Proposal Evaluation Form

EUROPEAN COMMISSION

Digital Europe Programme (DIGITAL)

Evaluation Summary Report

Call:	DIGITAL-ECCC-2024-DEPLOY-NCC-06
Type of action:	DIGITAL-SIMPLE
Proposal number:	101226928
Proposal acronym:	NCCEE2
Duration (months):	48
Proposal title:	Cybersecurity Community Building and Continuation of the Estonian Coordination Centre Activities
Activity:	DIGITAL-ECCC-2024-DEPLOY-NCC-06-MS-COORDINATION

N.	Proposer name	Country	Total eligible costs	%	Grant Requested	%
1	RIIGI INFOSUSTEEMI AMET	EE	2,282,438.4	42.55%	1,141,219.2	42.55%
2	ETTEVOTLUSE JA INNOVATSIOONI SIHTASUTUS	EE	1,605,000	29.92%	802,500	29.92%
3	SIHTASUTUS TALLINNA TEADUSPARK TEHNOPOL	EE	1,476,600	27.53%	738,300	27.53%
	Total:		5,364,038.4		2,682,019.2	

Abstract:

NCCEE2 is the next step of NCCEE project, moving towards a more capable cybersecurity community, a more sustainable impact in building those capabilities in Estonia and contributing to development of the cybersecurity sector. Building on the success of the activities of the previous, deployment oriented NCCEE project, it is paramount to continue on the path of advancing capabilities across the cybersecurity sector in Estonia. Moving from individual projects to a culture of innovation and capacity building to keep Estonia and Europe safe, NCCEE2 has the following objectives:
1. Creating sustained impact in capacity building in cybersecurity industry, research and technology alongside the cybersecurity community through events, knowledge sharing, sustainable innovation programs and facilitation of collaboration;
2. Promoting and encouraging a culture of innovation in cybersecurity, including increasing practical implementation of research outcomes, facilitating the participation in cross-border projects and entrepreneurship;
3. Increasing the number of specialists and youth acquiring knowledge and training in the field of cybersecurity, with a special focus on women and girls, while taking into account the needs of the cybersecurity community;
4. Promoting and supporting the uptake and dissemination of state-of-the-art cybersecurity solutions by all actors in society, with special attention paid to small and medium sized enterprises.
NCCEE2 aims to enhance the existing capabilities of the Estonian and European cybersecurity community, guiding them towards market opportunities and future-proof solutions. The NCCEE2 consortium will leverage the experience from the NCCEE deployment project to expand the scope and focus on the long-term viability of the local National Coordination Centre, supporting the mission and strategic goals of the European Cybersecurity Competence Centre and Network of NCCs.

Evaluation Summary Report

Evaluation Result

Total score: 13.00 (Threshold: 10)

Criterion 1 - Relevance

Score: **4.50** (Threshold: 3 / 5.00 , Weight: -)

The following aspects have been taken into account (Items 3 and 4 may not be applicable to all topics see call document):
1 - Alignment with the objectives and activities as described in the Call document
2 - Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level
3 - Extent to which the project would reinforce and secure the digital technology supply chain in the EU
4 - Extent to which the project can overcome financial obstacles such as the lack of market finance

The proposal intends to build on the previous Estonian NCCEE project, to achieve a more capable and sustainable cybersecurity community via market opportunities and future-proof solutions.

Four well-defined and concrete objectives are presented, which are aligned with the objectives and activities described in the Call document. These highlight the need for research, development, innovation and entrepreneurship in cybersecurity to tackle emerging threats.

Data is provided on the growing number of cyber incidents in Estonia, describing the significant challenges (highlighted in Estonia's 2024-2030 Strategic Plan for Cybersecurity) within Estonia's cybersecurity landscape.

The proposal demonstrates alignment with national priorities, including clear links to Estonia's national cybersecurity strategy and the intention to establish connections with neighbouring NCCs, fostering cross-border collaboration.

The proposal adequately describes its contribution to the long-term policy objectives of the call's domain, by indicating the way that the Estonian National Coordination Centre is focused to continue and enhance the efforts related to the "Estonia 2035" initiative with NCCEE2, ensuring - among other things - that the cyber risks of the digital society are well managed and that the Estonian cyberspace is highly reliable.

However, the links to long-term EU policies, such as the NIS2 Directive and the EU Cybersecurity Strategy are not sufficiently elaborated.

In addition, some of the objectives are not accompanied by measurable target levels.

Recommendations:
- Provide a more elaborate and clear narrative about the proposal's links to long-term EU policies.
- Define appropriate KPIs for the project objectives, with realistic estimated target values and/or qualifications (for instance, whilst the proposal describes goals such as capacity building and SME support, it does not specify measurable targets in this regard), together with explicit links between the objectives and the WP structure.

Criterion 2 Implementation

Score: **4.00** (Threshold: 3 / 5.00 , Weight: -)

The following aspects have been taken into account:
1 - Maturity of the project
2 - Soundness of the implementation plan and efficient use of resources
3 - Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work

The project builds on the NCCEE pilot project, leveraging on the results of this earlier project (including existing systems, processes and team). It therefore demonstrates an adequate level of maturity.

The provided implementation plan is largely sound and detailed, including a comprehensive 48 month plan, composed of 5 pertinent WPs that include tasks for monitoring performance, cooperation, resource utilisation, and dissemination.

However, interdependencies between WPs are not sufficiently clear, particularly considering that WPs tasks have a duration of 48 months (refer to table in page 63 /64). Also, milestones are not consistently specified for all WPs.

The presented approach to FSTP is adequate, however the selection process for FSTP beneficiaries is not sufficiently defined and the distributed method for fund allocation should be presented with further detail.

The consortium demonstrates that it possesses the necessary skills and capacity to carry out the project. The partners have complementary skills in Cybersecurity policy, national digital infrastructure, cybersecurity training, grant management and innovation support as well as supporting startups, and innovation testing.

Recommendations:
- Revise the WPs task timeframe definition for achieving a more balanced and realistic time distribution.
- Revise the Milestones Definitions for the WPs.
- Provide a more detailed description of the FSTP selection and fund allocation processes.

Criterion 3 - Impact

Score: **4.50** (Threshold: 3 / 5.00 , Weight: -)

The following aspects have been taken into account (Item 3 may not be applicable to all topics see call document):
1 - Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, where relevant, the plans to disseminate and communicate project achievements
2 - Extent to which the project will strengthen competitiveness and bring important benefits for society
3 - Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects

The proposal demonstrates to be very well placed to achieve the expected impacts of the Call, contributing towards the advancement of Estonia's cybersecurity landscape and strengthen the EU's broader digital security ecosystem.

The proposal presents clear and concrete expected outcomes and deliverables, with credible explanations of how they will support the achievement of the expected impacts, as outlined in the Call document.

A good dissemination and communication plan is also provided, however a comprehensive set of related KPIs, with appropriate quantitative baselines and target values, is not clearly presented.

The key contribution to competitiveness is through the support provided to start-ups and SMEs to enhance their cybersecurity. The described benefits for society include promoting cybersecurity education and workforce development, with a focus on diversity and inclusion as well as building a secure and digitally aware public environment, enhancing trust in digital systems and services.

The proposal also outlines several impactful activities, such as FSTP distribution, community-building events, and a youth-focused cybersecurity programme.

Recommendation:
- For better monitoring of the project's impact, the proposal should include a list of the Dissemination and Communication KPIs with quantitative estimations of appropriate indicators.

Scope of the application

Status: **Yes**

Comments (in case the proposal is out of scope)

Not provided

Exceptional funding

Entities from countries mentioned in the work programme (if any) are only exceptionally eligible, if the granting authority considers their participation essential for the implementation of the action.
Please list the concerned applicants and requested grant amount and explain the reasons why.

Based on the information provided, the following participants should receive exceptional funding:

Not provided

Based on the information provided, the following participants should NOT receive exceptional funding:

Not provided

Artificial Intelligence

Status: **No**

If YES, the technical robustness of the proposed system must be evaluated under the appropriate criterion.

Are security restrictions as per Article 12(5) and (6) applicable?

Status: **Yes**

If security restrictions apply and one (or more) applicants are found controlled from third countries (or third country entities), is the project feasible without the controlled entities?

Yes

Can the work be taken over by one of the other participants or will it be necessary to add new ones?

Yes

Not provided

Overall comments

Not provided