IDS WG Meeting Minutes
September 7, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on September 7, 2023.

Attendees

Graydon Dobson	Lexmark
Smith Kennedy	HP
Alan Sukert	
Brian Volkoff	Ricoh
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD iTC and the HCD Interpretation Team (HIT)
   - Special Topic on a new proposed EU cybersecurity law
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al began discussing the results of the August 28th HCD Integration Team (HIT) Meeting:

   There are currently 13 open HIT issues, including a new issue HCD-IT #13 that just came in that day. Issue HCD-IT #13 is titled "**The component name of FDP_DSK_EXT.1 in the HCD cPP ("Protection of Data on Disk") is misleading**".

   The issue here, as stated in HCD-IT #13 is that "The component name of FDP_DSK_EXT.1 in the HCD cPP section B.1.3 is "Protection of Data on Disk," which is misleading since it implies that it only applies to HCDs that include a disk drive. HCDs can have non-volatile storage holding D.USER.DOC and/or D.TSF.CONF without including a disk. The FDP_DSK_EXT.1.1 element refers to a "Nonvolatile Storage Device" rather than a disk, which seems more appropriate than "disk". However, ST authors reading the component name of the SFR could mistakenly determine that this SFR does not apply to their TOE simply because it does not include a disk.

   FDP_DSK_EXT.1 is loosely derived from the SFR of the same nomenclature in the FDE EE cPP. However, the FDE SFR refers to "disk" or "drive" in both the component name and elements, which is appropriate for the FDE EE cPP. The HCD cPP SFR modified the SFR elements to appropriately address the usage in the HCD cPP, but did not modify the SFR component name or family.

   At minimum, the SFR component name could be changed to more accurately reflect the SFR's usage in the HCD cPP. The suggested change is from "Protection of Data on Disk" to "Protection of Data in Nonvolatile Storage". This would impact both sections B.1.3 and D.3.1 of the HCD cPP. In the HCD SD, the title of section 3.1.3 is impacted.

   Since the FDP_DSK_EXT.1 SFRs in the FDE and HCD cPPs have little in common, there is no need to maintain the same SFR family. Therefore, it would also be appropriate to change the SFR's family in the HCD cPP to clarify its scope. The suggested change is from "FDP_DSK_EXT" to "FDP_NVS_EXT". This would again impact sections B.1.3 and D.3.1 of the HCD cPP and section 3.1.3 in the HCD SD. In addition, the following references to FDP_DSK_EXT.1 would need to be updated:

   - App Note in C.2.1 (FPT_WIPE_EXT.1
   - Row for FDP_DSK_EXT.1 in Table 24 (section I.10)
   - Row for O.STORAGE_ENCRYPTION with FDP_DSK_EXT.1 in Table 21 (section I.9)
   - HCD SD: Reference in the last paragraph of the TSS for FPT_WIPE_EXT (section 4.2.1.1)

The basic issue is that the name of this SFR implies that it is only for HCDs that store user or confidential data on non-volatile hard disk drives, but today many of not most HCDs use SSDs or wear-leveling drives instead of hard disk drives. So, a name change for the SFR to a more appropriate name that would give an ST author that shows it applies to all non-volatile memory and not just hard disk drive sis more appropriate.

This issue will be discussed fully at the next HIT Meeting on Monday, Sep 11th, but Brian and Graydon who are on the HIT both agreed this is a valid issue; Brian also said that he had experienced this problem at a previous HCD certification.

- As for the status of the other open issues:
  - Issue HCD-IT #1: Three HIT members have a proposal for AES CFB mode support for the CCDB WG crypto catalog that has been provide to Kwangwoo Lee. He will forward it the proposal to our CCDB Liaison ho will bring it to the CCDB for consideration.
  - Issue HCD-IT #2: Ohya-san and Al volunteered to review the changes to the SD; once that is done Jerry will finish the TD and move the file to the Interpretation Baseline.

    We agreed on a TD naming convention of HITRfIDecision<year><nn> with NN starting sequentially from '01'. We also agreed that all TDs would be posted on the HCD iTC OnlyOffice site and would be sent to NIAP to be posted on the NIAP and CC Portals.
  - Issues HCD-IT #4-7: Brian has made good progress and should be done in another week or two.
  - Issue HCD-IT #8. This is actively being worked on the two HIT members assigned to this issue..
  - Issue HCD-IT #9: Awaiting resolution of Issue #2 so Jerry can work on this issue.
  - Issue #10: We agreed to work resolution of this issue live at the next HIT Meeting..
  - HCD-IT #11: The HIT still needs to have the necessary discussion on this issue because it is a fundamental one – do we encrypt all keys or just plaintext keys.
  - HCD-IT #12: This issue is similar to Issues HCD-IT #4-7, except instead of coming from NIAP this came from the Canadian Scheme. Brian will work this issue along with Issues HCD-IT #4-7.

  The last thing we did at the meeting was prioritize the open issues. We felt issues HCD-IT #2, #9 and #10 were "low hanging fruit" that could be completed quickly. Of the remaining issues, the priories were:

  1. HCD-IT #4 - #7 and #12
  2. HCD-IT #11
  3. HCD-IT #8
  4. HCD-IT #1

4. Al then presented his special topic for the day, which is a look at a new proposed EU Cybersecurity Law – the EU Cyber Solidarity Law. The slides for this presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/EU Cyber Solidarity Act.pdf.

   Al did not cover every bullet on each of the slides during the discussion; he just pointed out select bullets or summarized the slide's content. See the slides in the link above to get the full content.

   The official name of this proposal, proposed on 18 April 2023, is "**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** - **laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents**". Its broad gals were to strengthen capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents through the following actions:

   - **Deployment of a pan-European infrastructure of Security Operations Centres ('European Cyber Shield')** to build and enhance common detection and situational awareness capabilities;

- **Creation of a Cybersecurity Emergency Mechanism** to support Member States in preparing for, responding to, and immediate recovery from significant and largescale cybersecurity incidents;
- Establish a European Cybersecurity Incident Review Mechanism to review and assess significant or large-scale incidents

a. The objectives of this Regulation are the standard objectives one would expect for an endeavor of this type:

   - Strengthen common Union detection and situational awareness of cyber threats and incidents;
   - Reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents;
   - Enhance Union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents

b. Some key definitions to help understand the EU Cyber Solidarity Act are:

   - **Cross-border Security Operations Centre ("Cross-border SOC"):** A multi-country platform that brings together in a coordinated network structure national SOCs from at least three Member States who form a Hosting Consortium, and that is designed to prevent cyber threats and incidents and to support the production of high-quality intelligence, notably through the exchange of data from various sources, public and private, as well as through the sharing of state-of-the-art tools and jointly developing cyber detection, analysis, and prevention and protection capabilities in a trusted environment
   - **public body:** A body governed by public law as defined in Directive 2014/24/EU of the European Parliament and the Council
   - **entity:** An entity as defined in Directive (EU) 2022/2555
   - **trusted providers:** Managed security service providers as defined in of Directive (EU) 2022/2555 selected in accordance with this Regulation

c. The key to the EU Cyber Solidarity Act is the establishment of the European Cyber Shield. It is an interconnected pan-European infrastructure of Security Operations Centres to develop advanced capabilities for the Union to detect, analyse and process data on cyber threats and incidents in the Union. The European Cyber Shield is to :

   - Pool and share data on cyber threats and incidents from various sources through cross-border SOCs;
   - Produce high-quality, actionable information and cyber threat intelligence, through the use of state-of-the art tools, notably Artificial Intelligence and data analytics technologies;
   - Contribute to better protection and response to cyber threats;
   - Contribute to faster detection of cyber threats and situational awareness across the Union;
   - Provide services and activities for the cybersecurity community in the Union, including contributing to the development advanced artificial intelligence and data analytics tools.

   Al noted the inclusion of AI in the European Cyber Shield goals.

d. To participate in the European Cyber Shield, each Member State is to designate at least one National Security Operations Centre (SOC). The National SOC is to be a public body

   Al didn't go through the specific roles for the National SOC, but in general its.role is to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cybersecurity threats and incidents and contributing to a Cross-border SOC

e. The regulation also creates Cross-Border Security Operations Centres (SOCs). These are a Hosting Consortium consisting of at least three Member States, represented by National SOCs, committed to working together to coordinate their cyber-detection and threat monitoring activities are to be eligible to participate in actions to establish a Cross-border SOC. The Regulation goes into how this Hosting Consortium is to be selected, the written consortium agreement for its implementation, its legal representation by a National SOC acting as coordinating SOC and the coordinating SOC's responsibilities.

Members of a Hosting Consortium are to exchange relevant information among themselves within the Cross-border SOC including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures and similar information, where such information sharing:

- Aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;
- Supports the development of an EU Cyber Shield
- Establishes and operates a Cyber Emergency Mechanism to support Member States in preparing for and responding to significant cybersecurity incidents

Al noted that this Regulation is building a large bureaucracy, which will become more evident as he goes further into the presentation.

To encourage exchange of information between Cross-border SOCs, Cross-border SOCs are to ensure a high level of interoperability between themselves via cooperation agreements with one another. To facilitate the interoperability between the Cross-border SOCs, the (EU) Commission may, by means of implementing acts, after consulting the ECCC, specify the conditions for this interoperability and the procedural arrangements for the information sharing.

f. From a security perspective, Member States participating in the European Cyber Shield are to:

- Ensure a high level of data security and physical security of the European Cyber Shield infrastructure
- Ensure that the infrastructure is adequately managed and controlled in such a way as to protect it from threats
- Ensure its security and that of the systems, including that of data exchanged through the infrastructure.
- Ensure that the sharing of information within the European Cyber Shield with entities which are not Member State public bodies does not negatively affect the security interests of the Union.

The Commission may adopt implementing acts laying down technical requirements for Member States to comply with their obligation under this Regulation.

Al noted these are the types of security :”measures” one would typically expect a Regulating like this to require.

g. The next thing the Regulation establishes is a Cyber Emergency Mechanism to improve the Union's resilience to major cybersecurity threats and prepare for and mitigate the short-term impact of significant and large-scale cybersecurity incidents. This Mechanism is to support the following types of actions:

- Preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;
- Response actions, supporting response to and immediate recovery from significant and large-scale cybersecurity incidents, to be provided by trusted providers participating in the EU Cybersecurity Reserve;
- Mutual assistance actions consisting of the provision of assistance from national authorities of one Member State to another Member State

Again, more bureaucracy. The main thread is that the Regulation establishes a hierarchy – there is the European Cyber Shield which is the overall umbrella. Under it are the National SOCs which are banded together in groups of at least three for form the Cross-Border SOCs. The EU Cybersecurity Reserve, which is discussed next, provides resources to the SOCs to help them and their entities to resolve cybersecurity incidents.

h. Next the Regulation establishes a EU Cybersecurity Reserve to assist in responding or providing support for responding to significant or large-scale cybersecurity incidents, and immediate recovery from such incidents. This "Reserve" consists of incident response services from trusted providers (see later in the presentation) selected in accordance with the criteria laid down in the Regulation and includes pre-committed services deployable in all Member States.

Users of the services from the EU Cybersecurity Reserve include Member States' cyber crisis management authorities, CSIRTs, Union institutions, bodies and agencies. Users use the services from the EU Cybersecurity Reserve to respond or support response to, and immediate recovery from, significant or large-scale incidents affecting entities operating in critical or highly critical sectors.

The Commission has overall responsibility for the implementation of the EU Cybersecurity Reserve and determines its priorities. The Commission may also specify the types and the number of response services required for the EU Cybersecurity Reserve.

Users may request services from the EU Cybersecurity Reserve to support response to and immediate recovery from significant or large-scale cybersecurity incidents. To receive support from the EU Cybersecurity Reserve, the users (in this case a 'User' is not defined in the Regulation but we think is a Nation State or entity within a Nation State) are to take measures to mitigate the effects of the incident for which the support is requested. Al found it interesting that before a User can request services from the Reserve it must first take some type of mitigation step against the incident it is asking for help to respond to – seems almost "bass ackwards" as the saying goes. Requests for support from users referred to in are transmitted to the Commission and ENISA via the Single Point of Contact designated or established by the Member State (Al notes establishing a single point of contact is a good thing).

Slide 15 gives the information that a request for support from the EU Cybersecurity Reserve must include – items such as affected entity and potential impacts of the incident and the planned use of the requested support and the measures taken to mitigate the incident for which the support is requested.

To prioritise requests for EU Cybersecurity Reserve services, in the case of multiple concurrent requests, the following criteria are to be taken into account, where relevant:

- The severity of the cybersecurity incident;
- The type of entity affected, with higher priority given to incidents affecting essential entities;
- The potential impact on the affected Member State(s) or users;
- The potential cross-border nature of the incident and the risk of spill over to other Member States or users;
- The measures taken by the user to assist the response, and immediate recovery efforts

Al noted these criteria are reasonable and are a good set to use making similar types of decisions in other circumstances.

EU Cybersecurity Reserve services are to be provided in accordance with specific agreements between the service provider and the user to which the support under the EU Cybersecurity Reserve is provided.

Within one month from the end of the support action, the users are to provide the Commission and ENISA with a summary report about the service provided, results achieved and the lessons learned

i. Slide 18 covers provisions for when significant or large-scale cybersecurity incidents originate from or result in disasters. Al did not go through this slid in any detail during the meeting; he just indicated that there are several EU offices and treaties involved.

j. For Trusted Providers, as defined in Slide 4 (think 3rd Party Providers in our terms), who are involved in providing services via the EU Cybersecurity Reserve, any contractual arrangement with a Trusted Provider must ensure that the Trusted Provider:

- Ensures the services that may be deployed in all Member States, taking into account in particular national requirements for the provision of such services, including certification or accreditation;
- Ensures the protection of the essential security interests of the Union and its Member States;
- Ensures that it brings EU added value, including promoting the development of cybersecurity skills in the EU

Slide 20 indicates what should be included a procurement document for obtaining a Trusted Provider's services. It includes items such as:

- The provider demonstrates that its personnel have the highest degree of professional integrity, independence, responsibility, and the requisite technical competence to perform the activities in their specific field;
- The provider, its subsidiaries and subcontractors have in place a framework to protect sensitive information relating to the service;
- The provider provides sufficient proof that its governing structure is transparent;
- The provider has appropriate security clearance;
- The provider has the relevant level of security for its IT systems

All reasonable things to ask for from a 3rd Party supplier.

The selection criteria for a Trusted Provider, per the Regulation, are to include:

- The provider is equipped with the hardware and software technical equipment necessary to support the requested service;
- The provider is able to demonstrate that it has experience in delivering similar services to relevant national authorities or entities operating in critical or highly critical sectors;
- The provider is able to provide the service within a short timeframe in the Member State(s) where it can deliver the service;

  The provider is able to provide the service in the local language of the Member State(s) where it can deliver the service – this may seem to be a unique criteria for the EU, but given the new demographics in the US per the 2020 Census a working knowledge of Spanish is almost a pre-requisite today of any 3rd Party supplier.

k. The Regulation also covers support for Third Countries not part of the EU such as the UK. Third countries may request support from the EU Cybersecurity Reserve where Association Agreements concluded regarding their participation in DEP (wasn't defined in the Regulation nor were a lot of acronyms used) provide for this. Support from the EU Cybersecurity Reserve is in accordance with this Regulation, and complies with any specific conditions laid down in the Association Agreements

Users from associated third countries eligible to receive services from the EU Cybersecurity Reserve is to include competent authorities such as CSIRTs and cyber crisis management authorities. Each third country eligible for support from the EU Cybersecurity Reserve is to designate an authority to act as a single point of contact for the purpose of this Regulation

Prior to receiving any support from the EU Cybersecurity Reserve, third countries are to provide to the Commission and the High Representative (does not define who that is) information about their cyber resilience and risk management capabilities, including at least information on national measures taken to prepare for significant or large-scale cybersecurity incidents, as well as information on responsible national entities, including CSIRTs or equivalent entities, their capabilities and the resources allocated to them

l. Finally, the Regulation provides for a Cybersecurity Incident Review Mechanism.

At the request of the Commission, the EU-CyCLONe (not sure what that is) or the CSIRTs network, ENISA is to review and assess threats, vulnerabilities and mitigation actions with respect to a specific significant or large-scale cybersecurity incident. Following the completion of a review and assessment of an incident, ENISA is to deliver an incident review report to the CSIRTs network, the EU-CyCLONe and the Commission to support them in carrying out their tasks. Where relevant, the Commission shall share the report with the High Representative.

To prepare the incident review report referred to above, ENISA is to collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA is to also collaborate with entities affected by significant or large-scale cybersecurity incidents and may also consult other types of stakeholders.

The report is to cover a review and analysis of the specific significant or large-scale cybersecurity incident, including the main causes, vulnerabilities and lessons learned. It is to protect confidential information, in accordance with Union or national law.

Where appropriate, the report is to draw recommendations to improve the Union's cyber posture. Where possible, a version of the report is to be made available publicly and only include public information.

At the end of the presentation Smith asked the question "What does the EU Cyber Solidarity Act have to do with PPs and cPPs?" We discussed the question for a few minutes, and came to the conclusion that there is no direct effect of this proposed Regulation, if enacted, on development of PPs and cPPs.

However, there is an indirect effect. Given the development of EUCC. it is certainly a possibility, however unlikely, that one of more of the provisions of this Regulation could find itself included in some fashion into one of the functional or assurance requirements in EUCC. And given the strong efforts by ENISA and the CCMB (Common Criteria Management Board) to find a way to get some type of a Recognition Arrangement (RA) between EUCC and Common Criteria, anything that is in EUCC could find its way into the CC if such an RA is eventually achieved.

So, in that sense what is in this proposed Regulation could be important to PP or cPP developers in some way in the future.

5. **Actions:** None

Next Steps

The next IDS WG Meeting will be September 21, 2023 at 3:00P ET / 12:00N PT. Main topics will be the latest status of the HCD iTC and HIT and likely a special topic on a TBD topic