**DRAFTING COMMITTEE MEETING**

**Microsoft Teams**

**4th October from 14:00 to 17:00**

**Minutes**

* Meeting was opened by the Chairperson
* Votes were taken regarding participation of additional NEMO Committee member to the Drafting Committee. The majority vote has been achieved and the participation has been approved.
* A vote was taken regarding participation of the full Development Team at a Workshop with the Drafting Committee. The vote was unanimous, and the Development Team has been invited to the 11th October Workshop.
* The meeting was followed by Tour de Table where the new members from SmartEN and T&D introduced themselves
* The agenda was approved without any objections
* A recap on the progress was presented.
* Logistics were arranged for review of the draft by the Drafting Committee in parallel with legal review, in advance of the public consultation.
* Chairperson informed about CEER’s decision not to participate in the Drafting Committee. A request for an ACER NRA observer will need to be confirmed by the Drafting Committee vote.
* The Terms of Reference of the Drafting Committee was voted upon and unanimously approved.
* General Chapter sub-group reminded the overall scope of the Network Code on Cybersecurity, the legislative context, and the drafting principles. The requirements included were presented and the methodology approach of Network Codes was described where more specific details are defined during the implementation phase.
* The process of elaboration, adoption, and consultation (as was followed for CACL/FCA/EBGL/SOGL legislation) was discussed to help understand the intended process for this Network Code.
* Content of the general chapter was explained especially definitions, protection of sensitive data, scope, and implementation monitoring.
* General Chapter sub-group presented the topics of applicability and scope, responsibilities and governance, and described the challenge of not duplicating existing requirements already in place at member state level. The questions of implementation timelines was raised, for specific requirements in the network code.
* Sharing of Technical Information sub-group introduced its group members and its scope and presented an update of their progress.
* Sharing of Technical Information sub-group presented topics on:
* Mandatory SOC for critical risk entities.
* Defining what is a reportable cybersecurity incident
* Requirements for appointed CSIRT for info collection, anonymisation, and dissemination
* Definition of cross border electricity crisis as an incident
* Difference between cyber-attack and non cyber operational incidents
* Process cycle for cyber security exercises
* Mandatory exercises for high-risk entities – a question of what was intended in the Framework Guidelines.
* National CSIRTs and their operations are not operating 24/7. Timeframes need to take this into account when requirements are set.
* Existing cybersecurity excercises in place across Europe were discussed and the interaction with Network Code requirements and timelines was clarified. Network Code on Cybersecurity exercises could be interlinked time wise with existing processes.
* Cooperation with CSIRT experts was discussed and the Drafting Committee will be informed on the outcome of this cooperation.
* Supply Chain Security, Certification and Cross Border Cyber Risk Management and Functional Security Requirements sub-groups held a common presentation. They presented the concept of a combined top down and bottom-up risk assessment approach proposal including timelines and division of deliverables.
* The dynamic nature of the implementation work, regarding scope and challenging timelines, was discussed.
* The interaction with NIS Directive was discussed, emphasising that critical supply chain requirements for the energy sector should be cross referenced with NIS Directive requirements.
* Sub-groups presented the categories of entities and associated requirements, and how the concept of cybersecurity perimeters described in the Framework Guidelines was elaborated in the Network Code draft.
* The mandatory nature of minimum and advanced controls and the derrogation process was discussed.
* Sub-groups presented the supply chain security mandatory aspects for procurement processes for entities to ensure cybersecurity of products supplied.
* Vice-chairperson thanked Supply Chain sub-group leader for his good work, particularly regarding the visual aids that help to understand the content presented.
* It was confirmed that a graphic and visual material to portray transitional period will be included in the supporting document.
* ENTSO-E Secretariat provided guidance about next steps regarding distribution and review of the draft text to the Drafting Committee.
* It was advised that the Drafting Committee and one-to-one meetings are the best way at this stage to incorporate and discuss comments, rather than adding additional members to the development team subgroups.
* Drafting Committee Chairperson and Vice-Chairperson closed the meeting.

|  |  |  |
| --- | --- | --- |
| Entity/Stakeholder | Representative | Alternate |
| ACER | Manuel Sánchez Jiménez | Oyvind Arntzen Tofteegaard, Maria Barroso Gomes |
| EC | Michaela Kollau | Felipe Castro Barrigon |
| ENISA | Konstantinos Moulinos | Edgars Taurins |
| ENTSO-E | Francesco Morelli | Julien Keller |
| EU DSO Entity | Christiane Gabbe | Bart Luijkx |
| NIS Cooperation Group, Work Stream 8 | Vinzenz Heussler | Arno Spiegel |
| NEMO Committee | Hilde Rosenblad | Martina Gabriel, Katerina Novotna, Antoine Donne |
| RCCs | Andrew Lorriman |  |
| SmartEN | Mario Jardim | Nicolas Roger-Machart |
| T&D Europe | Volker Distelrath | Pascal Sitbon |

Drafting Committee constituency