:
- the developer implemented the patch mechanisms into the ICT product in accordance to the patch management procedure that was submitted to certification;
- the target of evaluation boundaries are separated in a way that the changes made to the separated processes do not affect the security of the target of evaluation;
- the technical patch mechanism performs in accordance with the provisions of this section and the applicant's claims;
- the certification body shall include in the certification report the outcome of the assessed patch management procedure.

V. The holder of the certificate may proceed to apply the patch produced in compliance of the certified patch management procedure to the concerned certified ICT product and shall take the following steps within 5 working days in the following cases:

- in the case referred to in point 2(a), report the patch concerned to the certification body that shall not change the corresponding EUCC certificate;
- in the case referred to in point 2(b), submit the patch concerned to the ITSEF for review. The ITSEF shall inform the certification body after the reception of the patch upon which the certification body takes the appropriate action on the issuance of a

new version of the corresponding EUCC certificate and the update of the certification report;

- in the case referred to in point 2(c), submit the patch concerned to the ITSEF for the necessary re-evaluation but may deploy the patch in parallel. The ITSEF shall inform the certification body after which the certification body starts the related certification activities.

The only issue with these procedures is that, like everything else ENISA seems to produce, it is highly bureaucratic.

6. At this point Al turned the meeting over to Ira McDonald to lead the discussion on the status of the HCS Security Guidelines (there has been no progre4ss since the last IDS Session in November 2023) and to give his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF) – Slides 59-63. Contact Ira at blueroofmusic@gmail.com for any questions on his liaison report

7. **Wrap Up**

   - The next IDS Working Group Meeting will be on May 30, 2023. Main topics of the meeting will be updated status of the HCD iTC and HIT, debrief of this IDS May 2024 Face-to-Face, and the more complete discussion of the EUCC Implementation Regulation.
   - Next IDS Face-to-Face Meeting will be during the August 2024 PWG Virtual Face-to-Face Meeting August 12-14, 2024 (likely on August 14, 2024).

   Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 PM ET on May 8, 2024.