IDS WG Meeting Minutes
October 5, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on October 5, 2023.

Attendees

Smith Kennedy	HP
Alan Sukert	
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
    - Latest updates on the HCD Interpretation Team (HIT)
    - Special Topic on the EU NIS 2 Directive
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 October 2nd HCD Integration Team (HIT) Meeting:
    - The original intent of the meeting was to process in real time HCD-IT #10, **Mapping issue between Mandatory 'O.KEY_MATERIAL' objective and Cond. Mandatory 'FPT_KYP_EXT.1'**. However, Jerry began to ask several process issues about his Technical Decision and how it would be processed. There were also questions about what should be the published date for each TD and the corresponding file containing the fix in the HCD CPP or HCD SD (or both) for that TD. After some discussion we decided these process issues were best decided at a separate Editors Meeting that Jerry was to schedule later that week (Note: The meeting was eventually scheduled for Tuesday, Oct 10th).

      Also, because of these process issues we decided that we would hold off the real-time processing of HCD-IT #10 until the next HIT Meeting on Oct 16th.

      Smith asked about the transition to use of GitHub for the end-to-end process. Al indicated that that there are going to be issues that have t be worked out since we are the first Interpretation Team to use GitHub this way.
    - For the rest of the meeting, we did a status of the remaining open Issues:
        - HCD-IT #1: Tom Benkart added notes to the issue indicating that he thought Ohya-san's solution presented in his note in the issue would resolve the issue and urged HIT members to look at the PowerPoint slide linked in Ohya-san's comment. Al gave all HIT members an action to review Ohya-san's slides before the next HIT Meeting.
        - HCD-IT #2: See above text.
        - HCD-IT #4 – HCD-IT #7: Brian Volkoff has finished all the corrections for these four issues. He now needs a couple of HIT members to double check what he did to make sure (1) he made all the changes he needed to make and (2) he made them all correctly.
        - HCD-IT #8: Joe McDonald stated he needs more information on the path forward to properly address the threat of the data stored in NVM being removed from the device.
        - HCD-IT #8: This is awaiting Al's action to determine why the HCD PP only required plaintext keys to be destroyed and not all keys to be destroyed. (Note: This issue is linked to Issue HCD-IT #11)
        - HCD-IT #9: Jerry will fix this issue as soon as he finishes HCD-IT #2. Sato-san sent an email indicating that he needed this issue completed as soon as possible because of an ongoing certification. Al asked Jerry to start work on this issue in parallel with completing HCD-IT #2.
        - HCD-IT #10: We will go through resolution of this issue on-line as a team at the beginning of the next HIT Meeting once the process issues are addressed as indicated above.

- HCD-IT #11: Waiting on AL to complete his action to determine why the HCD PP only required plaintext keys to be destroyed and not all keys to be destroyed.
- HCD-IT #12: Cory included a note in the Issue proposing update to several of the threat definitions in the HCD cPP as the solution to this issue. Al gave everyone in the HIT the action to review Cory's threat definition updates before this HIT Meeting; that action has been extended to the next HIT Meeting.
- HCD-IT #13: The solution to this issue was agreed upon by the HIT at our last HIT Meeting; just need Tom, Brian and Jerry to create the TD and the updated HCD cPP and HCD SD for this issue.
- HCD-IT #14: This issue got lost because it was never formally processed by the HIT. This issue is titled "**Inconsistent section location of SFRs between PP and SD for FIA_AFL.1 and FCS_CKM.1/AKG**" and the issue reads:

  "This is an editorial comment, possibly on the Supporting Document (SD). Sections where FIA_AFL.1 and FCS_CKM.1/AKG differ between PP and SD, where it creates a confusion on whether these SFRs are Conditionally Mandatory or not.

  In PP:
  FIA_AFL.1 is listed under "Appendix B: Conditionally Mandatory Requirements".
  FCS_CKM.1/AKG is listed under Section "5. Security Functional Requirements".

  In SD:
  FIA_AFL.1 is listed under "Chapter 2. Evaluation Activities for SFRs" and not under "Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements" as per the PP.
  FCS_CKM.1/AKG is listed under "Chapter 3. Evaluation Activities for Conditionally Mandatory Requirements" and not under "Chapter 2. Evaluation Activities for SFRs" as per the PP."

  At the meeting we assigned a Priority 2 to the issue and assigned it initially to Brian and Jerry to work the fix.
- HCD-IT #15: This was the issue generate by Al per his action from the 9/18 HIT Meeting to address the problem raised via email between Jerry and Brian that was discussed at that HIT Meeting.

  This issue is titled **"FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication) improperly titled when referenced as a Dependency in HCD cPP v1.0**" and the issue text reads:

  In working on issue HCD-IT #2, Jerry Colunga noticed that multiple SFRs in HCD cPP v1.0 listed FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication) as a dependency. However, HCD cPP v1.0 defines in A.4.3 the SFR as FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication) and not the FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication).

  The title of SFR FCS_COP.1/CMAC being used when it is being cited as a dependency - FCS_COP.1/CMAC Cryptographic Operation (for keyed-hash message authentication) - is incorrect; the title of the SFR - FCS_COP.1/CMAC Cryptographic Operation (for cipher-based message authentication) - in A.4.4 is the correct title and should be used whenever SFR FCS_COP.1/CMAC is referenced in the HD cPP.

  The incorrect titles for FCS_COP.1/CMAC in the various dependency lists need to be changed to the proper title of the SFR.

  We gave this issue Priority 2 and initially assigned it to Brian to address

4. Al then presented his special topic for the day, which is a look at the EU NIS 2 Directive on "**measures for a high common level of cybersecurity across the Union"** The slides for this presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIS 2.pdf.

   NIS 2 was published on 14 December 2022 and superseded the NIS 1 Directive. As was the case in some previous special presentations. Al did not go through every slide in detail, but only picked out key points on some slides or just summarized other slides.

a. The general purpose of NIS 2 is to lay down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market: More specifically, the purpose of this Directive is to lay down:

   - Obligations that require Member States to adopt national cybersecurity strategies and to designate or establish
   - Competent authorities, cyber crisis management authorities, single points of contact on cybersecurity (single points of contact) and computer security incident response teams (CSIRTs);
   - Cybersecurity risk-management measures and reporting obligations for entities of a type referred to in Annex I or II as well as for entities identified as critical entities;
   - Rules and obligations on cybersecurity information sharing;
   - Supervisory and enforcement obligations on Member States

   The key point is that, unlike other EU Regulations and Directives. NIS 2 is aimed principally to the various Member States of the EU rather than to the EU as a whole.

b. The Scope of NIS 2, as shown in Slides 3 and 4, is aimed mainly at certain public or private entities of a type referred to in Annex I or II of the Directive (which are shown in Slides 37-39 and will be discussed later) and at public administration entities. Note that the definition of ‘entities’ will be discussed below.

c. NIS 2 is built around the concept of Essential and Important Entities. The easiest was to define the two is that any entity that is not an Essential Entity is an Important Entity. The types of entities that are deemed ‘Essential’ include entities defined as essential in Annex I and II (again see Slide 37-39), public administration entities and providers of public electronic communications networks.

d. Some key definitions to understand NIS 2:

   - ‘incident’: An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems
   - ‘large-scale cybersecurity incident’: An incident which causes a level of disruption that exceeds a Member State’s capacity to respond to it or which has a significant impact on at least two Member States
   - ‘risk’: The potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident
   - ‘vulnerability’: A weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat
   - ‘entity’: A natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations
   - ‘significant cyber threat’: A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage
   - ‘near miss’: An event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialize

   Al noted that the definitions of risk and vulnerability are somewhat different from the standard definitions of these terms we are used to. Also, the concept of a “near miss” is something he hasn’t seen in other standards or directives either if the US or in the U before, but shows up later several times in NIS 2.

e. NIS 2, like most EU Regulations and Directives, is very bureaucratic-centered. But NIS 2 does require each Member State to set up its own National Cybersecurity Framework, similar to the NIST Cybersecurity Framework. These National Cybersecurity Frameworks are to include items such as:

   - Objectives and priorities of the Member State's cybersecurity strategy
   - A governance framework to achieve the objectives and priorities
   - An identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors

     Note that like other EU Regulations the EU is big on measurements; you will see this throughout this Directive
   - A policy framework for enhanced coordination between the competent authorities under this Directive and the competent authorities for the purpose of information sharing on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks d

f. These National Cybersecurity Frameworks are required to adopt policies (always a good thing) for areas such as:

   - Addressing cybersecurity in the supply chain for ICT products and ICT services used by entities for the provision of their services;
   - On the inclusion and specification of cybersecurity-related requirements for ICT products and ICT services in public procurement, including in relation to cybersecurity certification, encryption and the use of open-source cybersecurity products;
   - Managing vulnerabilities, encompassing the promotion and facilitation of coordinated vulnerability disclosure under this Directive;
   - Related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables;
   - Promoting the development and integration of relevant advanced technologies aiming to implement state-of-the-art cybersecurity risk-management measures;
   - Promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at citizens, stakeholders and entities;
   - Strengthening the cyber resilience and the cyber hygiene baseline of small and medium-sized enterprises, in particular those excluded from the scope of this Directive, by providing easily accessible guidance and assistance for their specific needs

   You see the inclusion of the supply chain cybersecurity which is a current initiative with the EU

g. One of the "smart" things NIS 2 included was the requirement that there be a Single Point of Contact within each Member State for purposes of this Directive. More specifically, the Directive requires that:

   - Each Member State are to designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities) Note: NIS 2 does not define what a 'Competent Authority' is; just defines what the tasks of a 'Competent Authority' are
   - The competent authorities referred to above are to monitor the implementation of this Directive at national level
   - Each Member State are to designate or establish a single point of contact. Where a Member State designates or establishes only one competent authority pursuant to the 1st bullet, that competent authority is to also be the single point of contact for that Member State
   - Each single point of contact is to exercise a liaison function to ensure cross-border cooperation of its Member State's authorities with the relevant authorities of other Member

States, and, where appropriate, with the Commission and ENISA, as well as to ensure cross-sectoral cooperation with other competent authorities within its Member State

- Member States are to ensure that their competent authorities and single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive

h. As an example of the "bureaucracy" aspect of NIS 2, each Member State has to establish in addition to a National Cybersecurity Framework a National Cyber Management Framework. The requirements for this National Cyber Management Framework include items such as:

- Each Member State is to designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities
- Member States are to ensure coherence with the existing frameworks for general national crisis management
- Where a Member State designates or establishes more than one cyber crisis management authority, it is to clearly indicate which of those authorities is to serve as the coordinator for the management of large-scale cybersecurity incidents and crises
- Each Member State is to adopt a national large-scale cybersecurity incident and crisis response plan that is to lay down, in particular items such as:
    - The objectives of national preparedness measures and activities;
    - The tasks and responsibilities of the cyber crisis management authorities;
    - The cyber crisis management procedures;
    - National preparedness measures, including exercises and training activities;
    - The relevant public and private stakeholders and infrastructure involved;
    - National procedures and arrangements between relevant national authorities and bodies

i. Each Member Nation is to set up one or more Computer Security Incident Response Teams (CSIRTs). These CSIRTs must comply with the requirements set out in Slide 16 and are to cover at least the sectors, subsectors and types of entities referred to in Slides 37-39, and are responsible for incident handling in accordance with a well-defined process. Some of the other high-lever requirements on the CSIRTs are that they must:

- Member States are to ensure that each CSIRT has at its disposal an appropriate, secure, and resilient communication and information infrastructure through which to exchange information with essential and important entities and other relevant stakeholders
- The CSIRTs are cooperate and, where appropriate, exchange relevant information with sectoral or cross-sectoral communities of essential and important entities
- The CSIRTs are to participate in peer reviews
- The CSIRTs may establish cooperation relationships with third countries' national computer security incident response teams
- Member States are to facilitate effective, efficient and secure information exchange with those third countries' national computer security incident response teams
- The CSIRTs may cooperate with third countries' national computer security incident response teams or equivalent third-country bodies
- Member States may request the assistance of ENISA in developing their CSIRT

"Third Countries" in this context likely meant the UK.

The specific requirements that CSIRTs have to meet include:

- The CSIRTs are to ensure a high level of availability of their communication channels by avoiding single points of failure, and are to have several means for being contacted and for contacting others at all times;

- The CSIRTs' premises and the supporting information systems are to be located at secure sites;
- The CSIRTs are to ensure the confidentiality and trustworthiness of their operations;
- The CSIRTs are to be equipped with redundant systems and backup working space to ensure continuity of their services

Finally, CSIRTs are to perform the following tasks:

- Monitoring and analysing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;
- Providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyber threats, vulnerabilities and incidents, if possible in near real-time;
- Responding to incidents and providing assistance to the essential and important entities concerned, where applicable;
- Collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;
- Providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;
- Participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request;
- Where applicable, acting as a coordinator for the purposes of the coordinated vulnerability disclosure;
- Contributing to the deployment of secure information-sharing tools

These are the kinds of tasks one would expect an “incident response team” to perform.

j. Another of the CSIRTs additional roles is to act as a coordinator for the purposes of coordinated vulnerability disclosure. The tasks of the CSIRT designated as coordinator are to include:

- Identifying and contacting the entities concerned;
- Assisting the natural or legal persons reporting a vulnerability; and
- Negotiating disclosure timelines and managing vulnerabilities that affect multiple entities

Along with that ENISA is required to set up a European vulnerability database similar to the CVE security vulnerability database. The database is to include:

- Information describing the vulnerability;
- The affected ICT products or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited;
- The availability of related patches and, in the absence of available patches, guidance provided by the competent authorities or the CSIRTs addressed to users of vulnerable ICT products and ICT services as to how the risks resulting from disclosed vulnerabilities can be mitigated

k. NIS 2 also includes requirements pertaining to cooperation, both at the National level, between Member States and with Third Party Nations.

Regarding cooperation at the National level, Member States have to comply with requirements such as:

- Where they are separate, the competent authorities, the single point of contact and the CSIRTs of the same Member State are to cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive

- Member States are to ensure that their CSIRTs or, where applicable, their competent authorities, receive notifications of significant incidents and incidents, cyber threats and near misses
- Member States are to ensure that their CSIRTs or, where applicable, their competent authorities inform their single points of contact of notifications of incidents, cyber threats and near misses submitted
- Member States are to, to the extent possible, ensure appropriate cooperation between those bodies and law enforcement authorities, data protection, the national regulatory authorities, the competent authorities, as well as the competent authorities under other sector-specific Union legal acts, within that Member State
- Member States are to ensure that their competent authorities under this Directive and their competent authorities cooperate and exchange information on a regular basis with regard to the identification of critical entities, on risks, cyber threats, and incidents as well as on non-cyber risks, threats and incidents affecting entities identified as critical entities, and the measures taken in response to such risks, threats and incidents

l. In another bureaucratic part of NIS 2, the Directive requires the establishment of a Coordination Group. The Coordination Group is to be composed of representatives of Member States, the Commission and ENISA and is to have tasks that include:

- To provide guidance to the competent authorities in relation to the transposition and implementation of this Directive;
- To provide guidance to the competent authorities in relation to the development and implementation of policies on coordinated vulnerability disclosure;
- To exchange best practices and information in relation to the implementation of this Directive, including in relation to cyber threats, incidents, vulnerabilities, near misses, awareness-raising initiatives, training, exercises and skills, capacity building, standards and technical specifications as well as the identification of essential and important entities;
- To exchange advice and cooperate with the Commission on emerging cybersecurity policy initiatives and the overall consistency of sector-specific cybersecurity requirements;
- To exchange best practices and information with relevant Union institutions, bodies, offices and agencies;
- To carry out coordinated security risk assessments of critical supply chains;
- To provide strategic guidance to the CSIRTs network and EU-CyCLONe on specific emerging issues;

  To establish the methodology and organisational aspects of the peer reviews, as well as to lay down the self-assessment methodology for Member States, with the assistance of the Commission and ENISA, and, in cooperation with the Commission and ENISA, to develop codes of conduct underpinning the working methods of designated cybersecurity experts;
- To prepare reports for the purpose of the review referred to in this Directive on the experience gained at a strategic level and from peer reviews;
- To discuss and carry out on a regular basis an assessment of the state of play of cyber threats or incidents, such as ransomware

m. NIS 2 also required the Member States to set up a network of national CSIRTs composed of representatives of the CSIRTs designated or established and the computer emergency response team for the Union’s institutions, bodies and agencies. This network of national CSIRTs would have tasks such as:

- To exchange information about the CSIRTs’ capabilities;
- To facilitate the sharing, transfer and exchange of technology and relevant measures, policies, tools, processes, best practices and frameworks among the CSIRTs;
- To exchange relevant information about incidents, near misses, cyber threats, risks and vulnerabilities;

- At the request of a member of the CSIRTs network potentially affected by an incident, to exchange and discuss information in relation to that incident and associated cyber threats, risks and vulnerabilities;
- At the request of a member of the CSIRTs network, to discuss and, where possible, implement a coordinated response to an incident that has been identified within the jurisdiction of that Member State;
- To provide Member States with assistance in addressing cross-border incidents pursuant to this Directive;
- To cooperate, exchange best practices and provide assistance to the CSIRTs designated as coordinators with regard to the management of the coordinated disclosure of vulnerabilities which could have a significant impact on entities in more than one Member State;
- To discuss and identify further forms of operational cooperation, including in relation to:
  - Categories of cyber threats and incidents;
  - Early warnings;
  - Mutual assistance;
  - Principles and arrangements for coordination in response to cross-border risks and incidents;
  - Contribution to the national large-scale cybersecurity incident and crisis response plan at the request of a Member State;
- To cooperate and exchange information with regional and Union-level Security Operations Centres (SOCs) to improve common situational awareness on incidents and cyber threats across the Union

n. NIS-2 also requires establishment of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe). EU-CyCLONe is to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

   EU-CyCLONe is to be composed of the representatives of Member States' cyber crisis management authorities as well as, in certain cases, the Commission. EU-CyCLONe is to have the following tasks:

   - To increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
   - To develop a shared situational awareness for large-scale cybersecurity incidents and crises;
   - To assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;
   - To coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;
   - To discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans

o. The Union may, where appropriate, conclude international agreements with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements are to comply with Union data protection law

p. NIS-2 allows for voluntary Peer Review. Peer reviews are to be carried out by cybersecurity experts. The cybersecurity experts are to be designated by at least two Member States that are different from the Member State being reviewed. The Peer Reviews are to cover at least one of the following areas:

- The level of implementation of the cybersecurity risk-management measures and reporting obligations laid down in this Directive
- The level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the tasks of the competent authorities;
- The operational capabilities of the CSIRTs;
- The level of implementation of mutual assistance;
- The level of implementation of the cybersecurity information-sharing arrangements;
- Specific issues of cross-border or cross-sector nature

Al thought that the second bullet was probably the most important one.

There were several Peer Review requirements shown on Slide 29, The ones AL thought were the most important were:

- Prior to the commencement of the peer review, Member States may carry out a self-assessment of the reviewed aspects and provide that self-assessment to the designated cybersecurity experts
- Peer reviews are to entail physical or virtual on-site visits and off-site exchanges of information. The Member State subject to the peer review are to provide the designated cybersecurity experts with the information necessary for the assessment, without prejudice to Union or national law concerning the protection of confidential or classified information and to the safeguarding of essential State functions, such as national security
- The cybersecurity experts participating in the peer review are to not disclose any sensitive or confidential information obtained in the course of that peer review to any third parties
- Cybersecurity experts participating in peer reviews are to draft reports on the findings and conclusions of the peer reviews. Member States subject to a peer review may provide comments on the draft reports concerning them and such comments are to be attached to the reports. The reports are to include recommendations to enable improvement on the aspects covered by the peer review. The reports are to be submitted to the Cooperation Group and the CSIRTs network where relevant. A Member State subject to the peer review may decide to make its report, or a redacted version of it, publicly available

q. The EU likes to place a lot of emphasis on measurements, so NIS 2 does have a chapter on Cybersecurity Risk-Management Measures. The basic requirement is that “Member States are to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services”.

Measures are to include key items such as:

- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

r. NIS 2 does briefly mention Certification Schemes. The important statement (it isn’t stated as a requirement) is that “Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes". Further, the Commission can specify Directive by specifying which categories of essential and important entities are to be required to use certain certified ICT products, ICT services and ICT processes or obtain a certificate under a European cybersecurity certification scheme. That is very similar to Common Criteria, although in Common Criteria rather than being centralized it is up to each Nation to determine what products require a certificate.

Finally, where no appropriate European cybersecurity certification scheme for the purposes of this Directive is available, the Commission may request ENISA to prepare a candidate scheme; this is not something that is currently in the Common Criteria.

s. NIS 2 also has provisions for Cybersecurity Information-Sharing Arrangements. Member States are to facilitate the establishment of cybersecurity information-sharing arrangements. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. Member States are to ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect

t. Member States are to ensure that notifications can be submitted to the CSIRTs or, where applicable, the competent authorities, on a voluntary basis, by:
   - Essential and important entities with regard to incidents, cyber threats and near misses;
   - Entities other than those referred to above, regardless of whether they fall within the scope of this Directive, with regard to significant incidents, cyber threats and near misses

u. Slides 37-39 provide the contents of Annex I and Annex II. This turned out to be the liveliest part of the presentation, as Al pointed out that the entities that the EU considered to be critical were different form the entities that, for example, US NIST considered critical. The tables below capture the Sectors of High Criticality in Annex I and the Other Critical Sectors from Annex II.

HIGH CRITICALITY SECTORS

Sector	Subsector
Energy	Electricity
	District Heating and Cooling
	Oil
	Gas
	Hydrogen
Transport	Air
	Rail
	Water
	Road
Banking	
Financial Markets	
Health	
Drinking Water	

HIGH CRITICALITY SECTORS

Sector	Subsector
Energy	Electricity
	District Heating and Cooling
	Oil
	Gas
	Hydrogen
Transport	Air
	Rail
	Water
	Road
Banking	
Financial Markets	
Health	
Drinking Water	

OTHER CRITICAL SECTORS

Sector	Subsector
Postal and Courier Services	
Waste Management	
Manufacture, production and distribution of chemicals	
Production, processing and distribution of food	
Manufacturing	(a) Manufacture of medical devices and *in vitro* diagnostic medical devices
	(b) Manufacture of computer, electronic and optical products
	(c) Manufacture of electrical equipment
	(d) Manufacture of machinery and equipment n.e.c.
	(e) Manufacture of motor vehicles, trailers and semi-trailers
	(f) Manufacture of other transport equipment
Digital Providers	
Research	

What stood out to Al was that the EU considered sectors such as ‘Drinking Water’, ‘Waste Management’’ and ‘Postal Services’ high criticality sector and sectors like ‘Food Production’ a critical sector. The US has a different view of what is a critical sector. Al was asked what the US list would be; he didn’t know what it was but he agreed for the next HIT meeting to bring a slide showing what the US list was (per NIST) and compare it to the list in NIS 2 at the next IDS WG Meeting.

5. **Actions:** None

Next Steps

The next IDS WG Meeting will be October 19, 2023 at 3:00P ET / 12:00N PT. Main topics will be a review of the new Security page on the PWG web site and Al’s comparson of the EU NIS 2 and the US NIST critical entities.