DECISION No GB/2023/9

of

The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre

Adopting the draft Estimate of the ECCC's Revenue and Expenditure and endorsing the Draft Single Programming Document 2025-2027

THE GOVERNING BOARD,

Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (hereinafter "the Regulation"),[1] and in particular Article 13(3)(b), (c), and Article 25(3) thereof;

Having regard to Recital (23) of the Regulation, according to which Commission Delegated Regulation (EU) 2019/715[2] applies to the ECCC;

Having regard to Commission Communication C(2020) 2297 final, on the strengthening of the governance of Union Bodies under Article 70 of the Financial Regulation 2018/1046 and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report dated on 20 April 2020;

Having regard to Article 32 of the ECCC Governing Board Decision No GB/2023/1 on the ECCC's Financial Rules;

HAS ADOPTED THE FOLLOWING DECISION:

Article 1
Provisional draft Estimate of the Agency's Revenue and Expenditure

The provisional draft Estimate of the ECCC's Revenue and Expenditure, as annexed to this decision, is hereby adopted.

[1] OJ L 202, 8.6.2021, p. 1-31
[2] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1)

Article 2

Draft Single Programming Document 2025-2027

The draft Single Programming Document 2025-2027 including the preliminary work programme 2025, as annexed to this decision, is hereby endorsed.

Article 3

The present decision shall enter into force on the day following that of its adoption. It will be published on the ECCC's website.

Done at Athens on 12 October 2023,

For the European Cybersecurity Industrial,
Technology and Research Competence
Centre

(e-signed)

Pascal Steichen
Chairperson of the Governing Board

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Draft Single Programming Document 2025-2027

Version: Approved by the Governing Board of the ECCC in Decision No GB/2023/9.

CONTACT

To contact the European Cybersecurity Competence Centre (ECCC) or for general enquiries, please use:
Email address: eccc@ec.europa.eu
https://cybersecurity-centre.europa.eu/index_en

LEGAL NOTICE

This publication presents the draft ECCC Single Programming Document (SPD) 2025-2027 as approved by the Governing Board of the ECCC in Decision No GB/2023/9. The Governing Board may amend the Single Programming Document 2025–2027 at any time. The ECCC has the right to alter, update or remove the publication or any of its contents.

This publication is intended for information purposes only. All references to it or its use as a whole or partially must refer to the ECCC as the source. Third-party sources are quoted as appropriate. The ECCC is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither the ECCC nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. The ECCC maintains its intellectual property rights in relation to this publication.

TABLE OF CONTENT

FOREWORD

The European Cybersecurity Competence Centre (ECCC) was established to enhance cybersecurity capabilities in the EU and to support better coordination amongst relevant stakeholders to achieve common goals of EU citizens, society and economy. 2025 will be the year when the setup stage of the ECCC will be complete. The ECCC will be on cruising speed, fully operational, coordinating calls under the Horizon Europe and Digital Europe programmes (HEP, DEP), and fostering cooperation of the Cybersecurity Competence Community (the Community).

The activities of the ECCC are part of a bigger picture at EU level. In recent years, the EU has continued developing its cybersecurity policy. This includes the adopted revision of the NIS Directive (NIS 2 Directive), the legislative proposal for a Cyber Resilience Act and for a Solidarity Act, the policy Communications on the Cyber Skills Academy and on cyber defence, as well as funding calls for proposals launched in 2022 and 2023 under the HEP and DEP, amongst other initiatives.

The ECCC, together with the National Coordination Centres (NCCs) are an important component of this coordinated effort to enhance cybersecurity capabilities and improve resilience in the EU. The ECCC Regulation, which entered into force in mid-2021, aims to improve cyber capabilities in the EU, inter alia, in terms of scientific and industrial assets, specialised competences and general cyber awareness, and to improve coordination amongst relevant stakeholders. This implies setting strategic objectives for investment, deployment, and use of cybersecurity products and services, pooling resources from the EU, notably from the DEP, Member States and other players.

The present document provides a draft multiannual planning 2025-2027 and draft work programme for 2025, which will be updated over the course of 2023 (a first draft should be adopted by the ECCC Governing Board (GB) by early 2024) and during 2024, until its final adoption by the ECCC GB before the end of 2024. The document is in line with the Strategic Agenda of the ECCC adopted by the ECCC GB in March 2023 and proposes actions to monitor its implementation. It follows the guidelines from the Commission Communication on the strengthening of the governance of Union Bodies, under Article 70 of the Financial Regulation 2018/1046, and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report.

In 2025 the ECCC shall function as an autonomous EU body, with an Executive Director formally appointed and with all staff recruited. By then, the ECCC will capitalise on the results of the hard work from previous years and the engagement of all those that contributed to the set-up of the ECCC, including ECCC staff, European Commission (EC) staff working on the ECCC, and many in the Cyber Competence Community. The vision from the ECCC regulation will increasingly materialise, showing the added value of the EU strategic investments and enhanced coordination on cybersecurity.

October 2023
Miguel González-Sancho, Interim Executive Director

LIST OF ACRONYMS

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
BOA	Back Office Arrangements
CA	Contract agent
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DEP	Digital Europe Programme
DPO	Data Protection Officer
EC	European Commission
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
ED	Executive Director
EFTA	European Free Trade Association
EIB	European Investment Bank
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUAN	EU Agencies Network
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
GB	Governing Board (of the ECCC)
HEP	Horizon Europe Programme
ICT	Information and communication technology
ISAC	Information Sharing and Analysis Centre
IT	Information technology
JCU	Joint Cyber Unit
JU	Joint Undertaking
MoU	Memorandum of understanding
MS	Member State(s)
NCCs	National Coordination Centres
NIS	Networks and information systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
SAG	Strategic Advisory Group
SC	Secretary
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SOP	Standard Operating Procedure
SPD	Single Programming Document
TA	Temporary agent
TESTA	Trans European Services for Telematics between Administrations
TFEU	Treaty on the Functioning of the European Union

MISSION STATEMENT

The European Cybersecurity Competence Centre (ECCC)[1] is a European Union (EU) body established by Regulation (EU) 2021/887[2] of the European Parliament and of the Council ("the Regulation"), which entered into force on 28 June 2021.

The Regulation provides the ECCC with the mandate to support industrial technologies, research and innovation in the domain of cybersecurity, collaborating with the Network of National Coordination Centres (NCCs) and stakeholders from the Cybersecurity Competence Community (the Community). The ECCC manages EU financial resources dedicated to cybersecurity under the Digital Europe Program (DEP)[3] and the Horizon Europe Program (HEP)[4], and other EU programmes where appropriate, as well as additional contributions from Member States, to implement projects and initiatives on cybersecurity research, technology and industrial development. The ECCC has adopted an Agenda[5] for cybersecurity development and deployment, which pays particular attention to small and medium-sized enterprises (SMEs). The ECCC and the Network of NCCs contribute to Europe's technological sovereignty and open strategic autonomy through joint investment in strategic cybersecurity projects. More concretely, according to Article 3 of the Regulation, the ECCC and the Network of NCCs have the mission to help the EU to:

- Strengthen its leadership and strategic autonomy in the area of cybersecurity by developing the EU's research, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data in the Digital Single Market;
- Support the EU technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software; and
- Increase the global competitiveness of the EU's cybersecurity industry, ensure high cybersecurity standards throughout the EU and turn cybersecurity into a competitive advantage for other EU industries.

According to Article 4 the Regulation, the ECCC shall have the overall objective of promoting research, innovation and deployment in the area of cybersecurity. Beyond its overall objective, the ECCC has the following specific objectives:

- Enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society;

[1] https://cybersecurity-centre.europa.eu/index_en.
[2] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).
[3] Digital Europe Programme established by Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).
[4] Horizon Europe Programme established by Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).
[5] Such Agenda is foreseen by the ECCC regulation. The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

- Promoting cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services, in a manner that complements the efforts of other public and private entities; and
- Contributing to a strong European cybersecurity ecosystem bringing together all relevant stakeholders.

With a view to achieving those objectives, the ECCC shall:

- Establish strategic recommendations for research, innovation and deployment in cybersecurity, in accordance with EU legislation and policy orientations, and set out strategic priorities for the ECCC's activities;
- Implement actions under relevant EU funding programmes, in accordance with the relevant work programmes and the EU legislative acts establishing those funding programmes;
- Foster cooperation and coordination among the NCCs and with and within the Community; and
- Where relevant and appropriate, acquire and operate the Information and Communication Technologies (ICT) infrastructure and services required to fulfil its tasks.

With regards to the ECCC's tasks, according to Article 5 of the Regulation:

- The ECCC supported by the Network will make strategic investment decisions and pool resources from the EU, its Member States (MS) and, indirectly, other cyber constituencies, to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy.
- The ECCC will play a key role in delivering on the ambitious cybersecurity objectives of the DEP and HEP.
- The ECCC together with the Network will support the deployment of innovative cybersecurity solutions in the Community and beyond.
- It will also facilitate collaboration and coordination and the sharing of expertise between relevant stakeholders from the Cyber Community, in particular research and industrial communities, as well as NCCs.

SECTION I. GENERAL CONTEXT

The "*EU's Cybersecurity Strategy for the Digital Decade*"[6] outlines the EU vision and plan for cybersecurity. Building upon previous achievements, the strategy contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action:

- "Resilience, technological sovereignty and leadership", aiming to protect EU people, businesses and institutions from cyber incidents and threats;
- "Building operational capacity to prevent, deter and respond", aiming to enhance the trust of individuals and organisations in the EU's ability to promote secure and reliable network and information systems, infrastructure and connectivity; and
- "Advancing a global and open cyberspace through increased cooperation", aiming to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

As stated in the Council conclusions on the Joint Communication to the European Parliament and the Council entitled "*The EU's Cybersecurity Strategy for the Digital Decade*"[7], achieving strategic autonomy while preserving an open economy is a key objective of the EU in order to self-determine its own economic path and interests. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity with the aim to strengthen the EU's digital leadership and strategic capacities. Furthermore, it can also include diversifying production and supply chains, fostering and attracting investments and production in Europe, exploring alternative solutions and circular models, and promoting broad industrial cooperation across MS. The conclusions also acknowledge the importance of continued support for technical assistance and cooperation between MS for capacity-building purposes.

As highlighted in the Nevers Call[8], Russia's invasion of Ukraine and its repercussions in the cyber-space has reinforced the case for strengthening cooperation in cyber crisis management at EU level. The Cyber Posture Council Conclusions[9] notably call on the EC, the High Representative of the Union for Foreign Affairs and Security Policy, and MS to develop risk assessment and scenarios for an attack on a MS or partner country, which take into account relevant input and perspectives from all of the cyber communities, including civil, diplomatic and defence.

Such an initiative echoes the EU's ambition for a common situational awareness and coordinated preparation and response to threats. A key priority area on which efforts are focusing is the development of shared situational awareness. This includes stronger inter-agency cooperation among ENISA, CERT-EU and Europol in assessing the threat landscape while working closely with the EU MS and networks (i.e. EU CyCLONe, CSIRT network). Moreover, the political agreement on the NIS Directive 2[10] provides a legal basis for the CyCLONe network of MS cyber

[6] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.
[7] Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade (6722/21).
[8] 'Nevers Call to Reinforce the EU's Cybersecurity Capabilities'. Informal Meeting of the Telecommunications Ministers. Nevers, March 9, 2022.
[9] https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/
[10] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

agencies plus, in case of risks for the internal market, the EC to participate in crisis management coordination and situational awareness.

The establishment of the ECCC is taking place in a dynamic cybersecurity political context, including several initiatives at EU level:

- **Revision of the NIS Directive (NIS2).** To respond to the increased exposure of Europe to cyber threats, the EC proposed, in December 2020, a revision of the NIS Directive (NIS 2 Directive), for which the co-legislators reached a political agreement in May 2022. The new Directive raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.
- **Cybersecurity Resilience Act (CRA).** In September 2022, the EC adopted the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA)[11]. The CRA establishes a uniform legal framework for essential requirements for placing products with digital elements on the market. The CRA aims to ensure that hardware and software products are placed on the EU market with fewer vulnerabilities and that manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions that allow users to take cybersecurity into account when selecting and using products with digital elements.
- **Cybersecurity – uniform rules for EU institutions, bodies and agencies.** The EC presented a proposal to enhance the cybersecurity and information security of the EU institutions, bodies and agencies, on which the EU legislators reached political agreement in June 2023.
- **European Cybersecurity certification schemes**. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act[12] aims at creating market-driven European cybersecurity certification schemes and increasing "cybersecurity-by-design" in ICT products, services, and processes. The first European Cybersecurity Certification scheme was the Common Criteria-based European cybersecurity certification scheme (EUCC), and two other schemes are currently being prepared, based on preparatory work coordinated by ENISA: the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the European 5G Certification Scheme (EU5G). In support of certification, the EU Standardisation Strategy and the current EU funding framework both include essential topics such as the development of harmonised evaluation methodologies or innovations to the performance of testing ICT products, services and processes.
- **EU 5G Toolbox.** The EU 5G Toolbox[13] is a comprehensive and objective risk-based approach for the security of 5G and future generations of networks. While work is still ongoing in some MS, a vast majority of MS have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox, including putting in place frameworks for imposing appropriate restrictions on 5G suppliers considered to be high-risk. In addition, MS, with the support of the EC and ENISA, assessed and adopted a report on the cybersecurity of Open Radio Access Networks ('Open RAN')[14], which will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces.

[11] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.
[12] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).
[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Secure 5G deployment in the EU - Implementing the EU toolbox, COM(2020) 50 final.
[14] NIS Cooperation Group, Report on the cybersecurity of Open RAN, 11 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

Moreover, in June 2023 the NIS Cooperation Group also adopted a report on the status of implementation of the EU 5G Toolbox, and the EC adopted a Communication on this topic at the same time.[15]

- **EU funding in the 2021-2027 Multiannual Financial Framework.** In 2022 and 2023 funding was provided for projects on cybersecurity deployment under the DEP, and for cybersecurity research under the HEP, while further funding is foreseen under both EU programs. The respective work programmes 2023-2024, including support for cybersecurity, were adopted in 2023.
- **EU Cyber Solidarity Act.** In 2023 the EC adopted a legislative proposal on an EU Cyber Solidarity Act, including legislative changes to DEP, designed to: (1) strengthen common EU detection, situational awareness and response capabilities; (2) gradually build an EU-level cyber reserve with services from trusted private providers; (3) support testing of critical entities for potential vulnerabilities based on EU risk assessments (enabling ENISA, in close coordination with MS to draw lessons learned from cyber crisis and large scale incidents) . The solidarity mechanism will complement ECCC actions to provide long-term solutions to strengthen EU cyber security.
- **EU Cyber Skills Academy.** In 2023 the EC adopted a non-legislative initiative outlining policy and support measures to promote cyber skills.

Within this broad framework of EU cybersecurity policy priorities, the ECCC will pool resources from the EU, MS and other constituencies to improve and strengthen technological and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy, and offering a possibility to consolidate part of the cybersecurity-related activities funded under HEP and DEP. For instance, the ECCC will support the development of capabilities for early threat detection and sharing of cyber threat intelligence (CTI), reinforcing and linking the capabilities of Security Operation Centres (SOCs) and other relevant entities in the EU relaying on dedicated DEP projects. The ECCC will contribute to further support synergies with actions funded under the Recovery and Resilience Facility and the European Structural and Investment Funds, whose implementation to a large extent lies in the hands of MS and regional authorities.

The ECCC and the Network of NCCs and the Community will contribute to maximising the effects of investments to strengthen the EU's leadership and open strategic autonomy in the field of cybersecurity and support technological capacities, capabilities and skills, and to increase the EU's global competitiveness. They will do so with input from industry and academic communities in cybersecurity, including SMEs and research centres, through a more systematic, inclusive and strategic collaboration.

Furthermore, the ECCC shall cooperate with relevant EU institutions, bodies, offices and agencies, in particular with ENISA, in order to ensure consistency and complementarity while avoiding any duplication of effort.

[15] Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity | Shaping Europe's digital future (europa.eu)

SECTION II. MULTI-ANNUAL PROGRAMMING 2025 – 2027

The ECCC, in consultation with its GB, developed a multi-annual programming covering three years. Compared to the initial years of operation of the ECCC, this multiannual programming introduces a shift in focus given the maturity level reached by the ECCC. During the first years, following the establishment of ECCC, one of the main objectives was to make the ECCC operational, develop its financial and operational autonomy, and gradually deliver all it's the core tasks. For 2025 and the following years, the focus shifts to the core ECCC tasks: the implementation of programmes and fostering communities.

Article 4(3) of ECCC regulation presents the way ECCC should implements its specific operational objectives, by:

> *(a) establishing strategic recommendations for research, innovation and deployment in cybersecurity in accordance with Union law and setting out strategic priorities for the Competence Centre's activities;*
>
> *(b) implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes;*
>
> *(c) fostering cooperation and coordination among the national coordination centres and with and within the Community; and*
>
> *(d) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary […].*

This multiannual work programme of the ECCC is aligned with Article 4(3), comprising two operational activities: Activity 1, corresponding to paragraphs (b) and (d), and Activity 2, corresponding to paragraph (a) and (c) of Article 4(3) of the ECCC Regulation. One more horizontal/cross cutting activity: Activity 3, to support the functioning of the ECCC and its staff. As such the following activities are presented in this document:

- ***Activity 1 – Deployment of resources for cybersecurity***, dedicated to implementing actions under relevant Union funding programmes; and where relevant acquiring and operating ICT infrastructure and services to fulfil the tasks set out in Article 5 of the ECCC regulation.
- ***Activity 2 – Strategic advice, cooperation and coordination for cybersecurity***, dedicated to the NCCs and the Community, and also establishing strategic recommendations for research, innovation and deployment in cybersecurity, as well as priorities for the ECCC's activities.
- ***Activity 3 – Governance, establishment and compliance of the ECCC***, dedicated to the operation of the ECCC, its financial and human resources, IT and infrastructures, legal and compliance related activities.

The proposed activities are in line with the activities in previous SPDs, with some differences: new Activity 1 corresponds to Activity 2 in previous SPDs; new Activity 2 corresponds to Activities 3 and 4 in previous SPDs; Activity 3 corresponds to Activity 1 in previous SPDs.

The next table lists the ECCC responsibilities under its founding Regulation and their correspondence to the referred 3 activities.

ECCC tasks and responsibilities	Activity 1	Activity 2	Activity 3
Article 5 - Tasks of the Competence Centre			
1.(a) strategic tasks (as detailed in paragraph 2 and listed below), consist of			
2.(a) developing and monitoring the implementation of the Agenda		√	√
2.(b) through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and the Digital Europe Programme		√	
2.(c) ensuring synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities with those Union institutions, bodies, offices and agencies		√	
2.(d) coordinating national coordination centres through the Network and ensuring a regular exchange of expertise		√	
2.(e) providing expert cybersecurity industrial, technology and research advice to Member States at their request, including with regard to the procurement and deployment of technologies		√	
2.(f) facilitating collaboration and the sharing of expertise among all relevant stakeholders, in particular members of the Community		√	
2.(g) attending Union, national and international conferences, fairs and forums related to the mission, objectives and tasks of the Competence Centre with the aim of sharing views and exchanging relevant best practices with other participants		√	
2.(h) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products, services and processes, while seeking to avoid the fragmentation and duplication of efforts and replicating good cybersecurity practices and cybersecurity products, services and processes, in particular those developed by SMEs and those using open source software		√	
1.(b) implementation tasks (as detailed in paragraph 3 and listed below), consist of			
3.(a) coordinating and administrating the work of the Network and the Community in order to fulfil the mission set out in Article 3, in particular by supporting cybersecurity start-ups, SMEs, microenterprises, associations and civic technology projects in the Union and facilitating their access to expertise, funding, investment and markets		√	
3.(b) establishing and implementing the annual work programme, in accordance with the Agenda and the multiannual work programme	√	√	√
3.(c) supporting, where appropriate, the achievement of Specific Objective 4 – 'Advanced Digital Skills' as set out in Article 7 of Regulation (EU) 2021/694, in cooperation with European Digital Innovation Hubs	√	√	
3.(d) providing expert advice on cybersecurity industry, technology and research to the Commission when the Commission prepares draft work programmes pursuant to Article 13 of Decision (EU) 2021/764		√	
3.(e) carrying out or enabling the deployment of ICT infrastructure and facilitating the acquisition of such infrastructure, for the benefit of society, industry and the public sector, at the request of Member States, research communities and operators of essential services, by means of, inter alia, contributions from Member States and Union funding for joint actions, in accordance with the Agenda, the annual work programme and the multiannual work programme	√		
3.(f) raising awareness of the mission of the Competence Centre and the Network and of the objectives and tasks of the Competence Centre		√	√
3.(g) without prejudice to the civilian nature of projects to be financed from Horizon Europe, and in accordance with Regulations (EU) 2021/695 and (EU) 2021/694, enhancing synergies and coordination between the cybersecurity civilian and defence spheres		√	

ECCC tasks and responsibilities	Activity 1	Activity 2	Activity 3
Article 10 - Cooperation of the Competence Centre with other Union institutions, bodies, offices and agencies and international organisations		√	√
Article 17 - Tasks of the Executive Director	√	√	√
Article 25 - Establishment of the budget			√
Article 26 - Presentation of the Competence Centre's accounts and discharge			√
Article 27 - Operational and financial reporting			√
Article 28 - Financial rules			√
Article 29 - Protection of financial interests of the Union			√
Article 30 - Staff			√
Article 31 - Seconded national experts and other staff			√
Article 32 - Privileges and immunities			√
Article 33 - Security rules			√
Article 34 - Transparency			√
Article 35 - Gender balance			√
Article 36 - Security rules on the protection of classified information and sensitive non-classified information			√
Article 37 - Access to documents			√
Article 38 - Monitoring, evaluation and review			√

II.1 MULTI-ANNUAL WORK PROGRAMME

The Activities for the Multiannual Work Programme 2025-2027 of the ECCC correspond to three specific objectives, which are re-ordered and updated compared with SPD 2024-2026:

- **Objective #1: Implement DEP, HEP, and as relevant other funding mechanisms, and support acquisitions**

  For this Work Programme, the main funding sources foreseen will continue to come from DEP. The estimated budget for the Cybersecurity part of DEP during the 4-year period 2024-27 is approximately EUR 500 million.

  The adoption of the DEP work programme 2025-2027 by the ECCC will be a major milestone during this period. Key tasks will be the evaluation of DEP calls for proposals, preparation and signature of grants and procurements, and managing projects. The ECCC will entirely manage these tasks, independently from EC services after reaching full financial autonomy. Moreover, the EC services are expected to transfer to the ECCC the responsibility of managing existing DEP projects. Moreover, in line with Article 5.5 of the ECCC Regulation, the EC may delegate to the ECCC the implementation of HEP in the area of cybersecurity (evaluation of proposals, management of grants, etc.).

- **Objective #2: Coordinate and further develop the Network of NCCs and the Cybersecurity Competence Community; develop, implement and monitor the ECCC strategic advice and priorities under the Agenda, the multiannual and the annual work programme**

  The ECCC will facilitate and coordinate the work of the Network of NCCs. The Network is composed of one NCC from each MS[16]. Over the course of 2022, seven Working Groups (WGs) of the GB were established, of which several relate to the functioning of the NCCs Network (namely WGs 1-3):
  - WG1-Community membership and registration.
  - WG2-NCCs Reference Manual (working title, pending a final title).
  - WG3-NCCs Network functioning.
  - WG4-Strategic Agenda.

[16] NCCs are upon their request, in accordance with Article 6(2) or 6(5) of Regulation (EU) 2021/887, assessed by the Commission as to their capacity to manage EU funds to fulfil the mission and objectives laid down in the ECCC Regulation. Further to the Commission assessment, NCCs may receive direct EU financial support, including grants awarded without a call for proposals, in order to carry out their activities. The modalities for the EU financial support to NCCs (funding amounts, call dates and other details) are indicated in the DEP work programme.

- WG5-Cyber Skills.
- WG6-Collaboration with Ukraine.
- WG7-Security Operation Centres (SOCs).

Most of the WGs above have been actively delivering input. The WGs provide strategic advice to the ECCC GB, on the Strategic Agenda, the annual work programme and the multiannual work programme, through the organisation of activities with relevant stakeholders.

Article 18-20 of the ECCC Regulation foresee a Strategic Advisory Group (SAG) that will regularly advise the ECCC in respect of the performance of its activities and ensure communication with the Community and other relevant stakeholders. The SAG could be established once a critical mass of community members will be registered by MS. The Community, in particular through the SAG, should provide input to the activities of the ECCC, to the Agenda, to the multiannual work programme and to the annual work programme.

The Strategic Agenda[17] of the ECCC, adopted by the GB in 2023 based on input from a dedicated Working Group of the GB, is a comprehensive strategy which sets out priorities for the development of European cybersecurity capabilities and for ECCC's activities[18], according to the following high-level structure:

1. To support SMEs to develop and use strategic cybersecurity technologies, services and processes:
   1.1 Processes and tools for managing cybersecurity information and risk management
   1.2 Secure and resilient hardware and software systems
2. To support and grow the professional workforce:
   2.1 Development of cybersecurity skills: education and professional training
   2.2 Cybersecurity skills framework and competence assessment
3. To strengthen research, development and innovation expertise in the broader European cybersecurity ecosystem:
   3.1 Promoting post-quantum cryptography standardisation and adoption
   3.2 Support for European Cybersecurity Certification
   3.3 Strengthening market competitiveness
   3.4 Promoting collaboration and information sharing

The Strategic Agenda includes also 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.*

When drafting the annual work programme and the multiannual work programme, the ECCC will take into account the input received from the NCCs, the Community and its working groups, the Strategic Advisory Group (SAG), and ENISA. The GB will monitor the implementation and ensure the dissemination of the Strategic Agenda.

[17] The Strategic Agenda adopted by ECCC GB in March 2023 will be detailed in an Action Plan currently in preparation. The Action Plan will be presented for adoption to ECCC GB during 2024 and next version of this SPD document will be updated accordingly to reflect it.
[18] Article 2 point (8) of the Regulation

The Strategic Agenda will guide the drafting of the annual and multiannual work programmes of the ECCC, more specifically for Activity 1.

The annual work programme of the ECCC will define, in accordance with the Strategic Agenda and the multiannual work programme, the cyber priorities for the DEP and, to the extent that they are co-financed by the MS, also the priorities for the HEP, in line with article 13.3.c and 21.3.b of the ECCC Regulation The HEP and DEP work programmes may include "joint actions" between the ECCC and MS, as defined in article 2(5) of the ECCC Regulation.

- **Objective #3: Consolidate financial and operational autonomy**

Activities covered under this objective were predominant in previous SPDs of the ECCC, during the establishment stage. From 2025, when the ECCC will be at cruising speed, the focus is to ensure an efficient and effective management of resources, including:

- Governance, coordination and compliance
  - ED office, coordination and management of the ECCC
  - Planning and programming activities and documents
  - Relation with GB and ECCC stakeholders, including host country; Secretariat for ECCC GB
  - Liaison activities with other EU bodies in the remit of ECCC mandate
  - Compliance and internal control
  - Communication, dissemination and outreach
- Management of assets and of financial and human resources
  - Consolidate financial and human resources
  - Consolidate IT tools, ICT assets, security rules and other logistical aspects
  - Building and facilities management, including environmental management
  - Relations with host country and adequate implementation of the Host Agreement
  - Monitoring, evaluations, access to documents, reporting

II.2 HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2025 – 2027

II.2.1 Overview of the past and current situation

The ECCC Regulation entered into force on 28 June 2021. Since then, DG CONNECT of the EC has been working on the establishment of the ECCC. Preparatory actions, notably HR-related rules, were adopted in 2022 which enabled the recruitment of the majority of ECCC staff members during 2023. The EC services continue acting on behalf of the ECCC until the ECCC reaches full financial autonomy.

II.2.2 Outlook for the years 2025 – 2027

As of 2025, the management of DEP and HEP funding will be the focus of ECCC.

Selection and recruitment of the initial staff members of the ECCC which started in 2022, increased significantly in 2023 and reached full capacity in 2024, including the appointment of the ED. To improve synergies and efficiency gains, the Accounting Officer and Data Protection Officer are shared with ENISA since 2023 (see section below on synergies).

II.2.3 Resource programming for the years 2025 – 2027

Financial Resources

As defined in the Regulation, the ECCC is funded by the EU, with the possibility of joint actions funded by the EU and by voluntary contributions from MS.

The EU contribution shall be paid from the appropriations in the EU general budget allocated to Cybersecurity activities in the DEP Programme, the specific programme implementing HEP established by Decision (EU) 2021/764 and other relevant EU programmes, as needed for the implementation of the tasks or the achievement of the objectives of the ECCC, subject to decisions taken in accordance with the legal acts of the EU establishing those programmes.

While for 2024, all budget allocations foreseen come from DEP appropriations, for 2025 it is still to be determined. For further details please see Annex III.

Table 1. Appropriations

Year	2024	2025	2026	2027
Total appropriations for ECCC *(EUR)*	218.831.127,16	125.766.680,63	126.032.746,58	126.496.480,45

Human Resources

The Staff Regulations and Conditions of Employment of Other Servants of the EU apply to the staff of the ECCC. The first recruitments were initiated in 2022, and continued in 2023, including the selection of the ED. Before 2025 all posts are expected to be filled and no new posts are foreseen for 2025-2027. 2023 recruits started to work at the temporary ECCC headquarters in Bucharest, until the final move to permanent offices (in different floors of the same building) in 2024. For further info please see Annex IV.

II.2.4 Strategy for achieving efficiency gains

On July 2022, the ECCC became an ad hoc member of the EU Agencies Network (EUAN), of which full membership requires financial autonomy, thus gaining access to exchange knowledge and best practices on horizontal issues for EU agencies and bodies.

In 2023 the ECCC and ENISA signed a service-level agreement (SLA) regarding shared services (namely Data Protection Officer and Accounting Officer services).

Moreover, the ECCC is following the developments around the Back Office Arrangements for Joint Undertakings (BOA/JUs)[19] and may benefit from such arrangements at a later stage.

The ECCC will look for consolidation and new ways to cooperate with other EU bodies and agencies to benefit or take inspiration from already existing resources and approaches, e.g. use of existing framework contracts for procurement.

II.2.5 Negative priorities/decrease of existing tasks

By 2025 the ECCC should be at cruising speed and tasks associated to its set-up will decrease (e.g. legal advice regarding seat agreement with host country, etc.) allowing to allocate most resources to the implementation of operational tasks.

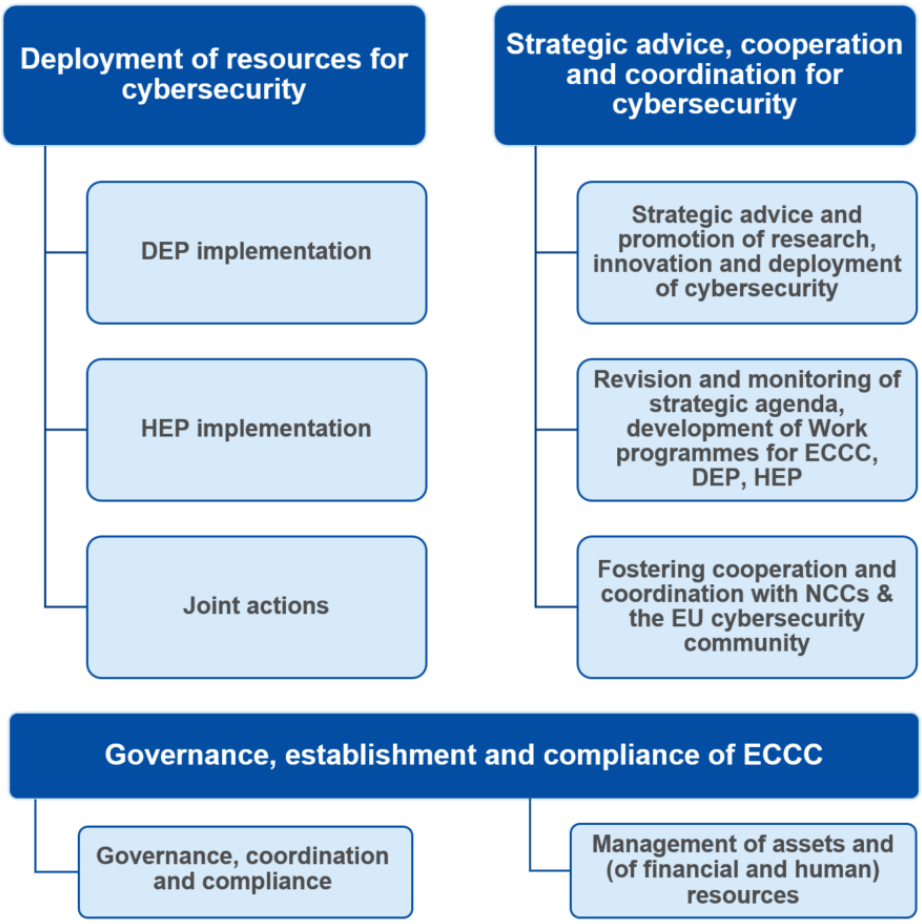
[19] According to the Single Basic Act (article 13), by 30.11.2022, Joint Undertakings shall operate Back Office Arrangements (setting out common corporate lines) by concluding service level agreements. BoA should cover areas like human resource support, legal support, accounting, communication, et al.

SECTION III. WORK PROGRAMME 2025

III.1 EXECUTIVE SUMMARY

The overall objectives described in the multiannual outlook 2025-2027 are elaborated in the activities indicated in this section for the year 2025. In 2025 the focus will shift from set-up related activities to operational tasks, notably regarding DEP and HEP implementation[20], and possibly also joint actions supported with MS contributions. Other activities will include the monitoring and possible update of the Strategic Agenda of the ECCC, the full operation of the Network of NCCs and of the Community. Another Activity will cover all actions required to support the work of the ECCC, its operations and its staff.

The image below provides an overview of the 2025 activities. The next sections elaborate on the context, expected activities and associated results for each of the 3 activities of the SPD.



[20] DEP assumes programming and execution, HE assumes execution while Joint actions (using both DEP and HE funding) assumes programming and execution

III.2 ACTIVITIES

III.2.1. ACTIVITY 1: Deployment of resources for cybersecurity

This Activity contributes to the objectives of Article 4 *(b) of the ECCC Regulation: "implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes;* and *(d) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary to fulfil the tasks set out in Article 5 and in accordance with the respective work programs set out in point (b) of Article 5(3)*."

This Activity is a continuation of Activity 2 in previous SPDs of ECCC and will follow closely the Strategic Agenda adopted by ECCC GB in 2023.

Building on the work delivered in previous years, the ECCC, together with the Network of NCCs, will continue to implement the actions under Specific Objective 3 (Cybersecurity and Trust) of the DEP. This includes the management of projects awarded under the DEP work programmes 2021-2022 and 2023-2024, as well as the evaluation of proposals, signature of grants and management of the proposals retained for funding under the first call of the DEP work programme 2025-2026. In addition, it is expected that the HEP will be implemented by ECCC by 2025.

Important actions to be undertaken in this Activity in 2025 include the following:

Area	Expected activities	Expected results
DEP implementation	Management of projects from DEP WP 2021-2022 and WP 2023-2024. Implement DEP calls for WP 2025-2026 (take financing decisions, launch calls, organise evaluations, conclude grant agreements) taking account of the adopted Strategic Agenda Where necessary, adopt guidelines for proposals and projects, model grant agreement, methodology to calculate MS in-kind contribution	Launch call for proposals and follow up on it Fulfilment of DEP KPIs: [DEP] Indicator 3.1a: Cybersecurity infrastructure and/or tools jointly procured: 15 tools and/or infrastructures by 2027[21] [DEP] Indicator 3.1b: Cybersecurity infrastructure and/or tools deployed: 165 infrastructure (15) and/or tools (150) deployed by 2027[22] [DEP] Indicator 3.2: Users and communities getting access to European cybersecurity facilities[23] : -150 by 2027 & 300 by 2028
HEP implementation	Possibly manage part of HEP further to EC services' delegation.	Fulfil HEP KPIs.
Joint actions	Identify possible joint actions to be supported by contributions from some MS and by EU budget from DEP or HEP	Fulfil KPIs associated with joint actions.

III.2.2 ACTIVITY 2: Strategic advice, cooperation and coordination for cybersecurity

This is a continuation of Activity 3 and 4 in previous SPDs of ECCC. The following actions are proposed:

(a) Strategic advice and promotion of research, innovation and deployment of cybersecurity

[21] [Method for setting the target] The number of joint infrastructure or joint actions will be defined by the ECCC. No joint action has been defined yet.
[22] [Method for setting the target] The number of joint infrastructures or joint actions will be defined by the ECCC. It should be noted that infrastructure and tools may be of a varied nature: the target for infrastructures is 15 and the number of tools is 150.
[23] [Method for setting the target] The target is to have at least 20 Member States using each facility.

ECCC will consult its stakeholders to develop together priorities for promoting research, innovation and deployment in the area of cybersecurity. ECCC will also receive relevant input from ENISA in accordance with Article 5 c) of ECCC regulation[24]. The main purpose of this task is to ensure a strong European cybersecurity ecosystem that brings together the relevant stakeholders. The results from this work will contribute to the other areas of this Activity and to the dissemination efforts.

(b) Revision and monitoring of Strategic Agenda, development of ECCC Work programmes under DEP and HEP.

According to Article 2 point (8) of the Regulation, the "Agenda" is a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out recommendations for the development and growth of the European cybersecurity industrial, technological and research sector, as well as priorities for the ECCC's activities; it is non-binding with respect to decisions to be taken on the annual work programmes. The Strategic Agenda, as adopted by the GB[25], should be regularly updated, setting out strategic recommendations for the annual work programme and the multiannual work programme. The implementation of the Strategic Agenda will be monitored.

The ECCC annual work programme will set, in accordance with the Strategic Agenda and the multiannual work programme, priorities for DEP and HEP, to what extent these will be co-financed by the MS.

EC services will take into account the input from the Strategic Agenda when preparing the HEP WP. After achieving its financial autonomy, the ECCC will prepare the cybersecurity parts of the DEP work programme and contribute to the HEP work programme in accordance with the actions set out in the Strategic Agenda.

(c) Fostering cooperation and coordination with NCCs and the EU Cybersecurity Community

The Network of NCCs is composed of all NCCs notified to the GB by the MS (Article 6.7 of the Regulation). NCCs function as contact points at the national level for the Community and the ECCC (Article 7.1(a) of the Regulation). They also provide support to carry out actions under the ECCC Regulation, and they can pass on financial support to local actors (Article 7.1(f) of the Regulation). 25 MS and 3 associated countries have notified to the GB the entities acting as their NCCs.

Moreover, even dedicated Working Groups of the GB have been established, which cooperate closely with the NCCs Network:

- *WG1-Community membership and registration.*
- *WG2-NCCs Reference Manual (working title, pending a final title).*
- *WG3-NCCs Network functioning.*
- *WG4-Strategic Agenda.*
- *WG5-Cyber Skills.*
- *WG6-Collaboration with Ukraine.*
- *WG7-Security Operation Centres (SOCs).*

The ECCC provides operational support to the NCCs, and their functioning as a Network, and to the European Cybersecurity Competence Community. A dedicated DEP Call 'Cybersecurity Community Support' (CNECT/2022/OP/0033) supports the activities of the Cybersecurity Competence Community at European level, within the scope and operations of the ECCC and the NCCs Network. The main objectives of this Action are to analyse the Cybersecurity Competence Community, link it with the ECCC and the NCCs Network, and stimulate collaboration. The EC services monitor this Action and manages the contractor. The ECCC will undertake certain tasks in cooperation with ENISA (Article 3.2 of the Regulation) to be defined

[24] The ECCC can benefit from ENISA's work in identifying research and innovation priorities as per Article 11.a) of the CSA, already resulting from extensive consultation with the EU research community and industry.
[25] Article 13.3(a) of the Regulation.

and planned in accordance to the Memorandum of Understanding (MoU) signed between the two organisations in August 2023.

The Cybersecurity Competence Community should involve a large, open, and diverse group of actors involved in cybersecurity technology, including in particular research entities, supply/demand-side industries and the public sector that should conduct activities in line with EU strategic autonomy. It provides, particularly through the SAG, input to the activities and work plan of the ECCC, and it benefits from the Community-building activities of the ECCC and the Network.

In cooperation with the NCCs and the Community, the ECCC should increase visibility of EU cybersecurity expertise, products and services, as well as bring together resources and knowledge on cybersecurity markets and research, providing an EU-wide overview of the cybersecurity ecosystem. This is supported also through the mentioned Coordination and Support Action on the Cybersecurity Competence Community, including an "EU cybersecurity market observatory" in coordination with ENISA. The ECCC can benefit from ENISA work on surveying the market. The ECCC and ENISA can jointly coordinate the access to the network of NCCs in relation to surveys, market related data, access to databases, market analytics and research results.

Moreover, as of 2023 Iceland, Liechtenstein and Norway are full ECCC members (without vote in the GB), contributing financially to ECCC activities and benefiting from them, including support to and involvement of their NCCs and Community members.

Actions to be undertaken in the Activity 2 area during the course of 2025 include the following:

Area	Expected activities	Expected results
Strategic advice and promotion of research, innovation and deployment of cybersecurity	Priorities for promoting research, innovation and deployment of cybersecurity Dissemination activities and strategic advice	Develop or update priorities for promoting research, innovation and deployment of cybersecurity Dissemination activities and strategic advice
Revision and monitoring of Strategic Agenda, development of Work programmes for ECCC, DEP, HEP	**Strategic Agenda** Revision of the adopted Strategic Agenda, following consultation with all relevant actors (EC, NCCs, Community, ENISA, SAG) to prepare next version of the Strategic Agenda Monitoring the implementation of the previous Strategic Agenda adopted in 2023. Periodic reporting on the monitoring of the Strategic Agenda. Dissemination of the Agenda to relevant stakeholders, including the HEP Program Committee **Work programmes related activities** Development, adoption and monitoring of the multiannual work programme and the annual work programme for ECCC and for DEP and HEP	Preparation of the next version of the Strategic Agenda Report on the implementation of the Strategic Agenda Contributions to dissemination activities regarding the Agenda and research and innovation priorities Timely delivery of draft and final SPDs Timely input into the consultation related to DEP or HEP
Fostering cooperation and coordination with NCCs and the EU cybersecurity community	**Network of National Coordination Centres:** Complete the setting-up of the Network and smooth functioning as an integrated Network Implement and update the indicative "service catalogue" for NCCs Further definition and implementation of modalities of interaction between the ECCC and the Network of NCCs (coordination mechanisms, alignment of activities, organisation of workshops/recurrent meetings, etc.) **Cybersecurity Competence Community (stakeholders):** Community registrations and development of associated tools Support new Community registrations, develop relevant tools and stimulate activities Community participation to the activities of the working groups, where relevant Maintain the EU "cybersecurity market observatory" in coordination with ENISA	The Network of National Coordination Centres (NCCs) is fully established and functioning seamlessly as an integrated network, enabling effective communication and collaboration among member countries. A comprehensive and up-to-date "service catalogue" for NCCs is implemented and maintained. This catalogue outlines the range of common services and capabilities offered by NCCs to the Cybersecurity Competence Community. Well-defined and efficient coordination mechanisms are established between the ECCC and the Network of NCCs. Regular workshops and meetings are organized to facilitate alignment of activities, sharing of best practices, and collaborative efforts. Measures to sustain the NCC's to ensure the continuous functioning of the network are essential, ensuring funding is in place is critical to achieving this.

III.2.3 ACTIVITY 3: Governance, establishment and compliance of ECCC

This Activity is a continuation of the Activity 1 in previous SPDs, dedicated to set up the operational activities of the ECCC during its growing stage.

The Activity focusses on all the managerial and administrative activities required to support the operational tasks of the ECCC. As already stated in previous SPDs, after achieving its financial autonomy, the ECCC will focus mainly on its operational tasks, benefitting from the governance structures, rules, procedures and infrastructure in place. Starting with 2024 and then in 2025, the focus will be on ensuring efficient and effective use of existing resources.

The main actions are as follows:

- Governance, coordination and compliance
  - ED office, coordination and management of the ECCC
  - Planning and programming activities and documents
  - Relation with GB and ECCC stakeholders including host country; Secretariat for ECCC GB
  - Liaison activities with other EU bodies in the remit of ECCC mandate
  - Compliance and internal control
  - Communication, dissemination and outreach
- Management of assets and (of financial and human) resources
  - Efficient and effective management of financial and human resources
  - Consolidate IT tools, ICT assets, security rules and other logistical aspects
  - Building and facilities management, including environmental management
  - Relations with host country and adequate implementation of the Host Agreement
  - Monitoring, evaluations, access to documents, reporting

Actions to be undertaken in this Activity area in 2025 include the following:

Area	Expected activities	Expected results
Governance, coordination and compliance	ED office, coordination and management of ECCC Planning and related programming activities and documents. Implement performance indicators. Relation with GB and ECCC stakeholders including host MS; Secretariat for ECCC GB Liaison activities with the other EU bodies in the remit of ECCC mandate Compliance and internal control Communication, dissemination and outreach	Timely preparation, consultations, reviews and adoption of documents dedicated to planning and programming Transparency in decision making and involvement of relevant staff or staff committee Satisfactory support to the relevant stakeholders SLAs and MoUs agreed and associated efficiency gains High level of compliance with reduced number of recommendations following audits Communication strategy development and implementation
Management of assets and (of financial and human) resources	Consolidate financial and human resources Consolidate IT tools, ICT assets, security rules and other logistics aspects Building and facilities management, including environmental management Relations with host MS and adequate implementation of the Host Agreement Monitoring, evaluations, access to documents, reporting	Commitment rates above 95% and limited number of exceptions HR policies and implementing rules in place, satisfaction of staff Availability of tools and coverage of service needs Sustainable and environmentally friendly working conditions Requests and requirements addressed in a reasonable interval Timely reporting and timely follow up on requests, evaluations and recommendations

[This section will be further detailed when the internal structure will be decided and more staff will be recruited.]

ANNEXES

ANNEX I. ORGANISATION CHART

Soon after the entering into force of the Regulation, an Interim ED was appointed. The recruitment of the ED was launched in 2022; the first staff members were recruited that year. A large number of recruitments, including that of the ED, is expected to be concluded over the course of 2023, and this process will continue in 2024. On organisation chart will be proposed by future ED.

ANNEX II. RESOURCE ALLOCATION PER ACTIVITY 2025 – 2027

Resource allocation forecast is introduced below, with aggregated values. It is assumed that the allocation to be revised after this stage of establishment and initial operation of the ECCC.

No	Activity name	2025			2026			2027		
		TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)
1	Deployment of resources for cybersecurity	4	16	217.569.554,05	4	16	124.390.444,96	4	16	125.112.258,75
2	Strategic advice, cooperation and coordination for cybersecurity	2	2	267.923,11	2	2	283.785,67	2	2	285.432,42
3	Governance, establishment and compliance of the ECCC	4	10	993.650,00	4	10	1.092.450,00	4	10	1.098.789,28
Total		10	28	218.831.127,16	10	28	125.766.680,63	10	28	126.496.480,45

ANNEX III. FINANCIAL RESOURCES 2025 - 2027[26]

Budget Revenue

In accordance with the provisions of the legal framework applicable to the ECCC, for 2024 the only contributor is the EU with the budget planned for Cybersecurity activities in the DEP and covering administrative and operational costs. Contributions from the MS may be taken up with an amendment of the WP and the budget.

The EU budget will constitute a ceiling for the actual EU contribution, in accordance with Article 21 of the Regulation. The amount of MS contributions will be determined by the MS themselves.

Table 1: Revenue. General revenue

Revenue	2024	2025
	Revenues estimated by the Agency	Budget forecast
EU contribution	211.267.742	121.419.850
Other revenue	7.563.385	4.346.831
TOTAL REVENUES	**218.831.127**	**125.766.681**

Remark - the revenue for 2024 refer to the commitment appropriations.

[26] 2024 figures in the tables are based on the current EU draft budget for 2024.
The 2023 EFTA percentage for DEP is 2.93 %, while from 2024 onwards is 3.58%.

REVENUES	General revenues						
	Budget 2023	Estimated by ECCC for 2024	2025		VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
			Agency request	Budget forecast			
1 REVENUE FROM FEES AND CHARGES							
2 EU CONTRIBUTION	179.058.443,00	211.267.742,00	121.419.850,00		-43%	121.676.720,00	122.124.426,00
- Of which assigned revenues deriving from previous years' surpluses							
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	5.246.412,00	7.563.385,16	4.346.830,63		-43%	4.356.026,58	4.372.054,45
- Of which EEA/EFTA (excl. Switzerland)	*5.246.412,00*	*7.563.385,16*	*4.346.830,63*		-43%	*4.356.026,58*	*4.372.054,45*
- Of which candidate countries							
4 OTHER CONTRIBUTIONS							
5 ADMINISTRATIVE OPERATIONS							
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)							
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT							
7 CORRECTION OF BUDGETARY IMBALANCES							
TOTAL	184.304.855,00	218.831.127,16	125.766.680,63		-43%	126.032.746,58	126.496.480,45

The 2023 EFTA percentage for DEP is 2.93 %, while from 2024 onwards is 3.58%.

Commitment appropriations

Table 2: Commitment appropriations

Expediture	2024		2025	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1 - Staff expenditure	1.827.000	1.827.000	1.667.356	1.667.356
Title 2 - Infrastructure and operating expenditure	1.273.000	1.273.000	1.389.000	1.389.000
Title 3 - Operational expenditure	215.731.127	192.520.247	122.710.325	122.710.325
TOTAL Expediture	**218.831.127**	**195.620.247**	**125.766.681**	**125.766.681**

EXPENDITURE	Commitment appropriations						
	Budget 2023	Budget 2024	2025		VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
			Agency request	Budget forecast			
Title 1 - Staff expenditure	**1.768.000,00**	**1.827.000,00**	**1.667.355,78**	**0,00**	**-9%**	**1.534.482,48**	**1.789.832,46**
Salaries and allowances for temporary and permanent staff	882.000,00	890.000,00	759.555,78		-15%	807.606,48	959.832,46
Salaries and allowances for contractual agents	440.000,00	500.000,00	470.800,00		-6%	303.756,00	400.000,00
Seconded national experts, interim staff and trainees	62.000,00	100.000,00	100.000,00		0%	120.000,00	100.000,00
Insurance against sickness, accidents, occupational disease, unemployment and related		60.000,00	60.000,00		-	60.000,00	65.000,00
Recruitment	62.000,00	15.000,00	15.000,00		0%	15.000,00	10.000,00
Trainings	62.000,00	140.000,00	140.000,00		0%	100.000,00	120.000,00
Mission expenses	208.000,00	80.000,00	80.000,00		0%	80.000,00	80.000,00
Social welfare and contacts between staff	42.000,00	30.000,00	30.000,00		0%	30.000,00	30.000,00
Medical service and expenses	10.000,00	12.000,00	12.000,00		0%	18.120,00	25.000,00
Title 2 - Infrastructure and operating expenditure	**1.151.239,00**	**1.273.000,00**	**1.389.000,00**	**0,00**	**9%**	**1.583.000,00**	**1.390.000,00**
Rental of building and associated costs	156.000,00	290.000,00	315.000,00		9%	330.000,00	250.000,00
Computer centre operations and data processing	62.000,00	290.000,00	300.000,00		3%	400.000,00	310.000,00
Moveable property and associated costs	353.912,00	218.000,00	218.000,00		0%	228.000,00	170.000,00
Current administrative expenditure	261.327,00	103.000,00	106.000,00		3%	120.000,00	120.000,00
Publication, communication and trasnlation costs	100.000,00	150.000,00	180.000,00		20%	200.000,00	250.000,00
Technical meetings	52.000,00	52.000,00	60.000,00		15%	70.000,00	75.000,00
Statutory meetings - Governing board, NCC etc	42.000,00	50.000,00	60.000,00		20%	70.000,00	75.000,00
Studies	124.000,00	120.000,00	150.000,00		25%	165.000,00	140.000,00
Title 3 - Operational expenditure	**181.385.616,00**	**215.731.127,16**	**122.710.324,85**	**0,00**	**-43%**	**122.915.264,10**	**123.316.647,99**
Operational expenditure	*181.385.616,00*	*215.731.127,16*	*122.710.324,85*		-43%	*122.915.264,10*	*123.316.647,99*
TOTAL	**184.304.855,00**	**218.831.127,16**	**125.766.680,63**	**0,00**	**-43%**	**126.032.746,58**	**126.496.480,45**

Remark: The budget appropriations are presented according to an amended budgetary nomenclature. For 2023 - presentation is according to the initial budget approved.

Payment appropriations

Table 3: Payment appropriations

EXPENDITURE	Payment appropriations						
	Budget 2023	Budget 2024	2025		VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
			Agency request	Budget forecast			
Title 1 - Staff expenditure	**1.768.000,00**	**1.827.000,00**	**1.667.355,78**	**0,00**	**-9%**	**1.534.482,48**	**1.789.832,46**
Salaries and allowances for temporary and permanent staff	882.000,00	890.000,00	759.555,78		-15%	807.606,48	959.832,46
Salaries and allowances for contractual agents	*440.000,00*	*500.000,00*	*470.300,00*		-6%	*303.756,00*	*400.000,00*
Seconded national experts, interim staff and trainees	*62.000,00*	*100.000,00*	*100.000,00*		0%	*120.000,00*	*100.000,00*
Insurance against sickness, accidents, occupational disease, unemployment and related		60.000,00	60.000,00		-	60.000,00	65.000,00
Recruitment	62.000,00	15.000,00	15.000,00		0%	15.000,00	10.000,00
Trainings	62.000,00	140.000,00	140.000,00		0%	100.000,00	120.000,00
Mission expenses	208.000,00	80.000,00	80.000,00		0%	80.000,00	80.000,00
Social welfare and contacts between staff	42.000,00	30.000,00	30.000,00		0%	30.000,00	30.000,00
Medical service and expenses	10.000,00	12.000,00	12.000,00		0%	18.120,00	25.000,00
Title 2 - Infrastructure and operating expenditure	**1.151.239,00**	**1.273.000,00**	**1.389.000,00**	**0,00**	**9%**	**1.583.000,00**	**1.390.000,00**
Rental of building and associated costs	156.000,00	290.000,00	315.000,00		9%	330.000,00	250.000,00
Computer centre operations and data processing	62.000,00	290.000,00	300.000,00		3%	400.000,00	310.000,00
Moveable property and associated costs	353.912,00	218.000,00	218.000,00		0%	228.000,00	170.000,00
Current administrative expenditure	261.327,00	103.000,00	106.000,00		3%	120.000,00	120.000,00
Publication, communication and trasnlation costs	100.000,00	150.000,00	180.000,00		20%	200.000,00	250.000,00
Technical meetings	52.000,00	52.000,00	60.000,00		15%	70.000,00	75.000,00
Statutory meetings - Governing board, NCC etc	42.000,00	50.000,00	60.000,00		20%	70.000,00	75.000,00
Studies	124.000,00	120.000,00	150.000,00		25%	165.000,00	140.000,00
Title 3 - Operational expenditure	**223.912.363,00**	**192.520.247,25**	**122.710.324,85**	**0,00**	**-36%**	**122.915.264,10**	**123.316.647,99**
Operational expenditure	223.912.363,00	192.520.247,25	122.710.324,85		-36%	122.915.264,10	123.316.647,99
TOTAL	**226.831.602,00**	**195.620.247,25**	**125.766.680,63**	**0,00**	**-36%**	**126.032.746,58**	**126.496.480,45**

Remark: The budget appropriations are presented according to an amended budgetary nomenclature. For 2023 - presentation is according to the initial budget approved.

Budget outturn table is not filled in for ECCC as it covers the period before the financial autonomy.

Details on the use of financial resources

TITLE 1

This appropriations from this title will cover the staff-related expenditure of the Centre, amongst which:

- the remuneration (salaries and allowances) of the temporary and contractual staff in accordance with the Staff Regulations.
- recruitment costs,
- mission expenditure;
- insurances and medical check-up of staff and associated analyses required;
- other staff-related expenses.

Details are revealed in the relevant budgetary tables.

TITLE 2

This appropriations from this title will cover the following main items:

- Logistical costs – utility costs, furniture and equipment of Permanent office, office supplies etc.
- IT infrastructure, equipment and data processing
- Meeting costs – technical meetings and statutory meetings
- Publications, communication and translation costs.
- External studies

TITLE 3

The title accommodates the appropriations for the operational expenditure of the ECCC, taking of board the non-differentiated character of the budgetary credits in the title, i.e. the distinction between commitment and payment appropriations.

ANNEX IV. HUMAN RESOURCES QUANTITATIVE

Table 1 - Staff population and its evolution; Overview of all categories of staff

A. Statutory staff and SNE (estimation September 2023)

Staff	2023			2024	2025	2026	2027
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12	Occupancy rate %	Authorised staff	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (AD)	10	5	50%	10	10	10	10
Assistants (AST)							
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	10	5	50%	10	10	10	10
EXTERNAL STAFF	FTE corresponding to the authorised budget	Executed FTE as of 31/12	Execution Rate %	Headcount as of 31/12/N-1	FTE corresponding to the authorised budget	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	27	24	89%	27	27	27	27
Seconded National Experts (SNE)	1	0	0%	1	1	1	1
TOTAL EXTERNAL STAFF	28	24	86%	28	28	28	28
TOTAL STAFF	38	29	76%	38	38	38	38

B. Additional external staff expected to be financed from grant, contribution or service-level agreements

Not applicable.

C. C. Other Human Resources

Structural service providers[27]

	Actually in place as of 31/12/2023
Security	0
IT	0
Other (specify)	0
.....	

Interim workers

	Total FTEs in year 2023
Number	1

[27] (6) Service providers are contracted by a private company and carry out specialized outsourced tasks of a horizontal/support nature. At the Commission, following general criteria should be fulfilled: 1) no individual contract with the Commission 2) on the Commission premises, usually with a PC and desk 3) administratively followed by the Commission (badge, etc.) and 4) contributing to the added value of the Commission

Table 2 – Multi-annual staff policy plan 2025, 2026, 2027

Function group and grade	2023				2024		2025		2026		2027	
	Authorised Budget		Actually filled as of 31/12/2023		Authorised Budget		Envisaged		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts
AD 16												
AD 15												
AD 14		1		0		1		1		1		1
AD 13												1
AD 12		2		0		2		2		2		2
AD 11		2		0		2		2		2		1
AD 10												
AD 9												2
AD 8		3		3		3		3		3		2
AD 7		2		2		2		2		2		1
AD 6												
AD 5												
AD TOTAL		10		5		10		10		10		10
AST 11												
AST 10												
AST 9												
AST 8												
AST 7												
AST 6												
AST 5												
AST 4												
AST 3												
AST 2												
AST 1												
AST TOTAL		0		0		0		0		0		0
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL		0		0		0		0		0		0
TOTAL		10		5		10		10		10		10
GRAND TOTAL		10		5		10		10		10		10

- External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget 2023	Executed FTE as of 31/12/2023	Headcount as of 31/12/2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027
Function Group IV	21	21	21	21	21	21	21
Function Group III	2	2	2	2	2	2	2
Function Group II	4	4	4	4	4	4	4
Function Group I	0	0	0	0	0	0	0
TOTAL	27	27	27	27	27	27	27

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2023	Executed FTE as of 31/12/2023	Headcount as of 31/12/2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027
TOTAL	1	0	0	1	1	1	1

Table 3, recruitment forecasts 2024 following retirement/mobility or new requested posts is not applicable due to early state of ECCC set-up. To be updated in future SPDs.

Number of inter-agency mobility year 2023 from and to the ECCC: 0.

ANNEX V. HUMAN RESOURCES QUALITATIVE

Due to limited data for the past years, part of the tables of this Annex will be filled in future SPDs.

A. Recruitment policy

All implementing rules required for recruitment are in place. Further HR related rules might be adopted by the GB.

		Yes	No	If no, which other implementing rules are in place
Engagement of CA	Model Decision C(2019)3016	X		
Engagement of TA	Model Decision C(2015)1508	X		
Middle management	Model decision C(2018)2540	X		
Type of posts	Model Decision C(2018)8800	X		

B. Appraisal and reclassification/promotions

		Yes	No	If no, which other implementing rules are in place
Reclassification of TA	Model Decision C(2015)9560	X		
Reclassification of CA	Model Decision C(2015)9561	X		

C. Gender representation

While acknowledging the difficulty of reaching gender balance in technical fields such as cybersecurity, the ECCC will take due account in its selection processes of the principle of gender balance in line with the Gender Equality Strategy 2020-2025[28].

Table **– Estimated data for 31/12/2023 /statutory staff**

		Official		Temporary		Contract Agents		Grand Total	
		staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level			1	20%	17	71%	18	62%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			1	20%	17	71%	18	62%
Male	Administrator level			4	80%	7	29%	11	38%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			4	80%	7	29%	11	38%
Grand Total				5	100%	24	100%	29	100%

D. Geographical Balance

Table – Estimated data for 31/12/2023 - statutory staff only

Nationality	AD +CA FG IV		AST/SC - AST + CA FGI / CA FGII / CA FGIII		Total	
	Number	% of total staff member in AD and FGIV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
Romanian	16	64%	4	100%	20	69%
Italian	4	16%	0	0%	4	14%
Greek	1	4%	0	0%	1	3%
Cypriot	1	4%	0	0%	1	3%
German	1	4%	0	0%	1	3%
Polish	1	4%	0	0%	1	3%
Bulgarian	1	4%	0	0%	1	3%
Total	25	100%	4	100%	29	100%

While the ECCC should seek as much as possible geographical diversity in its coming recruitments, it should be noted that the majority of applications received so far are from Romanian nationals.

[28] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Union of Equality: Gender Equality Strategy 2020-2025", COM/2020/152 final. Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0152.

E. Schooling

Policy to be defined.

ANNEX VI. ENVIRONMENT MANAGEMENT

Not applicable until permanent premises of ECCC are operational.

ANNEX VII. BUILDING POLICY

The ECCC headquarters is located in Bucharest. The ECCC opened its Temporary Premises in Bucharest located at the Politehnica Campus building in 2023. The ECCC also concluded an Administrative Agreement with the EC Representation in Bucharest, enabling ECCC staff to use the premises of EC Representation within the scope of the Administrative Agreement. The ECCC will move to its Permanent Premises by end of 2024 located at the Campus building. The process may follow the specific provisions regarding building projects as indicated in Article 266 of the Financial Regulation applicable to the general budget of the EU.

ANNEX VIII. PRIVILEGES AND IMMUNITIES

Not applicable until hosting agreement is adopted.

ANNEX IX. EVALUATIONS

To be updated in next versions, pending financial autonomy.

ANNEX X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The ECCC is in the process of developing its internal control in line with the Internal Control Framework developed by European Commission which consists of five internal control components and 17 principles based on the COSO 2013 Internal Control-Integrated Framework.

Until its full autonomy, the ECCC is operating based on the DG CONNECT's control management system, designed to provide reasonable assurance regarding the achievement of the five internal control objectives derived from the ECCC's Financial regulation as well as ensuring continuous improvement and the need to implement a flexible and effective governance.

Further, the ECCC is continuing to rely on the ENISA accounting officer who certifies the year-end accounts, thus providing reasonable assurance that the accounts present a true and fair view of the financial situation. ECCC's internal control strategy is foreseen to be proposed for adoption during first semester of 2024.

ECCC's anti-fraud strategy, which is to be developed in line with OLAF methodology, is foreseen to be proposed for adoption during second semester of 2024, following a standalone fraud risk assessment exercise which will take place after financial autonomy has been achieved.

ANNEX XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

The ECCC does not receive any form of grant. The ECCC initiated in 2021 the process of concluding a number of SLAs and agreements that the ECCC has to undertake during the establishment phase in order to launch recruitments and reach operational autonomy. The preparatory work started in 2021 and has

resulted to concrete agreements in the course of 2022, while further work is ongoing. The table below presents the status of SLAs and budget as of September 2023.

Service-level agreement	Actual or expected date of signature	Total amount (EUR)	Duration	Counterpart	Short description
DG DIGIT	Signed	31.283,15	1 year (automatic renewal)	DIGIT	Global SLA for provision of IT services
DG HR	Signed	N/A	1 year (automatic renewal)	HR	SLA where DG HR provides implementation and operation of SYSPER and related services to ECCC
PMO	Signed	3.055,30	1 year (automatic renewal)	PMO	SLA for general assistance and/or provision of applications for which the PMO is system owner
EPSO	Signed	N/A	1 year (automatic renewal)	EPSO	SLA providing to ECCC assistance and access to Job oportunities page, reserve lists, EPSO's planning, ex-post controls, 3rd language testing and organisation of tailor made selections
EU Agencies Network	Signed	719,13	Indefinite period of time	SG	SLA to to mutualise the costs for the Shared Support Office
ENISA	Signed - 20/12/2022	54.604,32	1 year (automatic renewal)	ENISA	SLA for the provision of data protection officer services and accounting officer sercices
DG BUDG	*Under preparation*			BUDG	SLA for implementation and usage of ABAC
DG DIGIT / CERT-EU	*Under preparation*			DIGIT	SLA for the use of CERT-EU
RTD	*Under preparation*			RTD	SLA for the usage of eGrants tool

ANNEX XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

To be updated in future versions of SPD.