

CONCORDIA LSG

The Liaisons Stakeholder

Introduction

Cybersecurity does not offer the luxury to be just a localized national interest concern. The inter-linked digital world necessitates a community solution. In this context, CONCORDIA¹ is developing an EU-wide Cybersecurity community and matching ecosystem to exchange and collate EU competences to become a potent coordinated force to address current and upcoming cyber threats at the EU level.

For this, a (draft) regulationⁱ is proposed to strengthen the (development, build-up and deployment of) competitiveness and capacities in cybersecurity at EU and national level, and support research to facilitate and accelerate standardisation and certification processes, this all while reducing digital dependence.

In lieu of the above, a key objective for CONCORDIA is to inclusively and comprehensively engage diverse competencies/stakeholders to result in a high-impact EU-wide Cybersecurity ecosystem. Recognizing that different stakeholders (national or institutional) represent different levels of competencies and with associated differing levels of engagement, CONCORDIA has established dedicated processes to engage the initial set (to be expanded as needed) of stakeholders to the consortium as:

- A. The National Cybersecurity Coordination Centres Stakeholder Group (NSG);
- B. The Liaison Stakeholder Group (LSG), and;
- C. The Observer Stakeholder Group (OSG).

The Purpose of LSG

The purpose of LSG is to engage European institutions such as for instance potentially the European Union Agency for Cybersecurity (ENISA), the European Defence Agency (EDA), the Europol or European Central Bank (ECB), World Economic Forum (WEF) and the Munich Security Conference (MSC) and others for coordinated coverage across such European agencies. These institutions are involved in cybersecurity issues from different perspectives of policy, governance and financial oversight among others.

The main mission of the LSG is support the development of the proposed network (including both the National Cybersecurity Coordination Centres ('NCCCs') and Cybersecurity Competence Community) including without limitation interconnecting existing, developing or to be developed ecosystem in and across the member states with the other stakeholders of this evolving network. The LSG will focus on the Cybersecurity Competence Community.

Based on the (draft) Regulation, and recognizing that cybersecurity is a broad dimension where various domains and stakeholders – also within the various sectors' perspectives in each member state and the European Union – should be identified in order to enable

¹ <https://www.concordia-h2020.eu/>



and facilitate each member state to work on, build and foster cybersecurity capabilities, competences and sources, in consultation with the Commission we have made the distinction between four (4) main domains:

- A. Sovereignty, CERT & NIS;
- B. Economic Development & Competition;
- C. Research & Innovation, and;
- D. Education & Skills.

The LSG is envisioned to have three main task, based on the main mission to help build a platform for trustworthy exchange of ideas, approaches, topics of joint actions and collaborations:

1. Build and maintain a trusted zone of dialogue and collaboration, including without limitation sharing, develop and sustain good practices and other information regarding the various objectives of the Cybersecurity Competence Community, the network, the proposed Regulation, and the public Cybersecurity Atlas, including without limitation mapping common state of play and state of the art and addressing relevant gaps;
2. Discuss how to coordinate, operationalize and sustain the various domains set forth above within scope of the proposed Regulation, including addressing both the numerous engagements as well as preconditions, also with the aim to add to the actual functioning of the Cybersecurity Competence Community of which the respective liaisons may or will become part of;
3. Cooperate in the field of cybersecurity innovation, research, economic and societal implications encouraging cross-borders and other collaboratives programs, projects and event-driven developments.

Participation

The LSG is an invite-only Stakeholder Group. CONCORDIA, also under the suggestions of the EC and our NSG members, will invite organisations to join the LSG and where relevant a specific domain.

During the membership process we would request you to sign the form attached to this document to become officially part of the LSG.

We envision the stakeholder groups to primarily communicate via electronic means. The periodic meeting (as agreed by the stakeholder members with a maximum of twice a year) will be coordinated by CONCORDIA with an invitation to attend the yearly physical meeting organized by CONCORDIA for all the stakeholder groups. Only public information will be made available. We are looking forward to engage.

ⁱ [https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328\(COD\)&I=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&I=en). EUR-Lex status quo: https://eur-lex.europa.eu/procedure/EN/2018_328. Proposal 2018/0328 (COD): https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf. Commission Staff Working Paper to 2018/0328 (COD): <https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-403-F1-EN-MAIN-PART-1.PDF>

