NCC ROLE IN THE EU CYBERSECURITY POLICY AND LINKS WITH ECCC

KATARZYNA PRUSAK – GÓRNIAK, VICE-CHAIR OF THE ECCC GOVERNING BOARD

THE CENTRE (ECCC)

- REGULATION (EU) 2021/887 of 20 May 2021 - the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs)
- ECCC - strategic tasks – a vision for the EU investment in cybersecurity to boost cybersecurity sector in the EU
- ECCC - implementation tasks – mainly the cybersecurity component of the DEP; in cooperation with EDIH support 'Advanced Digital Skills'
- NCCs and the Network of NCCs
- The Cybersecurity Community

NCC

- One in every MS – list published by ECCC
- Public sector entity or an entity with a majority of public participation – could be EDIH
- Capacity to support ECCC and Network
- Possess or have access to research and technological expertise in cybersecurity
- Capacity to engage effectively and coordinate with industry, the public sector, the academic and research community and citizens, as well as with NIS authorities
- Need to align activities with EDIHs to reach synergies and avoid duplication of efforts.

TASKS OF NCC

- Points of contact for Community
- Provide expertise and actively contributing to ECCC strategic tasks
- Promote and facilitate participation in cross-border projects and in cybersecurity actions funded by EU
- Provide technical assistance to stakeholders/ support in the application phase for projects
- Seek for synergies with relevant activities at national, regional and local level
- Implement grants, including through financial support to third parties
- Contribute to promoting and disseminating cybersecurity educational programmes;
- Promote and disseminating the works of Network, Community and ECCC
- Assess requests to become part of Community

SUPPORT FOR SME

- Facilitate access to knowledge
- Tailor access to the results of research and development,
- Make SMEs sufficiently secure
- SMEs active in cybersecurity to be competitive and contribute to the Union’s leadership in the area of cybersecurity.

COMMUNITY

- Main stakeholders in cybersecurity technological, industrial, academic and research
- Industry, including SMEs, academic and research organisations, civil society associations, European Standardisation Organisations, public entities and other entities dealing with cybersecurity operational and technical matters
- European Digital Innovation Hubs to be involved
- Entities established within the MS having cybersecurity expertise with regard to at least one of the following domains:

  (a) academia, research or innovation;

  (b) industrial or product development;

  (c) training and education;

  (d) information security or incident response operations;

  (e) ethics;

  (f) formal and technical standardisation and specifications.
- Application through the NCC/ registration by ECCC

STRATEGIC AGENDA

- Adopted by the GB in March 2023
- Goals to achieve by investing in projects that will *"strengthen the EU leadership and strategic autonomy, support Union technological capacities and increase the global competitiveness of the Union's cybersecurity industry"*
- Three short-term impact statements (2023-2027).
    - By 2027, the ECCC and the Network will have funded European SMEs in developing and using strategic cybersecurity technologies, services and processes through a coordinated cascade funding mechanism via NCCs and national co-financing that lowers the application threshold for SMEs.
    - By 2027, the ECCC and the Network will have supported and grown the cybersecurity professional workforce in both quantity and quality through the standardisation and certification of cybersecurity skills and investments in education and training of cybersecurity professionals.
    - By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan.
- ECCC could support implementation of the CRA especially in relation to the SMEs

Thank you for attention