NCC-DE
NATIONAL CYBERSECURITY COORDINATION CENTRE GERMANY

Group work: Sketching a proposal – where to get started?

Berlin, 02 September 2025

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT DEUTSCHLAND

Co-funded by the European Union
The project funded under Grant Agreement No. 101126787 is supported by the European Cybersecurity Competence Centre

Your application in 8 steps

How to create a proposal?

Step 1: **"Funding & Tenders Portal" ->** "Start submission"

Step 2: Early registration **"Electronic Submission Service"; apply for participant code (PIC) if necessary**

Step 3: Create a draft application

Step 4: Add a partner

Step 5: Fill in part A online

Step 6: Download part B of the application and edit in the consortium

Step 7: Upload part B as PDF

Step 8: **"Submit"** the proposal (part A + B and annexes)

Link: SEP Proposal Submission Guide

Application process & participation rules

Application Structure:

For Horizon and Digital
Part A
1. general information
2. participants
3. budget
4. other questions

For Horizon Europe
Part B
1. Excellence
2. Impact
3. Implementation
3.1 Work plan
4. Other

For Digital Europe
Part B
1. Relevance
2. Implementation
3. Impact
4. Work plan
5. Other
6. Declarations

What needs to be Adressed in the proposal?

For Horizon Europe
Work Programme 2025
6. Civil Security for Society

- The work programme contains the relevant details[1]
- Infos are available in the appendix starting on p. 90
- Details about the **expected impact** and **outcome** as well as about the **scope** of the deliverables

For Digital Europe
Digital Europe Cybersecurity Work Programme 2025-2027

- Call for Proposals in PDF format [2]
- Infos about the **objectives, the scope, the expected outcome** and **the deliverables are available per topic**
- Details about the administrative aspect are laid out in seperate chapters

1: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en
2: https://cybersecurity-centre.europa.eu/document/download/da2e1929-9320-4ae7-97e6-4c3e2ae7de3f_en

Dedicated action to reinforcing hospitals and healthcare providers

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe

1

This topic from the **Digital Europe** programme has a budget of **€ 30 million**, which is administrated by the **ECCC**. The project grant size ranges from € 3 to € 5 million.

2

Funding rate: 50%
Project runtime: 1,5 - 2 years
Opening date: 12th June 2025
Closing date: 7th October 2025
Project partners: from at least two EU member states
Eligibility: EU legal entities, otherwise restricted based on Article 12(5) of the DEP Regulation (2021/694). Particularly clusters of hospitals and healthcare providers.

Objectives

Strengthening the cybersecurity of hospitals and healthcare providers, particularly against ransomware, to enhance the resilience of the European healthcare system.

Scope

Deployment of pilot projects to analyse the state of preparedness, identification of cybersecurity needs, development of technical implementation plans, conduction of demo implementations as well as provision of education and training for clusters of hospitals and healthcare providers.

Activities

Implementation and testing of modern security solutions such as Security Operation Centres, SIEM platforms, automated incident response and staff training.

Expected Outcomes

Mapping of common cybersecurity needs, guidelines to assess cybersecurity state, technical plans to enhance preparedness and resilience, pilot cybersecurity demo installations in hospitals as well as wide dissemination campaigns.

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT DEUTSCHLAND

Do you have any questions? Get in touch at:
www.nkcs.bund.de/en/kontakt

Generative AI for Cybersecurity applications

HORIZON-CL3-2025-02-CS-ECCC-01

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Horizon Europe

1

The total funding volume for this topic from **Horizon Europe** 2025 is **€40 million** and is initiated by the ECCC. The planned project size is between €12 and €14 million.

2

Type of Action: Research and Innovation Actions
Funding rate: 100 %
Opening Date: 12 June 2025
Deadline: 12 November 2025
Targeted Stakeholders: Rechtsträger mit Sitz in EU-Mitgliedstaaten und assoziierten Ländern, die nicht direkt oder indirekt von Drittländern kontrolliert werden

Expected Results

Funded projects should make targeted use of generative AI for cybersecurity, for example for faster threat detection, automated responses and better compliance support. The solutions must meet EU legal, ethical and data protection requirements, increase the resilience of digital systems and be documented in a traceable manner. Significant progress beyond the state of the art and consideration of trustworthy AI principles are expected.

Scope

Projects are sought that develop new AI models for cybersecurity applications with large amounts of data – e.g. for threat detection, adaptive defence and authentication. The aim is to automate and improve monitoring, compliance and reporting in accordance with legal requirements (e.g. AI Act, NIS2). The solutions should be transferable and reusable across industries.

Your proposal idea (10 min + 25 min)

Brainstorming and discussion

- What could you work on in a project?
- What would move Europe forward?
- What is your organisation good at?

What needs to be Adressed in the proposal?

- How is my idea aligned with the objectives of the call
  - Make notes for Relevance (DEP) / Excellence (HEP)
- What is the output of your project, what kind of deliverables could be generated? How will you communicate / disseminate results?
  - Make notes for the Impact section
- How will you work on the project? What will the team be like and why is your consortium a good choice for the project? What are possible risks and what are the project management strategies?
  - Make notes for the implementation section
- How should work packages be structured? And how much resources need to be invested in which parts?
  - Make notes for the work plan

Wrap-up and Networking

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT DEUTSCHLAND

Contact us

HOME

General information and NCC-DE head office

FEDERAL OFFICE FOR INFORMATION SECURITY (BSI)

The NCC-team at the BSI is based within the Section T 21 "Technology- and Research Strategie".

Please feel free to contact us via:
ncc@bsi.bund.de

HEAD OF NCC-DE

Dr. Dörte Rappe

NCC-TEAM AT BSI

Christian Hartlage
Dr. Natalie Peter
Dr. Angelika Praus
Sarah Filippczyk
Julia Ringies
Beatrix Welter

DLR Projektträger

FOCUS RESEARCH

Stefan Hillesheim
0228 3821-2230
stefan.hillesheim@dlr.de

Dr. Alexander Khanin
0228 3821-2667
alexander.khanin@dlr.de

Dr. Marvin Richter
0228 3821-2147
marvin.richter@dlr.de

FOCUS START-UPS AND SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

Dr. Christian Fischer
0228 3821-1948
ch.fischer@dlr.de

Simon Etzold
0228 3821-2724
simon.etzold@dlr.de

Website

LinkedIn

Mastodon

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT DEUTSCHLAND