DECISION No GB/2023/8

of

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

Adopting the Single Programming Document 2024-2026

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(7) 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

The Single Programming Document 2024-2026 is adopted as set out in the Annex 1 of this decision.

[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

The Statement of estimates for the financial year 2024 is adopted as part of SPD financial annexes of this Decision.
The Single Programming Document, including the 2024 work programme and statements of estimates for 2024, shall become definitive after the final adoption of the General Budget of the European Union for 2024. In the event of a change in the amount of the European Union contribution and/or in the establishment plan, the respective provisions of the work programme shall be adjusted accordingly.

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

Single programming document 2024-2026

Version: Approved by the Governing Board of the ECCC in Decision No GB/2023/8

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 ECCC Single Programming Document (SPD) 2024-2026 as approved by the Governing Board of the ECCC in Decision No GB/2023/8. The Governing Board may amend the Single Programming Document 2024–2026 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

Our society and economy are increasingly dependent on digital technologies, while being increasingly exposed to cyber threats, which have been propelled by the Covid-19 pandemic and, more recently, by geopolitical tensions around the Russian war of aggression against Ukraine. Such greater dependence on digital technologies and rise in intensity of cyber threats call for enhanced cyber resilience, as a condition for EU stability, prosperity and autonomy while preserving an open economy.

The EU has continued developing its action on cybersecurity in various ways. These include recently adopted revision of the NIS Directive and the legislative proposal for a Cyber Resilience Act, policy initiatives such as the Communication on cyber defence, as well as funding support including three calls for proposals launched in 2022 under the Horizon Europe and Digital Europe programmes (HEP, DEP). The European Cybersecurity Competence Centre (ECCC), together with the National Coordination Centres (NCCs) are an important component of this coordinated effort to enhance cybersecurity capabilities and 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 better coordination amongst relevant stakeholders. This implies setting strategic objectives for investment, deployment, and use of cybersecurity, while pooling EU and national resources, notably the Digital Europe Program, to deliver on those objectives.

The three first Single Programming Documents (SPDs) of the ECCC, i.e. SPD 2021-2023, SPD 2022-2024 and SPD 2023-2025, set the foundations for the functioning of the ECCC, focusing on legal, administrative and governance aspects. SPD 2024-2026 places a greater focus on operationalisation than the previous SPD.

In 2023 the ECCC GB held three in person meetings, and adopting number of decisions necessary for the ECCC to function and start to deliver its tasks. In 2023 the majority of NCCs were established. The ECCC provided NCCs with guidance and support for their activities, including opportunities for the NCCs to have exchanges amongst NCCs, EU funding for NCCs' operations and for support to third parties. The NCCs play an increased role regarding the objectives of the ECCC Regulation, notably strengthening the cyber community and collaborating with the ECCC.

In 2023, the ECCC recruitment most of its staff, and had its Executive Director (ED) selected by the ECCC GB. The ECCC moved to its temporary offices in Bucharest in May 2023, and advanced towards financial autonomy. Overall, European Commission's (EC) services continued cooperating closely with all Member States (MS), and ENISA.

Until the ECCC reaches sufficient operational capacity and financial autonomy, EC services continue acting on behalf of the ECCC, contributing with the EC's own resources. This includes preparing DEP and HEP work programmes, launching and evaluating calls for proposals for both programs, and managing the projects selected for funding. The ECCC started to take over some of these tasks as its resources increased during the second part of 2023.

During the period covered by this SPD (2024-2026), the ECCC and the NCCs are expected to deliver fully on their mission and objectives regarding cybersecurity investment, innovation and uptake thus contributing to make the EU more cyber resilient and prosperous.

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) is a European Union (EU) body established by Regulation (EU) 2021/887[1] 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 pursue measures in support of industrial technologies and in the domain of research and innovation. The ECCC[2] is the EU's main vehicle to pool investment in cybersecurity research, technology and industrial development, and to implement relevant projects and initiatives, together with the Network of NCCs and in support of the Cyber Community and relevant stakeholders. The ECCC will be in charge of managing EU financial resources dedicated to cybersecurity under DEP[3] and HEP[4] and other EU programmes where appropriate, as well as additional contributions from Member States.

The ECCC is developing and implementing, with the Network of NCCs, industry and the cybersecurity technology community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular small and medium-sized enterprises (SMEs). The ECCC and the Network contribute to Europe's technological sovereignty and open strategic autonomy through joint investment in strategic cybersecurity projects. More concretely, the ECCC and the Network of NCCs have the mission[5] 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

[1] 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).

[2] https://cybersecurity-centre.europa.eu/index_en.

[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] Article 3 of the Regulation.

- 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 the Regulation[6], 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;
- 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 ICT infrastructure and services** required to fulfil its tasks.

With regards to the ECCC's **tasks**[7]:

- the ECCC supported by the Network, will make strategic investment decisions and pool resources from the EU, its 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.

[6] Article 4 of the Regulation.

[7] Article 5 of the Regulation.

- 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.

I. GENERAL CONTEXT

The "*EU's Cybersecurity Strategy for the Digital Decade"*[8] outlines a strong 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[9] on the Joint Communication to the European Parliament and the Council entitled "*The EU's Cybersecurity Strategy for the Digital Decade*", achieving strategic autonomy while preserving an open economy is a key objective of the EU in order to self-determine its 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.

This 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 ongoing support for technical assistance and cooperation between MS for capacity-building purposes.

As highlighted in the Nevers Call[10], 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 conclusions[11] 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 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

[8] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.

[9] Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade (6722/21).

[10] 'Nevers Call to Reinforce the EU's Cybersecurity Capabilities'. Informal Meeting of the Telecommunications Ministers. Nevers, March 9, 2022.

[11] https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/.

development of shared situational awareness. This includes stronger inter-agency cooperation among ENISA, CERT-EU and Europol in assessing the threat landscape. Moreover, the political agreement on the NIS Directive 2[12] provides a legal basis for the CyCLONe network of MS cyber agencies plus, in case of risks for the internal market, the EC to participate in crisis management coordination and situational awareness, is a further essential step towards solidarity and mutual assistance.

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 revised NIS Directive (NIS 2 Directive), for which the co-legislators reached a political agreement in May 2022. The new Directive will raise 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)[13]. 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 manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions allowing 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, which are now under consideration by the legislators.

- **European Cybersecurity certification schemes**. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act[14] aims at creating market-driven and least fragmented EU certification schemes and increasing trust in “cybersecurity-by-design” ICT products, services, and processes. The first European Cybersecurity Certification scheme was adopted in 2023, the Common Criteria-based European cybersecurity certification scheme (EUCC), and two other schemes are still 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.

[12] 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.

[13] 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.

[14] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

- **EU 5G Toolbox.** The EU 5G Toolbox[15], which is currently being implemented at EU and national level, 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')[16], which will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces. Moreover, in 2023 the NIS Cooperation Group also adopted a report on the status of implementation of the EU 5G Toolbox.

- **EU funding in the 2021-2027 Multiannual Financial Framework.** In 2022 and 2023 funding was provided for projects on cybersecurity deployment under the Digital Europe programme, 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.

- **Cooperation on cyber detection, analysis and sharing.** In the face of the growing number and impact of cybersecurity incidents, the EU Cybersecurity Strategy stresses the urgent need to improve our collective detection capacities. A lot of potential for improving detection of cyber threats and incidents can come through creating, reinforcing and connecting relevant entities such as Security Operation Centres (SOCs), Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), Information Sharing and Analysis Centres (ISACs), as well as sharing of cyber threat intelligence across the EU. The ECCC will play a central role in capacity building (e.g., through grants under the Digital Programme), and by taking on a central role in joint procurement with MS, with the aim to set up several cross-border platforms for pooling data on cyber threats between several MS.

- **EU Cyber Solidarity Mechanism.** In 2023 the EC adopted a legislative proposal on an EU Cyber Solidarity Mechanism, including legislative changes to DEP: (1) to strengthen common EU detection, situational awareness and response capabilities. (2) to support testing of critical entities for potential vulnerabilities based on EU risk assessments (3) to gradually build an EU-level cyber reserve with services from trusted private providers. This support 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 a policy and support measures to promote cyber skills.

[15] 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.

[16] 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.

Within this broader framework of EU policy priorities in cybersecurity, 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 SOCs and other relevant entities in the EU. 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 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, which will benefit from a more systematic, inclusive and strategic collaboration, having regard to the cohesion of the EU and all of its MS.

The ECCC, the Network and the Community are intended to benefit from the experience and the broad representation of relevant stakeholders built through the public-private partnership on cybersecurity between the EC and the European Cyber Security Organisation (ECSO) as well as from the lessons learnt from relevant projects[17] under Horizon 2020.

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.

In general, the multiannual work programme shall be reflecting the EU's policy priorities and the Agenda[18], while containing common, industrial, technology and research priorities which are based on the needs identified by MS in cooperation with the Community and which require the focus of EU financial support, including key technologies and domains for developing the EU's own capabilities in cybersecurity (*Article 13 of the Regulation*).

[17] CONCORDIA, ECHO, SPARTA and CyberSec4Europe.

[18] The Agenda, as defined in Article 2 point (8) of the Regulation, means "*a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and strategic priorities for the Competence Centre's activities and is not binding with respect to decisions to be taken on the annual work programmes*".

The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

II. MULTI-ANNUAL PROGRAMMING 2024 – 2026

II.1. MULTI-ANNUAL WORK PROGRAMME

The Activities for the Multiannual Work Programme 2024-2026 of the ECCC fall under the following four (4) main objectives:

- **Objective #1:** Consolidate financial and operational autonomy

  Activities covered under this objective were predominant in the first three SPDs of the ECCC (2021-2023, 2022-2024 and 2023-2025). They are expected to decrease in proportion to the total number of activities after the ECCC reaches its financial autonomy.

  Key tasks and related decisions cover notably the following areas:

  - Governance and management of the ECCC:
    - Confirmation of the ED further to successful probation period
    - Organise the selection and appointment of members of the Strategic Advisory Group (SAG)
    - Programming documents
    - Implement public communication and dissemination policy
    - Reports from the Accounting Officer
    - Assess initial operations and make necessary adjustments
  - Infrastructure:
    - Move in ECCC permanent premises and make necessary adjustments to ensure optimal conditions for staff
    - Work closely and collaborate with the host MS to receive optimal support and adequate implementation of the Host Agreement
    - Ensure on-boarding of IT tools and other logistics aspects
  - Staff:
    - Selection and recruitment of new staff members
    - Management of staff
    - Development of necessary functions and developing capacities
    - Growth and adaptation of internal structure
    - Integration and training
    - Support the integration of new staff members in Bucharest

- **Objective #2:** Implement DEP and, where relevant, HEP

For this Work Programme, the main funding sources foreseen will come from DEP. The estimated budget for ECCC in the Cybersecurity part of DEP during the 2-year period 2023-2024 is approximately EUR 375 million.

The adoption by the EC of the future DEP work programme will be a major milestone during this period. Key tasks will be the evaluation of the calls for proposals, the signature of grants and procurements, and managing projects receiving DEP funding. The ECCC will entirely manage these tasks, independently from EC services, after reaching full financial autonomy. Moreover, the EC services will transfer the responsibility of managing existing DEP projects to the ECCC.

In line with Article 5.5 of the ECCC Regulation, the EC may decide to delegate to the ECCC the implementation of HEP in the area of cybersecurity (proposal evaluation, management of grants, etc.)

- **Objective #3:** Develop, implement and monitor the Agenda of the ECCC, the multiannual work programme and the annual work programme

The Agenda of the ECCC, adopted by the Governing Board (GB) in 2023 based on input from a dedicated Working Group of the GB, is a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out recommendations for the development and growth of European cybersecurity capabilities and priorities for the ECCC's activities[19]. The GB will monitor the implementation and ensure the dissemination of the first Agenda.

The Agenda will also guide the drafting of the annual and multiannual work programmes of the ECCC.

The annual work programme of the ECCC will define, in accordance with the 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, MS may contribute to HEP. Should that be the case, the ECCC will decide on the work programme for HEP to the extent of MS contributions. Accordingly, the HEP, and also the DEP, work programmes will include, where relevant, joint actions between the ECCC and MS, in line with Articles 2(5) of the ECCC Regulation.

When drafting the annual work programme and the multiannual work programme, the ECCC will take into account the adopted Strategic Agenda of the ECCC and the input received from the NCCs, the Community and its working groups, the SAG, and ENISA.

- **Objective #4:** Coordinate and further develop the Network of NCCs and the Cybersecurity Competence Community

The ECCC should facilitate and coordinate the work of the Network of NCCs. The Network should be composed of one NCC from each MS[20]. Over the course of 2022, seven Working Groups of the

[19] Article 2 point (8) of the Regulation.

[20] 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

GB were established, of which several aim to providing support to the function 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.
- WG5-Cyber Skills.
- WG6-Collaboration with Ukraine.
- WG7-Security Operation Centres (SOCs).

The Working Groups and their chairs shall provide strategic advice on the Agenda, the annual work programme and the multiannual work programme, in accordance with the rules of procedure of the GB. The WGs will organise activities (e.g. public consultations open to all public and private stakeholders who have an interest in the area of cybersecurity), in order to collect input relevant for the designing of the Agenda and to provide advice to the ED and the GB.

The ECCC aims to stimulate and support the long-term strategic cooperation and coordination of the activities of the Community. The latter gathers a large, interdisciplinary and diverse group of European stakeholders involved in cybersecurity technology. The Community includes academic and research entities, industries and the public sector. It is open to other EU and MS bodies (including ENISA and others) and relevant stakeholders (e.g. ECSO). Relevant activities should increase the visibility of EU cybersecurity expertise, products and services.

According to the Regulation, the assessment of Community members is made by the NCCs, and the NCCs should cooperate through the Network and align the procedures they follow for assessing entities. Over the course of 2022, the GB adopted a decision on guidelines for assessing and registering entities as members of the Community[21] to provide support to NCCs and ensure a minimum level of alignment.

The SAG shall regularly advise the ECCC in respect of the performance of the ECCC's activities and shall ensure communication with the Community and other relevant stakeholders. The Community, in particular through the SAG, should provide input to the activities of the ECCC, to the multiannual work programme and to the annual work programme.

In the context of the NCCs and the Community, it is important to increase the visibility for EU cybersecurity expertise, products and services. Based on the efforts of the NCCs, the four pilot projects, local/regional efforts in MS, and the "Cybersecurity Atlas"[22] platform, the ECCC will seek to bring together resources and knowledge on the cybersecurity market. This may include interconnecting relevant tools and platforms. The NCCs have a primary role in providing, facilitating,

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.

[21] Decision No GB/2022/7 of the ECCC Governing Board on the Community membership and registration guidelines.

[22] European Cybersecurity Atlas | Cybersecurity Atlas (europa.eu).

and collecting relevant information. This enables the creation of market intelligence and insights, as well as provided an EU-wide overview of the cybersecurity ecosystem. Further work is needed to build on these first efforts, and to keep updating and upgrading this EU cybersecurity ecosystem.

The Cybersecurity Atlas will continue its pivotal role as a knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts, and also present NCC activities and information at European level. NCCs should continue notifying the Community members registration to the ECCC, using the Atlas for this purpose. Front-end solutions and other tools should be updated according to the identified needs during the first phase of the registration.

Operational support to the mission of the NCCs, and their functioning as a network, and to the European Cybersecurity Competence Community, including the organization of industrial matchmaking and partnering events, started to be provided from early 2023 through the European Cybersecurity Community support action (“ECCO”). The contract for this action was signed in December 2022, further to the open procurement of the DEP Call ‘Cybersecurity Community Support’ (CNECT/2022/OP/0033).

The EC, the European Investment Bank (EIB) and the European Investment Fund will look at options to create additional private investment opportunities in Cybersecurity through the InvestEU instrument, based on a market study recently performed by the EIB. The ECCC will look for synergies with the EIB whenever relevant.

II.2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2024 – 2026

II.2.1.OVERVIEW OF THE PAST AND CURRENT SITUATION

The Regulation entered into force on 28 June 2021. Since then, DG CONNECT of the EC has been working on the establishment of the ECCC. Since then, preparatory actions, notably HR-related rules, were adopted which enabled the recruitment of over 20 staff members by end of 2023. The Accounting Officer and Data Protection officer were shared with ENISA from 2023 (see section below on synergies).

The EC services continued acting on behalf of the ECCC until the ECCC reached full financial autonomy.

II.2.2.OUTLOOK FOR THE YEARS 2024 – 2026

This work programme aims to provide the ECCC activities with the necessary legal and budgetary resources during its establishment and initial operation phase. Selection and recruitment of the initial staff members of the ECCC which started in 2022, and increased significantly in 2023, will continue during 2024 and the following years, in order for the ECCC to step up its operations. The long-term ED was selected in 2023. During 2024, all ECCC staff is expected to be recruited. In 2024, it is also expected to take over the permanent premises of the ECCC.

From 2024, the most important actions requiring legal and budgetary resources will relate to ECCC’s responsibilities regarding management of DEP funding.

The adoption of this Work Programme 2024 will enable the ECCC to:

- Continue the recruitment of staff with the targets indicated in Section II.2.3.
- Gradually take over the implementation of the DEP (and HEP, if applicable), including the evaluation of the calls for proposals, the signature of grants and the management of the projects.
- Adopt, implement and monitor the Agenda of the ECCC, which shall guide the drafting of the next annual and multi-annual work programmes of the ECCC.
- Fulfil its mandate as described in the Mission Statement by performing the activities described in this Work Programme.
- Support the mission of the NCCs and their functioning as a Network of NCCs, as well as the Cybersecurity Competence Community.

II.2.3.RESOURCE PROGRAMMING FOR THE YEARS 2024 – 2026

Financial Resources

As defined in the Regulation, the ECCC shall in principle be funded by the EU, while joint actions shall be funded by the EU and by voluntary contributions from MS.

Generally, 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.
For 2024, all budget projected below will come from DEP appropriations.

Table 1

	2024	2025	2026
Total estimated revenue for ECCC (EUR) [23]	218.831.127,16	125.766.680,63	126.032.746,58

Human Resources

In 2023 some of the staff have started to work in the temporary ECCC offices in Bucharest.
The first staff recruitments took place in 2022 with further recruitments made in 2023, including the selection of the ED. Recruitment will continue in 2024 and in the following years.
The Staff Regulations and Conditions of Employment apply to the staff of the ECCC.

[23] EFTA percentage used 3,58%.

II.2.4.STRATEGY FOR ACHIEVING EFFICIENCY GAINS

The ECCC is committed to continuously implement measures to obtain efficiency gains in all activities.

Whenever possible, the ECCC will continue seeking synergies and the most efficient ways of action. On July 2022, the ECCC became an ad hoc member of the EU Agencies Network (EUAN, of which full membership requires financial autonomy), which gives access to a Network of agencies, JUs (Joint Undertakings) and other EU bodies, and the opportunity to exchange knowledge and best practices on horizontal issues for EU 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)[24] and might benefit from such arrangements at a later stage.

The following table summarises the expected results:

Objectives	Expected results
Premises/Infrastructure	Handover of the Permanent Premises of the ECCC in Bucharest
	Ensure the necessary IT infrastructure for the ECCC operations
Governance and management (structure, legal & procedural framework)	Assessment of the ECCC ED further to a probation period.
	Adoption of programming documents
	Support the registration of members of the EU Cybersecurity Competence Community
	Implementation of a public communication and dissemination policy
	Implementation of the Internal control framework
	Implementation of the Anti-fraud and anti-corruption strategy
	Implementation of the prevention, identification and resolution of conflicts of interest in respect of its members, bodies and staff, including the ED and the GB members, and SAG members
	Implementation of the ECCC’s Security rules
Staff	Implementation of the secondment of SNEs
	Approval of working arrangements between the ECCC and EU institutions, bodies, offices and agencies (e.g. ENISA, EEAS, JRC, REA, HADEA, Europol, EDA) and international organisations, where relevant
	Continue the adoption of further HR-related legal framework (e.g. implementing rules to the Staff Regulations and to the Conditions of Employment of Other Servants of the EU)
	Continue selection and recruitment of more staff members of the ECCC
	Management and integration of newly recruited staff, including necessary trainings

[24] 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.

III. WORK PROGRAMME 2024

III.1. EXECUTIVE SUMMARY

The overall objectives described for the multiannual outlook 2024-2026 are elaborated in the activities indicated in this section. The priority for 2024 are additional recruitment of staff members, and completing the fulfilment of administrative and operational capabilities of the ECCC so that the ECCC can operate autonomously, notably regarding DEP implementation. Other activities will include the monitoring of the Agenda of the ECCC, the full operation of the Network of NCCs and of the Cybersecurity Competence Community. Also possibly the implementation of the HEP, further to the delegation from EC services, and of joint actions supported with MS contributions.

III.2. ACTIVITIES

II.2.1. ACTIVITY DOMAIN #1: Legal and operational activities of the ECCC

The activities described under this chapter are related to Objective #1 of the Multiannual Work Programme: "*Consolidate the legal and operational autonomy of the ECCC*".

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. In particular, one key task for the ECCC will be to implement part of the DEP (see activity 2 below).

The administrative budget of the ECCC will cover the expenditures required to accomplish the activities described in this section. These may include, but are not limited to: reimbursement of travel expenses of GB members, expenses for contracting staff as well as integrating and training that staff, salaries, costs related to procurement and integration of IT systems. A smooth transition towards the new accounting system of the EC ("Summa") should be ensured, including the alignment of treasury services with the new platform.

The ECCC permanent premises is expected to be ready to accommodate new employees by end of 2024, including the provision of the necessary IT equipment and services.

See also chapter 2.4 (under Section II) on strategy for efficiency gains.

II.2.2. ACTIVITY DOMAIN #2: Implementation of Digital Europe and Horizon Europe programmes

The actions under Specific Objective 3 (Cybersecurity and Trust) of the DEP will be implemented primarily through the ECCC and the Network of NCCs.

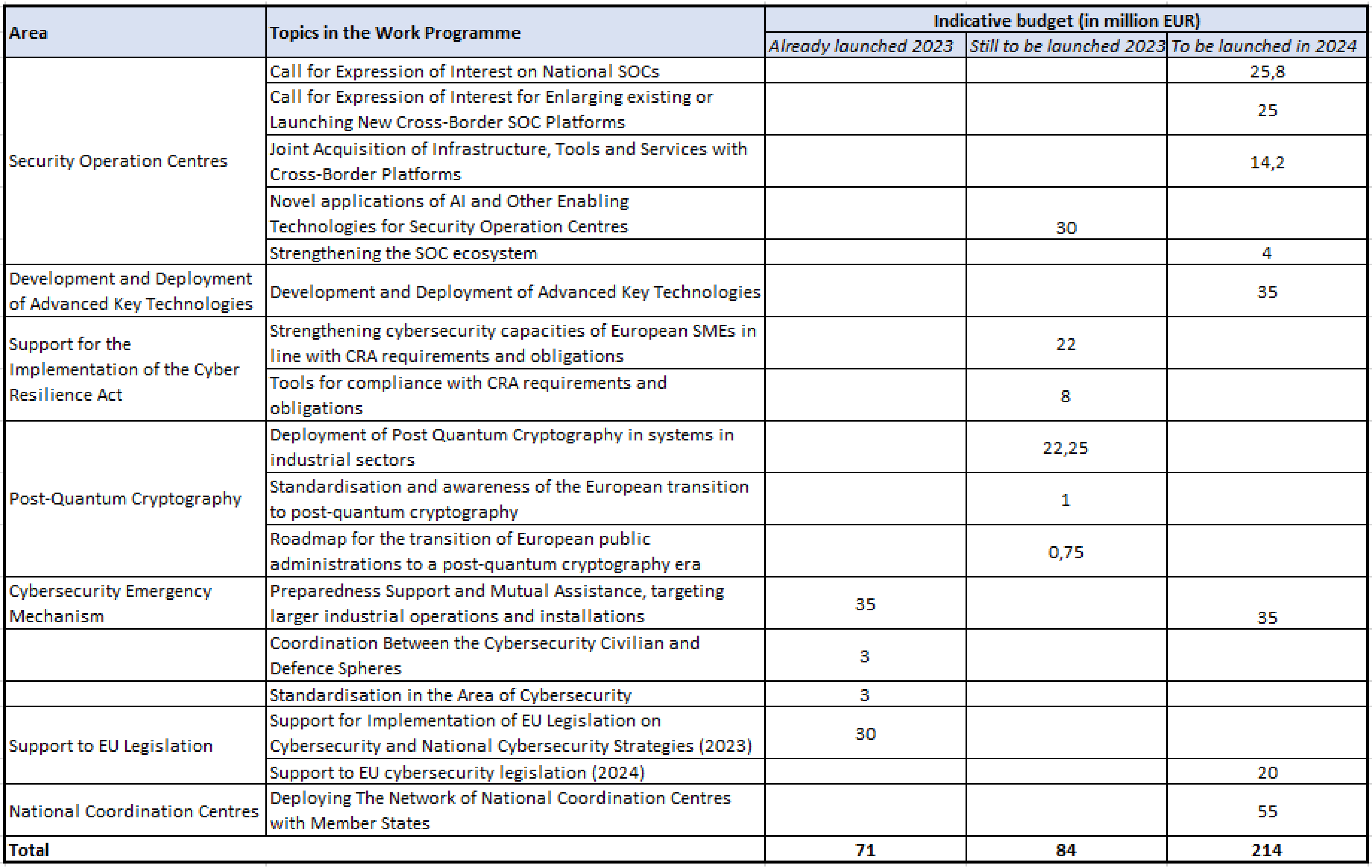
This includes the management of projects awarded under the first and second calls of the DEP work programme 2021-2022, the evaluation of proposals under the first call of the DEP work programme

2023-2024 and the signature of grants and the management of the proposals retained for funding under that call.

Important actions to be undertaken in this activity area in 2024 include the following:

Objectives	Expected results
Programme implementation	ECCC implementing DEP calls for WP 2023-2024 (take financing decisions, launch calls, organise evaluations, conclude grant agreements)
	Where necessary, adopting guidelines for proposals and projects, model grant agreement, methodology to calculate MS in-kind contribution
	Identify possible Joint Actions to be supported by contributions from some MS and by EU budget from DEP or HEP
	Possibly manage part of HEP further to EC services' delegation.

The following table summarises the WP 2023-2024 calls and topics, where out of 375 mil EUR, 214 are dedicated to calls during 2024:



Area	Topics in the Work Programme	Indicative budget (in million EUR)		
		Already launched 2023	*Still to be launched 2023*	*To be launched in 2024*
Security Operation Centres	Call for Expression of Interest on National SOCs			25,8
	Call for Expression of Interest for Enlarging existing or Launching New Cross-Border SOC Platforms			25
	Joint Acquisition of Infrastructure, Tools and Services with Cross-Border Platforms			14,2
	Novel applications of AI and Other Enabling Technologies for Security Operation Centres		30	
	Strengthening the SOC ecosystem			4
Development and Deployment of Advanced Key Technologies	Development and Deployment of Advanced Key Technologies			35
Support for the Implementation of the Cyber Resilience Act	Strengthening cybersecurity capacities of European SMEs in line with CRA requirements and obligations		22	
	Tools for compliance with CRA requirements and obligations		8	
Post-Quantum Cryptography	Deployment of Post Quantum Cryptography in systems in industrial sectors		22,25	
	Standardisation and awareness of the European transition to post-quantum cryptography		1	
	Roadmap for the transition of European public administrations to a post-quantum cryptography era		0,75	
Cybersecurity Emergency Mechanism	Preparedness Support and Mutual Assistance, targeting larger industrial operations and installations	35		35
	Coordination Between the Cybersecurity Civilian and Defence Spheres	3		
	Standardisation in the Area of Cybersecurity	3		
Support to EU Legislation	Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2023)	30		
	Support to EU cybersecurity legislation (2024)			20
National Coordination Centres	Deploying The Network of National Coordination Centres with Member States			55
Total		**71**	**84**	**214**

II.2.3. ACTIVITY DOMAIN #3: adoption of the agenda, the multiannual work programme and the annual work programme

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 strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector, and strategic priorities for the ECCC's activities, and is not binding with respect to decisions to be taken on the annual work programmes. The Agenda focuses notably on retaining and developing essential cybersecurity research and technological capacities to secure the network and information systems of citizens and businesses, and in particular to protect critical network and information systems and provide key cybersecurity services.

The 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 annual work programme of the ECCC will define, in accordance with the Agenda and the multiannual work programme, the priorities for the DEP and, to the extent that they are co-financed by the MS, also the priorities for the HEP. For the rest, EC services will take into account the input from the Agenda when preparing the HEP WP. These work programmes will include, where relevant, joint actions between the ECCC and MS.

Important actions to be undertaken in this activity area during the period which completion is expected over the course of 2024 include the following:

Objective	Expected results
Agenda	Adoption of the next agenda, following consultation with all relevant actors (EC, NCCs, Community, ENISA, SAG)
	Monitoring the implementation of the previous Agenda
	Dissemination of the Agenda to relevant stakeholders, including the HEP Program Committee
Multiannual work programme & Annual work programme	Development, adoption and monitoring of the multiannual work programme and the annual work programme

II.2.4. ACTIVITY DOMAIN #4: Activities related to the NCCs and the cybersecurity competence community

The Network of NCCs is composed of all NCCs that has been notified to the GB by the MS (Article 6.7 of the Regulation). They function as contact points at the national level for the Cybersecurity Competence Community and the ECCC (Article 7.1(a) of the Regulation). They are the interfaces of the cybersecurity community in their country. They will also provide support to carry out actions under this Regulation, and they can pass on financial support to local actors (Article 7.1(f) of the Regulation).

By 2023, most of the MSs have notified to the GB the entities acting as their NCCs. Since the ECCC started to operate, seven dedicated Working Groups of the GB were established with the aim of providing support to the function of the NCCs Network:

- WG1-Community membership and registration.

[25] Article 13.3(a) of the Regulation. The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

- 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).

In 2024, the Network of NCCs will have regular meetings and interactions, fulfilling its tasks as set out in the founding Regulation, and functioning as an integrated Network.

The ECCC provides operational support to the NCCs, and their functioning as a Network, and to the European Cybersecurity Competence Community. A dedicated Coordination and Support Action procured through the 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, stimulate collaborations, and link the Cybersecurity Competence Community with the ECCC and the NCCs Network. EC services monitor this action and leases with the contractor.

The cybersecurity 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. 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”.

Moreover, in 2024 Iceland, Liechtenstein and Norway will be 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 this activity area in 2024 include the following:

Objective	Expected results
Network of National Coordination Centres	Completion of the setting-up of the Network and smooth functioning as an integrated Network
	Implement and update of 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 the evolution of the associated tools Support new Community registrations, develop relevant tools and stimulate activities
	Community participation to the activities of the working groups, where relevant
	Develop an EU “cybersecurity market observatory” in coordination with ENISA

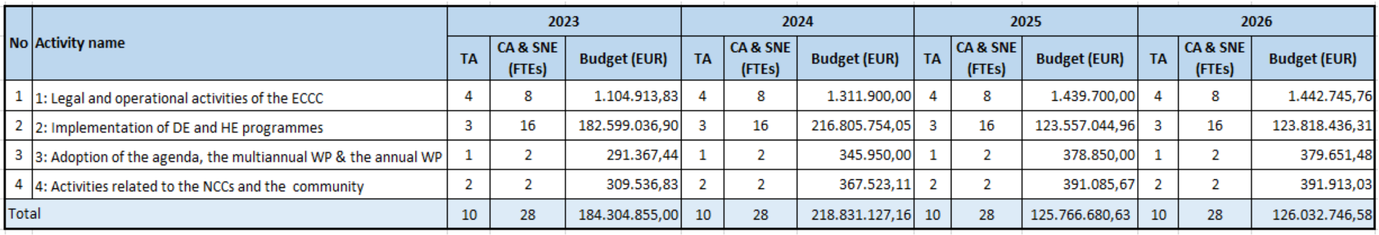
ANNEXES

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 2024 – 2026

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	2023			2024			2025			2026		
		TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)
1	1: Legal and operational activities of the ECCC	4	8	1.104.913,83	4	8	1.311.900,00	4	8	1.439.700,00	4	8	1.442.745,76
2	2: Implementation of DE and HE programmes	3	16	182.599.036,90	3	16	216.805.754,05	3	16	123.557.044,96	3	16	123.818.436,31
3	3: Adoption of the agenda, the multiannual WP & the annual WP	1	2	291.367,44	1	2	345.950,00	1	2	378.850,00	1	2	379.651,48
4	4: Activities related to the NCCs and the community	2	2	309.536,83	2	2	367.523,11	2	2	391.085,67	2	2	391.913,03
Total		10	28	184.304.855,00	10	28	218.831.127,16	10	28	125.766.680,63	10	28	126.032.746,58

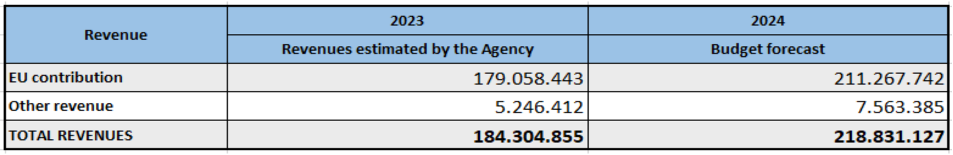
ANNEX III. FINANCIAL RESOURCES 2024 - 2026[26]

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	2023	2024
	Revenues estimated by the Agency	Budget forecast
EU contribution	179.058.443	211.267.742
Other revenue	5.246.412	7.563.385
TOTAL REVENUES	**184.304.855**	**218.831.127**

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					
	Estimated by ECCC for 2023	2024		VAR 2024/2023 (%)	Envisaged 2025	Envisaged 2026
		Agency request	Budget forecast			
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	**179.058.443,00**	**211.267.742,00**		**18%**	**121.419.850,00**	**121.676.720,00**
- 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**		**44%**	**4.346.830,63**	**4.356.026,58**
- Of which EEA/EFTA (excl. Switzerland)	*5.246.412,00*	*7.563.385,16*		**44%**	*4.346.830,63*	*4.356.026,58*
- 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**		**19%**	**125.766.680,63**	**126.032.746,58**

The 2023 EFTA percentage for DEP is2.93 %, while from 2024 onwards is 3.58%.

Commitment appropriations

Table 2: Commitment appropriations

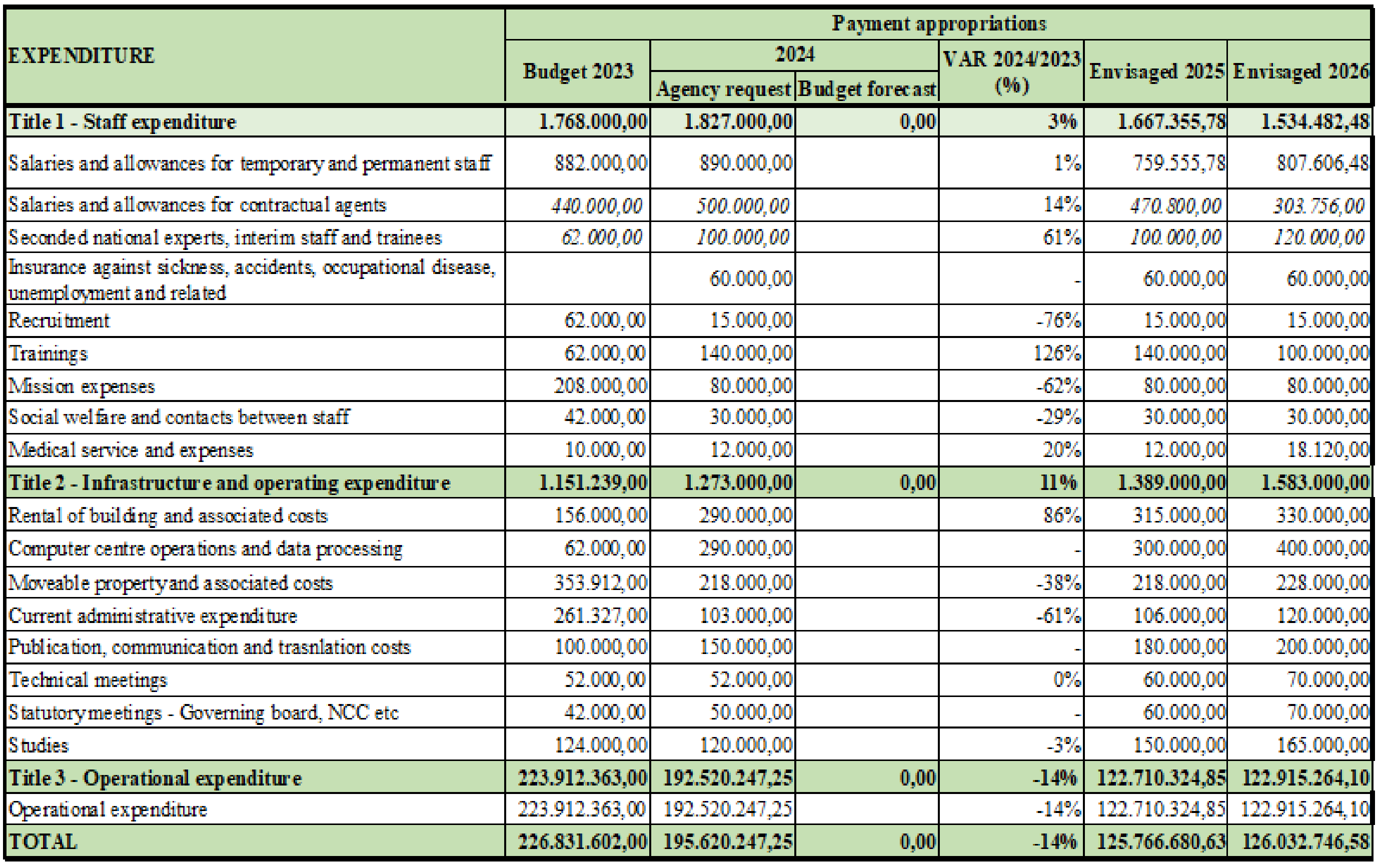
Expediture	2023		2024	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1 - Staff expenditure	1.768.000	1.768.000	1.827.000	1.827.000
Title 2 - Infrastructure and operating expenditure	1.151.239	1.151.239	1.273.000	1.273.000
Title 3 - Operational expenditure	181.385.616	223.912.363	215.731.127	192.520.247
TOTAL Expediture	**184.304.855**	**226.831.602**	**218.831.127**	**195.620.247**

EXPENDITURE	Commitment appropriations					
	Budget 2023	2024		VAR 2024/2023 (%)	Envisaged 2025	Envisaged 2026
		Agency request	Budget forecast			
Title 1 - Staff expenditure	**1.768.000,00**	**1.827.000,00**	**0,00**	**3%**	**1.667.355,78**	**1.534.482,48**
Salaries and allowances for temporary and permanent staff	882.000,00	890.000,00		1%	759.555,78	807.606,48
Salaries and allowances for contractual agents	440.000,00	500.000,00		14%	470.800,00	303.756,00
Seconded national experts, interim staff and trainees	62.000,00	100.000,00		61%	100.000,00	120.000,00
Insurance against sickness, accidents, occupational disease, unemployment and related		60.000,00		-	60.000,00	60.000,00
Recruitment	62.000,00	15.000,00		-76%	15.000,00	15.000,00
Trainings	62.000,00	140.000,00		126%	140.000,00	100.000,00
Mission expenses	208.000,00	80.000,00		-62%	80.000,00	80.000,00
Social welfare and contacts between staff	42.000,00	30.000,00		-29%	30.000,00	30.000,00
Medical service and expenses	10.000,00	12.000,00		20%	12.000,00	18.120,00
Title 2 - Infrastructure and operating expenditure	**1.151.239,00**	**1.273.000,00**	**0,00**	**11%**	**1.389.000,00**	**1.583.000,00**
Rental of building and associated costs	156.000,00	290.000,00		86%	315.000,00	330.000,00
Computer centre operations and data processing	62.000,00	290.000,00		-	300.000,00	400.000,00
Moveable property and associated costs	353.912,00	218.000,00		-38%	218.000,00	228.000,00
Current administrative expenditure	261.327,00	103.000,00		-61%	106.000,00	120.000,00
Publication, communication and trasnlation costs	100.000,00	150.000,00		-	180.000,00	200.000,00
Technical meetings	52.000,00	52.000,00		0%	60.000,00	70.000,00
Statutory meetings - Governing board, NCC etc	42.000,00	50.000,00		-	60.000,00	70.000,00
Studies	124.000,00	120.000,00		-3%	150.000,00	165.000,00
Title 3 - Operational expenditure	**181.385.616,00**	**215.731.127,16**	**0,00**	**19%**	**122.710.324,85**	**122.915.264,10**
Operational expenditure	*181.385.616,00*	*215.731.127,16*		19%	*122.710.324,85*	*122.915.264,10*
TOTAL	**184.304.855,00**	**218.831.127,16**	**0,00**	**19%**	**125.766.680,63**	**126.032.746,58**

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	2024		VAR 2024/2023 (%)	Envisaged 2025	Envisaged 2026
		Agency request	Budget forecast			
Title 1 - Staff expenditure	**1.768.000,00**	**1.827.000,00**	**0,00**	**3%**	**1.667.355,78**	**1.534.482,48**
Salaries and allowances for temporary and permanent staff	882.000,00	890.000,00		1%	759.555,78	807.606,48
Salaries and allowances for contractual agents	*440.000,00*	*500.000,00*		14%	*470.800,00*	*303.756,00*
Seconded national experts, interim staff and trainees	*62.000,00*	*100.000,00*		61%	*100.000,00*	*120.000,00*
Insurance against sickness, accidents, occupational disease, unemployment and related		60.000,00		-	60.000,00	60.000,00
Recruitment	62.000,00	15.000,00		-76%	15.000,00	15.000,00
Trainings	62.000,00	140.000,00		126%	140.000,00	100.000,00
Mission expenses	208.000,00	80.000,00		-62%	80.000,00	80.000,00
Social welfare and contacts between staff	42.000,00	30.000,00		-29%	30.000,00	30.000,00
Medical service and expenses	10.000,00	12.000,00		20%	12.000,00	18.120,00
Title 2 - Infrastructure and operating expenditure	**1.151.239,00**	**1.273.000,00**	**0,00**	**11%**	**1.389.000,00**	**1.583.000,00**
Rental of building and associated costs	156.000,00	290.000,00		86%	315.000,00	330.000,00
Computer centre operations and data processing	62.000,00	290.000,00		-	300.000,00	400.000,00
Moveable propertyand associated costs	353.912,00	218.000,00		-38%	218.000,00	228.000,00
Current administrative expenditure	261.327,00	103.000,00		-61%	106.000,00	120.000,00
Publication, communication and trasnlation costs	100.000,00	150.000,00		-	180.000,00	200.000,00
Technical meetings	52.000,00	52.000,00		0%	60.000,00	70.000,00
Statutorymeetings - Governing board, NCC etc	42.000,00	50.000,00		-	60.000,00	70.000,00
Studies	124.000,00	120.000,00		-3%	150.000,00	165.000,00
Title 3 - Operational expenditure	**223.912.363,00**	**192.520.247,25**	**0,00**	**-14%**	**122.710.324,85**	**122.915.264,10**
Operational expenditure	223.912.363,00	192.520.247,25		-14%	122.710.324,85	122.915.264,10
TOTAL	**226.831.602,00**	**195.620.247,25**	**0,00**	**-14%**	**125.766.680,63**	**126.032.746,58**

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:

a. the remuneration (salaries and allowances) of the temporary and contractual staff in accordance with the Staff Regulations.
b. recruitment costs,
c. mission expenditure;
d. insurances and medical check-up of staff and associated analyses required;
e. 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:

f. Logistical costs – utility costs, furniture and equipment of Permanent office, office supplies etc.

g. IT infrastructure, equipment and data processing
h. Meeting costs – technical meetings and statutory meetings
i. Publications, communication and translation costs.
j. External studies

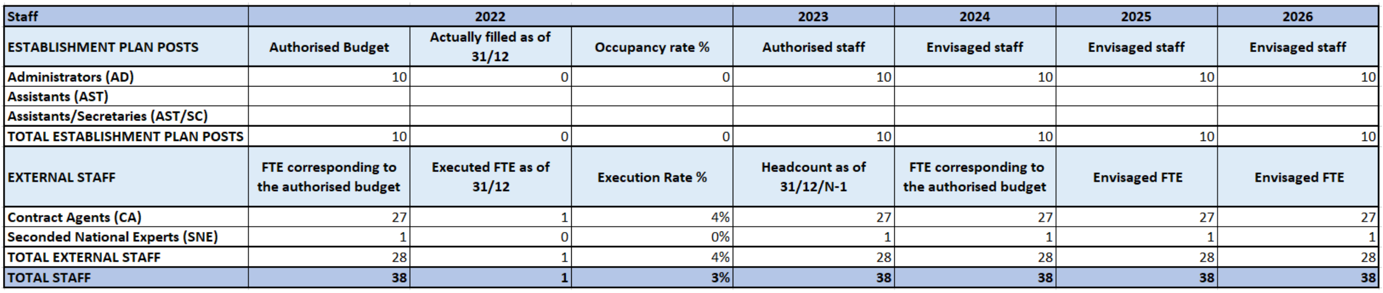
TITLE 3

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



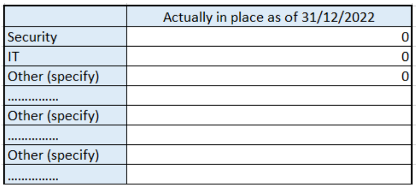
Staff	2022			2023	2024	2025	2026
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12	Occupancy rate %	Authorised staff	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (AD)	10	0	0	10	10	10	10
Assistants (AST)							
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	10	0	0	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	1	4%	27	27	27	27
Seconded National Experts (SNE)	1	0	0%	1	1	1	1
TOTAL EXTERNAL STAFF	28	1	4%	28	28	28	28
TOTAL STAFF	38	1	3%	38	38	38	38

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

Not applicable.

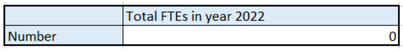
C. C. Other Human Resources

Structural service providers[27]



	Actually in place as of 31/12/2022
Security	0
IT	0
Other (specify)	0
……………	
Other (specify)	
……………	
Other (specify)	
……………	

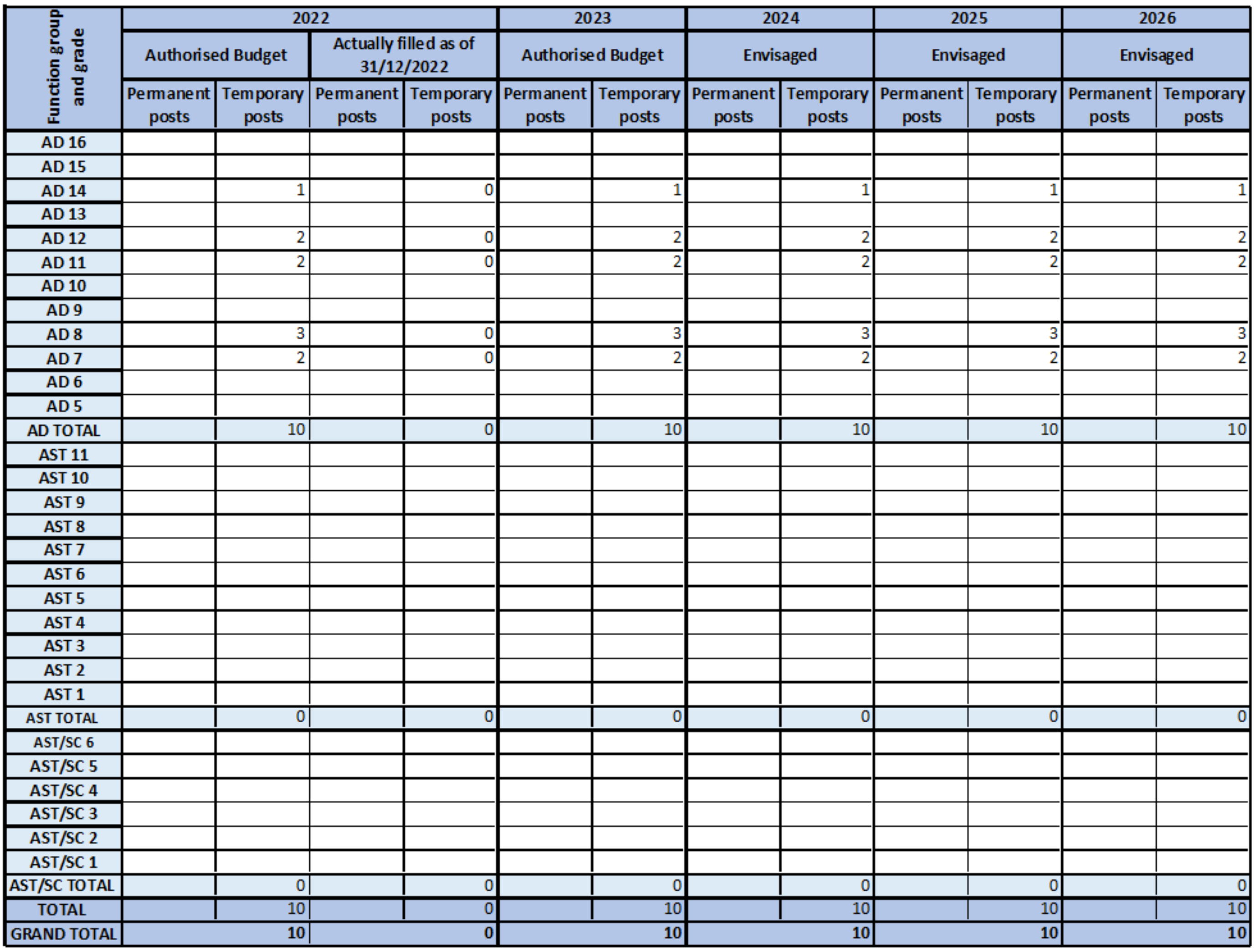
Interim workers



	Total FTEs in year 2022
Number	0

[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

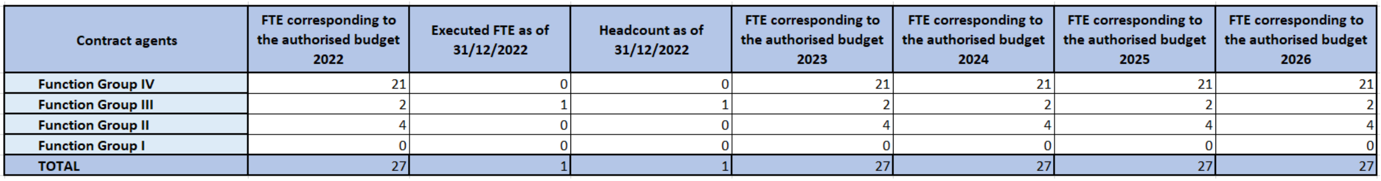
Table 2 – Multi-annual staff policy plan 2024, 2025, 2026



Function group and grade	2022				2023		2024		2025		2026	
	Authorised Budget		Actually filled as of 31/12/2022		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												
AD 12		2		0		2		2		2		2
AD 11		2		0		2		2		2		2
AD 10												
AD 9												
AD 8		3		0		3		3		3		3
AD 7		2		0		2		2		2		2
AD 6												
AD 5												
AD TOTAL		10		0		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		0		10		10		10		10
GRAND TOTAL	10		0		10		10		10		10	

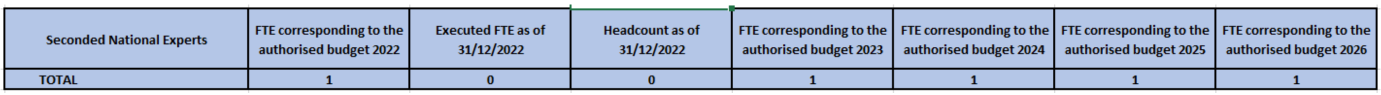
- External personnel

Contract Agents



Contract agents	FTE corresponding to the authorised budget 2022	Executed FTE as of 31/12/2022	Headcount as of 31/12/2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026
Function Group IV	21	0	0	21	21	21	21
Function Group III	2	1	1	2	2	2	2
Function Group II	4	0	0	4	4	4	4
Function Group I	0	0	0	0	0	0	0
TOTAL	27	1	1	27	27	27	27

Seconded National Experts



Seconded National Experts	FTE corresponding to the authorised budget 2022	Executed FTE as of 31/12/2022	Headcount as of 31/12/2022	FTE corresponding to the authorised budget 2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026
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.

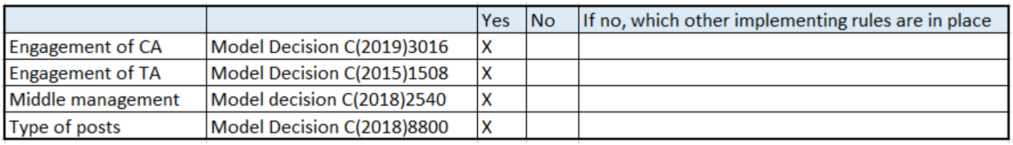
Number of inter-agency mobility year 2023 from and to the ECCC: 0.

ANNEX V. HUMAN RESOURCES QUALITATIVE

Due to limited data for the past years, part of the tables of this Annex (gender and geographical representation, evolution of management) will be filled in future SPDs.

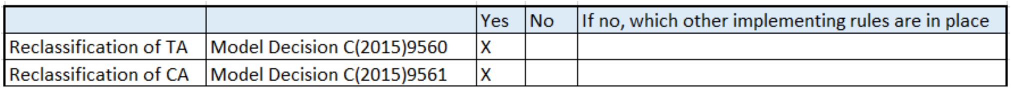
A. Recruitment policy

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].

D. Geographical Balance

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.

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.

[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.

ANNEX VIII. PRIVILEGES AND IMMUNITIES

Not applicable until hosting agreement is adopted.

ANNEX IX. EVALUATIONS

Not applicable in this Work Programme.

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.

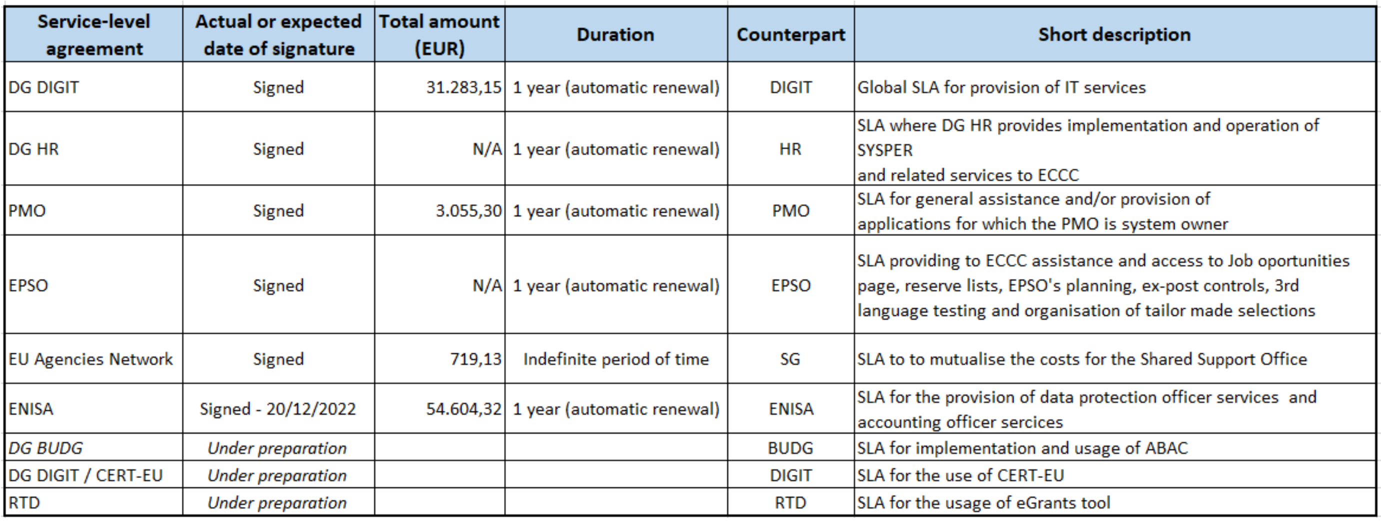
Until its full autonomy, the ECCC is operating based on the DG CONNECT's control management system, designed to provide reasonable assurance regarding the achievement of the five internal control objectives derived from the ECCC's Financial regulation as well as ensuring continuous improvement and the 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 during 2023. 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

Not applicable in this Work Programme.