# 2019-2 CEF Telecom Call: Cybersecurity

Jean-Francois Junger, Deputy Head of Unit &
James Caffrey, Policy Officer, DG-CONNECT

Innovation and Networks Executive Agency

# Policy Framework

- **Sustainability of the Digital Single Market in terms of reliability and trustworthiness of networks and services**
- **Cybersecurity Package –Resilience, Deterrence and Defence: Building strong cybersecurity for the EU**
  - **Cyber Resilience**
  - **Communication –Making the Most of NIS (NIS Toolkit)**
  - **Recommendation on Large Scale Response to Cyber Security Incidents and Crises**
- **Security of Network and Information Systems (NIS) Directive (2016/1148)**
- **EU Cybersecurity Act (Regulation 2019/881) (Objective 5)**

# Cybersecurity Digital Service Infrastructure (DSI)

- The Cybersecurity DSI is underpinned by the Security of Network and Information Systems (NIS) Directive (2016/1148) and the EU Cybersecurity Act (Regulation 2019/881).

- Generic Services under this DSI will:
  - ✓ support MS cooperation and capabilities development of **CSIRTs, OES, SPOCs, and NCAs** in accordance with the NIS Directive
  - ✓ support **trans-European cooperation** for joint cybersecurity operations and mutual trust
  - ✓ support capacity building and cooperation with **cybersecurity certification**

# Overview of the call

- **General scope**: funding under this call is intended to facilitate improved capabilities on cybersecurity in the Member States, as well as cooperation
- **Financial Support Instrument**: Grants
- **Budget**: €10 million

  Note: Out of the total budget of €10 million, it is expected to allocate €3 million under Objective 2 and allocate €1 million under Objective 5
- **Co-funding rate**: Up to 75% of the eligible costs of the action
- **Pre-financing:**50% within 30 days after signed grant agreement, balance on completion
- **Indicative duration of the actions**: 36 months

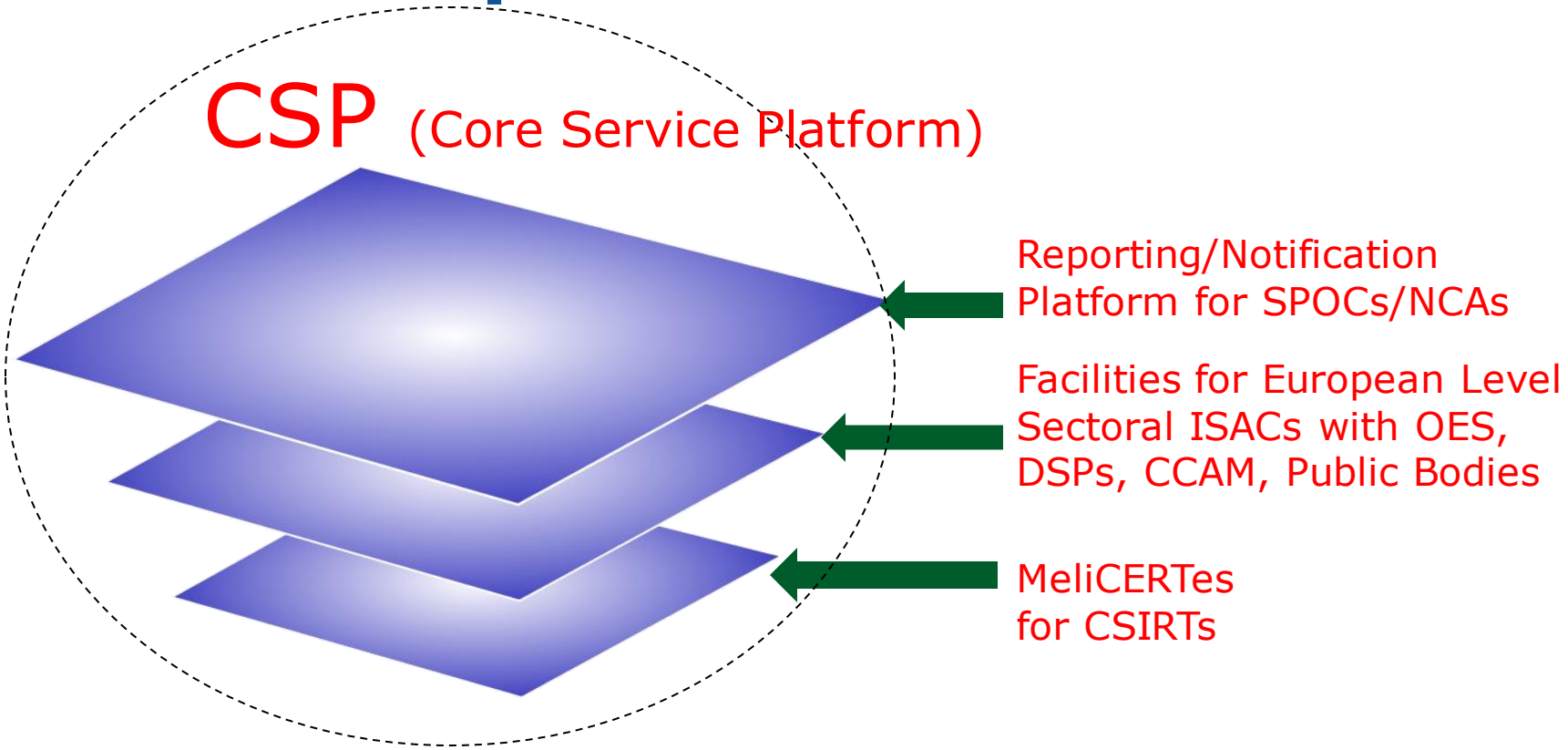
# Objectives and eligibility

| Call Objective | Title | Eligibility |
|---|---|---|
| 1 | Cooperation among designated **national CSIRTs** for the joint use of **MeliCERTes** | Consortium of at least **two national CSIRTs**, located in at least two different Member States. |
| 2 | Support for identified O**perators of Essential Services (OES)** for capability development and for the set-up of **Information Sharing and Analysis Centres (ISACs)** | Must include at least **one OES**. OES must provide a **letter of support** from relevant authority. |
| 3 | Support to **National Competent Authorities (NCAs)** and **Single Points of Contact (SPOCs)** to undertake the liaison, regulation and enforcement obligations set out in the NIS Directive | Must include at least **one NCAs or SPOCs** designated under Article 8 of the NIS Directive |
| 4 | **Trans-European cooperation** for effective joint cybersecurity operations and to build mutual trust/confidence | Consortium of at least **two national public bodies/institutions entrusted with national level cybersecurity**, located in at least two different Member States. |
| 5 | Support to a common level of maturity in **cybersecurity certification** | Must include at least one entity with primary responsibility for cybersecurity certification at the national level. It must provide a letter of support from relevant authority. |

# Expected Outcomes

| Call Objective | Title | Beneficiaries are expected to… |
|---|---|---|
| 1 | Cooperation among designated **national CSIRTs** for the joint use of **MeliCERTes** | Demonstrate the sustained use of the MeliCERTes facility at least throughout the duration of the Action |
| 2 | Support for identified O**perators of Essential Services (OES)** for capability development and for the set-up of **Information Sharing and Analysis Centres (ISACs)** | Join a relevant European Level Sectoral ISAC, or participate in events to establish a relevant European Level Sectoral ISAC organised by the ISAC facilities manager (set-up by the EC) and to have used the support services of that manager |
| 3 | Support to **National Competent Authorities (NCAs)** and **Single Points of Contact (SPOCs)** to undertake the liaison, regulation and enforcement obligations set out in the NIS Directive | Participate in activities and events organised by the cybersecurity co-operation facilitation manager for NCAs and SPOCs (set-up by the EC) and to use the support services of that manager |
| 4 | **Trans-European cooperation** for effective joint cybersecurity operations and to build mutual trust/confidence | Participate in activities and events organised by the cybersecurity co-operation facilitation manager for NCAs and SPOCs (set-up by the EC) and to use the support services of that manager |
| 5 | Support to a common level of maturity in **cybersecurity certification** | Contribute to activities and working groups of the European Cybersecurity Certification Group established in line with the EU Cybersecurity Act. |

# Cybersecurity
# CSP Co-operation Mechanisms



# Obj. 1: Cooperation among national CSIRTs for the joint use of MeliCERTes

- *Proposals **must** address both activities:*
  - **Activities to complement the functionality of the MeliCERTes facility to enhance swift and effective cross-border cooperation between different national CSIRTs**
  - **Trust-building activities to enhance cross-border cooperation**
- *If a national CSIRT has not received funding, they may also address:*
  - **Activities for improving its cyber capabilities**

# Obj. 2: Support for OES for capability development and for the set-up of ISACs

- *Proposals **must** address one or both activities:*
  - **Improving internal capabilities to meet security and reporting requirements under national and EU legislation**
  - **Setting-up a national or European level ISAC**
- *Note:*
  - Applications from OES providing essential services in more than one MS are particularly encouraged
  - €3 million allocated to this Objective

# Obj. 3: Support to NCAs and SPOCs to undertake NIS obligations

- *Proposals must address:*
  - **activities to build up in-house capabilities to undertake effectively the liaison, regulation, and enforcement obligations set out in the NIS Directive**
- *In addition, they may also address:*
  - **facilitating reporting from OESs and DSPs to NCAs and SPOCs**
  - **structured interaction between NCAs and SPOCs and OESs and DSPs**

# Obj. 4: Trans-European cooperation for joint cybersecurity operations and mutual trust

- *Proposals could address, but might not be limited to, the type of activities outlined below:*
  - **Further development and implementation of the operational layer of the Blueprint on coordinated response to cyber incidents**
  - **Secure cybersecurity information exchange**
  - **Joint awareness raising initiatives for the public and industries**
  - **Joint cyber rapid response, hybrid threat monitoring, mutual assistance initiatives**

# Obj. 5: Support to a common level of maturity in cybersecurity certification

- *Proposals could address, but might not be limited to, the type of activities outlined below:*
  - **Building up internal capabilities**
  - **Increasing operational capabilities for certification**
  - **Exchange of best practices**

- *Note:*
  - €1 million allocated to this Objective

# Award criteria: Relevance

- **Alignment with the objectives and activities required for the deployment of the Cybersecurity Digital Service Infrastructure described in Chapter 3.8 of the work programme and priorities set in Section 2 of the call text**
  - ***How well does the proposal fit with the Objective you have chosen and its description in the call text?***

**TIP!** Did you check what is a MUST HAVE? Have you explained clearly how you are addressing it?

  - ***How does it help meet expected outputs and outcomes of the Objective you have chosen?***

**TIP!** Did you check what beneficiaries are expected to do? E.g. participation in specific activities

- **Alignment and synergies with relevant policies, strategies and activities at European and national level**
  - ***Does the proposal demonstrate awareness of and, as appropriate, support and alignment with for example the NIS Directive, the Cybersecurity Act, the Cybersecurity package from September 2017, other CEF and Horizon 2020 cybersecurity projects etc.?***

**TIP!** Are you name-dropping or are you actually explaining how the proposals fits into the European/National contexts?

# Award criteria: Quality & Efficiency

- **Maturity in terms of readiness of the action to be implemented and operational level of the proposed solution(s) at the end of the action *e.g. will the proposed solution be ready to be used at the end of the action?***

  **TIP!** Have you asked yourself:
  - *E.g. Is there sufficient detail on the architecture of what you want to implement?*
  - *E.g. Is it clear what will be developed from scratch and what is already available?*
  - *E.g. Is it clear what will be the OUTPUT of the Action?*

- **Coherence and effectiveness of the work plan**

  **TIP!** Have you asked yourself:
  - *E.g. Is there sufficient detail on project management, and risk management?*
  - *E.g. Are the tasks described in sufficient detail?*
  - *E.g. Is the allocation of tasks and resources appropriate? Are the costs justified?*

- **Quality and relevant experience of the participants**

  **TIP!** *Have you asked yourself:*
  - *E.g. Are CVs provided with the proposal including relevant experience, qualifications and industry/sector certifications? Is the consortium composition relevant and well-balanced?*
  - *E.g. Does the proposal has the support needed from the entities important for its implementation?*

- **Appropriate attention to security, privacy, inclusiveness and accessibility**
  - *E.g. How the proposal addresses operational security, protection of personal data*

# Award criteria: Impact & Sustainability

- **Quality of the approach to facilitate wider deployment and take-up**

  **TIP!** Have you asked yourself:

  - *E.g. Is there an adequate dissemination plan? Does it explain in practice what you will do*
  - *E.g. Are concrete actions to facilitate the take-up internally/for external stakeholders foreseen?*

- **Capability of long-term sustainability without EU funding**

  **TIP!** Have you asked yourself:

  - *E.g. Does the proposal foresee concrete measure to ensure long term knowledge transfer takes place (especially when subcontracting)?*
  - *E.g. are the actions mainstreamed and embedded in cyber security operations of your organisation? Are they resulting in a step change in maturity levels of your organisation*
  - *E.g. Does the proposal foresee a business model or a concrete plan to carry on without EU-funding after the end of the action?*

# Cyber Security Call: Other information

- **Call text and supporting information**
  - https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-cybersecurity
- **Background info online:**
  - **NIS Directive:** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
  - **EU Cybersecurity Act:** https://eur-lex.europa.eu/eli/reg/2019/881/oj
  - **NIS Directive Introduction:** https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
  - **Cybersecurity Package (Sept. 2017):** https://ec.europa.eu/digital-single-market/en/cyber-security

# More information on the calls…

**inea-cef-telecom-calls@ec.europa.eu**

**inea@ec.europa.eu**

**https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cef-telecom-calls-proposals**

**@inea_eu**

**INEA**


Innovation and Networks Executive Agency