Council of the
European Union

Brussels, 14 September 2018
(OR. en)

12104/18

Interinstitutional File:
2018/0328(COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	12 September 2018
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2018) 630 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

Delegations will find attached document COM(2018) 630 final.

Encl.: COM(2018) 630 final

EUROPEAN
COMMISSION

Brussels, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

As daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends on enhancing the ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.

In order to address the growing challenges, the Union has steadily increased its activities in the area, building on the 2013 Cybersecurity Strategy[1] and its goals and principles to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted its first measures in the area of cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council[2]on security of network and information systems.

In view of the fast evolving cybersecurity landscape in September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication[3] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks. The Joint Communication, building also on previous initiatives, outlined a set of proposed actions including, among others, reinforcing the European Union Agency for Network and Information Security (ENISA), creating a voluntary Union-wide cybersecurity certification framework to increase the cybersecurity of products and services in the digital world as well as a blueprint for quick, coordinated response to large scale cybersecurity incidents and crises.

In the Joint Communication, it was recognised that it is also in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services. The Union must be in a position to autonomously secure its digital assets and to compete on global cybersecurity market.

At the moment, the Union is a net importer of cybersecurity products and solutions and largely depends on non-European providers.[4] The cybersecurity market is globally a 600 billion EUR market that is expected to grow in the next five years on average by approximately 17% in terms of sales, number of companies and employment. However, in the

---

1 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

3 JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final

4 Draft Final Report on the Cybersecurity Market Study, 2018

top 20 of the leading cybersecurity countries from a market perspective, there are only 6 Member States[5].

At the same time, in the Union a wealth of expertise and experience in cybersecurity exists - more than 660 organisations from across the EU registered to the recent mapping of cybersecurity centres of expertise conducted by the Commission.[6] This expertise, if transformed into marketable products and solutions could allow the Union to cover the whole cybersecurity value-chain. Yet, the efforts of research and industrial communities are fragmented, lacking alignment, and a common mission, which hinders EU's competitiveness in this domain as well as its ability to secure its digital assets. The relevant cybersecurity sectors (e.g. energy, space, defence transport) and sub-domains are today insufficiently supported.[7] Synergies between the civilian and defence cybersecurity sectors are not fully exploited in Europe either.

The creation in 2016 of the Public-Private Partnership ('cPPP') on cybersecurity in the Union was a solid first step bringing together the research, industry and public sector communities to facilitate research and innovation in cybersecurity and within the limits of the 2014-2020 financial framework should result in good, more focused outcomes in research and innovation. The cPPP allowed industrial partners to express commitment about their individual spending on areas defined in the partnership's Strategic Research and Innovation Agenda.

However, the Union can pursue a much larger scale investment and needs a more effective mechanism which would build lasting capacities, pool efforts, competences and stimulate the development of innovative solutions responding to cybersecurity industrial challenges in the field of new multi-purpose technologies (e.g. artificial intelligence, quantum computing, blockchain and secure digital identities) as well as in critical sectors (e.g. transport, energy, health, financial, government, telecom, manufacturing, defence, space).

The Joint Communication considered the possibility of reinforcing Union cybersecurity capability through a network of cybersecurity competence centres with a European Cybersecurity Competence Centre at its heart. This would seek to complement the existing capacity building efforts in this area at Union and national level. The Joint Communication expressed the Commission's intention to launch an impact assessment in 2018 to examine the available options with a view to set up the structure. As a first step and to inform future thinking, the Commission launched a pilot phase under Horizon 2020 to help bring national centres together into a network to create a new momentum in cybersecurity competence and technology development.

The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."

---

5 Draft Final Report on the Cybersecurity Market Study, 2018

6 JRC Technical Reports: European Cybersecurity Centres of Expertise, 2018

7 JRC Technical Report: Outcomes of the Mapping Exercise (See Annex 4 and 5 for details)

The Council Conclusions[8] adopted in November 2017, called on the Commission to provide rapidly an impact assessment on the possible options and propose by mid-2018 the relevant legal instrument for the implementation of the initiative.

The Digital Europe Programme proposed by the Commission in June 2018[9] seeks to enlarge and maximise the benefits of digital transformation for European citizens and businesses in all relevant EU policy areas, reinforcing the policies and supporting the ambitions of the Digital Single Market. The programme proposes a coherent and overarching approach to ensuring the best use of advanced technologies and the right combination of technical capacity and human competence for the digital transformation – not only in the area of cybersecurity, but also as regards to smart data infrastructure, artificial intelligence, advanced skills and applications in industry and in areas of public interest. These elements are interdependent, mutually reinforcing and, when fostered simultaneously, can achieve the scale necessary to allow a data economy to thrive.[10] The *Horizon Europe Programme* [11].- the next EU R&I Framework programme also puts cybersecurity among its priorities.

In this context the present Regulation proposes the set-up of a European Cybersecurity Industrial, Technology and Research Competence with a network of National Coordination Centres. This made-for-purpose cooperation model should work as follows in order to stimulate the European cybersecurity technological and industrial ecosystem: The Competence Centre will facilitate and help coordinate the work of the Network and nurture the Cybersecurity Competence Community, driving the cybersecurity technological agenda and facilitating access to the expertise so gathered. The Competence Centre will in particular do so by implementing relevant parts of the Digital Europe and Horizon Europe programmes by allocating grants and carrying out procurements. In view of the considerable investments in cybersecurity made in other parts of the world and of the need to coordinate and pool relevant resources in Europe, the Competence Centre is proposed as a European Partnership[12], thus facilitating joint investment by the Union, Member States and/or industry. Therefore the proposal requires Member States to contribute a commensurate amount to the actions of the Competence Centre and Network. The principal decision-making body is the Governing Board, in which all Member States take part but only those Member States which participate financially have voting rights. The voting mechanism in the Governing Board follows a double majority principle requiring 75 % of the financial contribution and 75 % of the votes. In view of its responsibility for the Union budget, the Commission holds 50 % of the votes. For its work on the Governing Board, the Commission will avail itself, wherever appropriate, of the expertise of the European External Action Service. The Governing Board is assisted by an Industrial and Scientific Advisory Board to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders.

---

8 Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, adopted by the General Affairs Council on 20 November 2017.

9 COM(2018) 434 Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027

10 See SWD(2018) 305

11 COM 2018) 435 Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination

12 As defined in COM(2018) 435 Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination; and as referenced in COM(2018) 434 Proposal for a Regulation of the European Parliament and of the Council establishing Digital Europe Programme for the period 2021-2027.

Working closely with the Network of National Coordination Centres and cybersecurity competence community (involving a large and diverse group of actors involved in cybersecurity technology development such as research entities, supply-side industries, demand side industries, and the public sector) established by this Regulation, the European Cybersecurity Industrial, Technology and Research Competence Centre would be the main implementation body for EU financial resources dedicated to cybersecurity under the proposed *Digital Europe Programme*and *Horizon Europe Programme*

Such a comprehensive approach would allow supporting cybersecurity across the entire value chain, from research to supporting the deployment and uptake of key technologies. The Member States' financial participation should be commensurate to the EU financial contribution to this initiative and is an indispensable element for its success.

In view of its particular expertise and broad and relevant stakeholder representation, the European Cybersecurity Organisation, which is the Commission's counterpart to the contractual public-private partnership on cybersecurity under Horizon 2020, should be invited to contribute to the work of the Centre and the network.

In addition, the European Cybersecurity Industrial, Technology and Research Competence Centre should also seek to enhance synergies between the civilian and defence dimensions of cybersecurity. It should give support to Member States and other relevant actors by providing advice, sharing expertise and facilitating collaboration with regard to project and actions. When requested by Member States it could also act as a project manager notably in relation to the European Defence Fund. The present initiative aims to contribute to tackling the following problems:

- **Insufficient cooperation between cybersecurity demand and supply industries.** The European businesses face the challenge of both remaining secure and offering secure products and services to their clients. Yet, often they are not able to appropriately secure their existing products, services and assets or to design secure innovative products and services. Key cybersecurity assets are often too costly to be developed and set up by individual players, whose core business activity is not related to cybersecurity. At the same time, the links between the demand and supply side of the cybersecurity market are not sufficiently well developed resulting in sub-optimal supply of European products and solutions adapted to different sectors' needs, as well as in insufficient levels of trust among market players.

- **Lack of an efficient cooperation mechanism among Member States for industrial capacity building.** At the moment, there is also no efficient cooperation mechanism for Member States to work together towards building necessary capabilities supporting cybersecurity innovation across industrial sectors and deployment of cutting-edge European cybersecurity solutions. The existing cooperation mechanisms for Member States in the field of cybersecurity under Directive (EU) 2016/1148 do not envisage this type of activities in their mandate.

- **Insufficient cooperation within and between research and industrial communities.** Despite Europe's theoretical capacity to cover the full cybersecurity value chain, there are relevant cybersecurity sectors (e.g. energy, space, defence, transport) and sub-domains that are today poorly supported by the research community, or supported only by a limited number of centres (e.g. post-quantum and quantum cryptography, trust and cybersecurity in AI). While this collaboration obviously exists, it is very often a short-term, consultancy-

type of arrangement, which does not allow engaging in long-term research plans to solve cybersecurity industrial challenges.

- **Insufficient cooperation between civilian and defence cybersecurity research and innovation communities.** The problem of insufficient levels of cooperation also concerns the civilian and defence communities. The existing synergies are not used to the full extent due to lack of efficient mechanisms allowing these communities to cooperate efficiently and build trust, which, even more than in other fields, is a prerequisite for successful cooperation. This is coupled with limited financial capabilities in the EU cybersecurity market, including insufficient funds to support innovation.

- **Consistency with existing policy provisions in the policy area**

The Cybersecurity competence network and the European Cybersecurity Industrial, Technology and Research Competence Centre will act as an additional support to existing cybersecurity policy provisions and actors. The mandate of the European Cybersecurity Industrial, Technology and Research Competence Centre will be complementary to ENISA's efforts but has a different focus and requires a different set of skills. While ENISA's mandate envisages an advising role on cybersecurity research and innovation in the EU, its proposed mandate focuses first and foremost on other tasks crucial for strengthening cybersecurity resilience in the EU. In addition, ENISA's mandate does not envisage the types of activities, which would be the Centre and Network's core tasks - to stimulate the development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level.

The European Cybersecurity Industrial, Technology and Research Competence Centre, together with the Cybersecurity competence network will also work towards supporting research to facilitate and accelerate standardisation and certification processes, in particular those related to cybersecurity certification schemes in the meaning of the proposed Cybersecurity Act[13][14].

The present initiative is *de facto* scaling up the Public-Private Partnership on Cybersecurity (cPPP), which was the first EU-wide attempt to bring together the cybersecurity industry, the demand side (buyers of cybersecurity products and solutions, including public administration and critical sectors such as e.g. transport, health, energy, financial) and the research community to build the platform of sustainable dialogue and create conditions for voluntary co-investment. The cPPP was created in 2016 and has triggered up to EUR 1.8 billion of investment by 2020. However, the scale of the investment under way in other parts of the world (e.g. the US invested 19 billion dollars in cybersecurity in 2017 alone) shows that the EU needs to do more to achieve a critical mass of investment, and to overcome the fragmentation of capacities spread across the EU.

---

[13] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act", COM(2017) 477 final/3)

[14] This is without prejudice to the certification mechanisms under the General Data Protection Regulation, in which data protection authorities have a role to play, in line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation")

- **Consistency with other Union policies**

The European Cybersecurity Industrial, Technology and Research Competence Centre will act as a single implementation body for various Union programmes supporting cybersecurity (Digital Europe Programme and Horizon Europe) and enhance coherence and synergies between them.

This initiative will also allow to complement the efforts of the Member States by providing appropriate input to education policy makers in order to enhance cybersecurity skills (e.g. by developing cybersecurity curricula in civilian and military educational systems) to help develop a qualified EU cybersecurity workforce – a key asset for cybersecurity companies as well as other industries with a stake in cybersecurity. As to cyber defence education and training, this initiative will be consistent with the ongoing work of the cyber defence education, training and exercises platform established under the European Security and Defence College.

This initiative will be complementary with and support the efforts of the Digital Innovation Hubs under Digital Europe Programme. Digital Innovation Hubs are non-for-profit organisations helping companies – especially Start-ups, SMEs, and mid-caps to become more competitive by improving their business/production processes as well as products and services through smart innovation enabled by digital technology. Digital Innovation Hubs provide business-oriented, innovation services, such as market intelligence, financing advice, access to relevant testing and experimentation facilities, training and skills development, to help new products or services to successfully reach the market, or to introduce better production processes. Some Digital Innovation Hubs, with specific cybersecurity expertise, could be directly involved in cybersecurity competence community established by this initiative. In most cases, however, Digital Innovation Hubs, which do not have specific cybersecurity profile, would facilitate access of its constituency to the cybersecurity expertise, knowledge and capacities available with the cybersecurity competence community by cooperating closely with the Network of National Coordination Centres and the European Cybersecurity Industrial, Technology and Research Competence Centre. Digital Innovation Hubs would also support the deployment of innovative cybersecurity products and solutions corresponding to the needs of the companies and other end-users they serve. Last but not least, sector specific Digital Innovation Hubs could share their knowledge of real-life sectorial needs with the Network and the Centre to feed the reflection on the research and innovation agenda responding to industrial requirements.

Synergies with relevant Knowledge and Innovation Communities of the European Institute of Innovation & Technology, and, in particular, with EIT Digital will be sought.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The Competence Centre should be established on a double legal basis due to its nature and specific objectives. Article 187 TFEU, setting up the structures needed for the efficient execution of Union research, technological development and demonstration programmes, allows the Competence Centre to create synergies and pool resources to invest in necessary capacities at the Member States' level and develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). The first paragraph of Article 188 provides for the adoption of such measures. Nonetheless, the first

subparagraph of Article 188 as a sole legal basis would not allow for the activities to go beyond the sphere of research and development as needed to fulfil all the objectives of the Competence Centre set out in this Regulation supporting the market deployment of cybersecurity products and solutions, helping the European cybersecurity industry to become more competitive and increase their market share and adding value to the national efforts of addressing cybersecurity skills gap. Therefore in order to achieve these objectives it is necessary to add Article 173(3) as a legal basis which allows the Union to provide for measures to support the competitiveness of the industry.

- **Justification for proposal in terms of subsidiarity and proportionality principles**

Cybersecurity is an issue of common interest of the Union, as confirmed by the Council Conclusions mentioned above. The scale and cross-border character of incidents such as *WannaCry* or *NonPetya* are a point in case. The nature and scale of the cybersecurity technological challenges, as well as insufficient coordination of efforts within and across the industry, public sector and research communities require the EU to further support coordination efforts both to pool a critical mass of resources and ensure better knowledge and assets management. This is needed in view of the resource requirements related to certain capabilities for cybersecurity research, development and deployment; the need to provide access to interdisciplinary cybersecurity know-how across different disciplines (often only partially available at the national level); the global nature of industrial value chains, as well as the activity of global competitors working across the markets.

This requires resources and expertise at a scale that can be hardly matched by the individual action of any Member State. For example, a pan-European quantum communication network could require EU investment of approximately EUR 900 million, depending on the investments by Member States (to be interconnected/complemented) and to what extent the technology will allow the reuse of existing infrastructures. The initiative will be instrumental in pooling financing and allowing this type of investment to happen in the Union.

The objectives of this initiative cannot be fully achieved by the Member States alone. As shown above they can be better achieved at the Union level by pooling efforts and avoiding their unnecessary duplication, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way. At the same time, in accordance with the principle of proportionality, this Regulation does not go beyond what is necessary in order to achieve that objective. EU action is therefore justified on grounds of subsidiarity and proportionality.

This instrument does not foresee any new regulatory obligations for businesses. At the same time, businesses and especially SMEs are likely to reduce the costs related to their efforts in designing innovative cyber secure products as the initiative allows pooling resources to invest in necessary capacities at the Member States' level or develop European shared assets (e.g. by jointly procuring necessary cybersecurity testing and experimentation infrastructure). These assets could be used by industries and SMEs across different sectors to ensure that their products are cybersecure and turn cybersecurity into their competitive advantage.

- **Choice of the instrument**

The proposed instrument establishes a body dedicated to implementing cybersecurity actions under Digital Europe Programme and Horizon Europe Programme. It outlines its mandate, tasks as well as governance structure. Setting up such a Union body requires the adoption of a Regulation.

3. STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

The proposal to create a Cybersecurity competence network with a European Cybersecurity Industrial, Technology and Research Competence Centre is a new initiative. It acts as a continuation and scaling up of the contractual Public Private Partnership on cybersecurity created in 2016.

- **Stakeholder consultations**

Cybersecurity is a broad, cross-sectoral topic. The Commission used different consultation methods in order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in this initiative. This method ensures transparency and accountability in the Commission's work. While no open public consultation was conducted specifically for this initiative given its target audience (industrial and research community and Member States), the thematic was already covered by several other open public consultations:

- A general open public consultation carried out in 2018 on the topic of investment, research & innovation, SMEs and the single market.

- A 12-week online public consultation launched in 2017 to seek views of the wider public (approx. 90 respondents) on ENISA evaluation and review.

- A 12-week online public consultation that was carried out in 2016 at the occasion of the launch of the contractual public-private partnership on cybersecurity (approx. 240 respondents).

The Commission also organised targeted consultations on this initiative including workshops, meetings and targeted requests for input (from ENISA and European Defence Agency). The consultation period spanned over 6 months, starting in November 2017 until March 2018. The Commission also conducted a mapping of centres of expertise, which allowed to gather input from 665 cybersecurity expertise centres on their know-how, activity, working fields, international cooperation. The survey was launched in January and surveys submitted until 08 March 2018 were taken into consideration for the report analysis.

Stakeholders from the industrial and research communities considered that the Competence Centre and the Network could add value to the current efforts on the national level by helping create a Europe-wide cybersecurity ecosystem allowing better cooperation between the research and industry communities. They also considered it necessary that the EU and Member States take a proactive, longer-term and strategic perspective to cybersecurity industrial policy going beyond research and innovation only. Stakeholders expressed the need to gain access to key capabilities such as testing and experimentation facilities and to be more ambitious in closing the cybersecurity skills gap e.g. through large-scale European projects attracting the best talents. All of the above was also seen as necessary for Union to be recognised globally as a leader in cybersecurity.

Member States, in the framework of the consultation activities undertaken since last September[15] as well as in dedicated Council Conclusions[16] welcomed the intention to set up a

[15] E.g. High level Roundtable with Member States, VP Ansip, Commissioner Gabriel, 5 December 2017

[16] General Affairs Council: Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (20 November 2017)

Cybersecurity competence network to stimulate the development and deployment of cybersecurity technologies, stressing the need to be inclusive towards all Member States and their existing centres of excellence and competence and to pay special attention to complementarity. Specifically with regard to the future Competence Centre, Member States stressed the importance of its coordinating role in the support of the network. In particular with regard to national activities and needs in cyber defence, the mapping exercise on Member States' cyber defence needs conducted by the European External Action Service in March 2018, demonstrated that most of the Member States see the added value in EU support for cyber training and education as well as in supporting industry through research and development.[17] The initiative would indeed be implemented together with Member States or entities supported by them. Collaborations between the industry, research and/or public sector communities would bring together and strengthen existing entities and efforts at not create new ones. Member States would also be involved in defining specific actions targeting the public sector as a direct user of cybersecurity technology and know-how.

- **Impact assessment**

An Impact Assessment supporting this initiative was submitted to the Regulatory Scrutiny Board on 11 April 2017 and received a positive opinion with reservations. The Impact Assessment was subsequently reviewed in light of the Board's comments. The Opinion of the Board and the Annex explaining how the Board's comments were addressed is published along with this proposal.

A number of policy options have been considered in the Impact Assessment, both legislative and non-legislative. The following options were retained for an in-depth assessment:

- Baseline scenario - Collaborative Option - assumes the continuation of the current approach to building cybersecurity industrial and technological capacities in the EU through supporting research and innovation and related collaboration mechanisms under FP9.

- Option 1: Cybersecurity competence network with a European Cybersecurity Industrial, Technology and Research Competence Centre with a dual mandate to pursue measures in support of industrial technologies as well as in the domain of research and innovation.

- Option 2: Cybersecurity competence network with a European Cybersecurity Research and Competence Centre focused on research and innovation activities

The options discarded at an early stage included 1) the option of no action at all, 2) the option of creating the cybersecurity competence network only, 3) the option of creating a centralised structure only as well as 4) the option of using an existing agency (European Union Agency for Network and Information Security – (ENISA), Research Executive Agency (REA) or Innovations and Networks Executive Agency (INEA).

The analysis concluded that Option 1 is best suited to achieve the goals of the initiative while offering the highest economic, societal, and environmental impact and safeguarding the Union's interests. The main arguments in favour of this option included the ability to create a real cybersecurity industrial policy by supporting activities related not only to research and

[17] EEAS, March 2018

development but also to market deployment; the flexibility to allow different cooperation models with the network of competence centres to optimise the use of existing knowledge and resources; ability to structure cooperation and joint commitments of the public and private stakeholders coming from all relevant sectors, including defence;. Last but not least, Option 1 allows as well increasing synergies and can act as an implementation mechanism for two different EU cybersecurity funding streams under the next Multi-annual financial framework (Digital Europe Program, Horizon Europe).

- **Fundamental rights**

This initiative will allow public authorities and industries across Member States to more effectively prevent and respond to cyber threats by offering and equipping itself with more secure products and solutions. This is in particular relevant for the protection of access to essential services (e.g. transport, health, banking and financial services).

Increased capacity of the European Union to autonomously secure its products and services is also likely to help citizens enjoy their democratic rights and values (e.g. better protect their information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life) and consequently increase their trust in the digital society and economy.

4. BUDGETARY IMPLICATIONS

The European Cybersecurity Industrial, Technology and Research Competence Centre, in cooperation with the cybersecurity competence network, will be the main implementation body for EU financial resources dedicated to cybersecurity under Digital Europe and Horizon Europe.

The budgetary implications related to the implementation of Digital Europe are listed in detail in the Legislative Financial Statement annexed to this proposal. The contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached. The proposal will be based on the outcome of the strategic planning process as defined in Article 6 (6) of Regulation XXX [Horizon Europe framework programme].

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

An explicit evaluation clause, by which the Commission will conduct an independent evaluation, is foreseen in this proposal (Article 38). The Commission will subsequently report to the European Parliament and the Council on its evaluation accompanied where appropriate by a proposal for its review, in order to measure the impact of the instrument and its added value. The Commission Better Regulation methodology on evaluation will be applied.

The Executive Director should present to the Governing Board an ex-post evaluation of the European Cybersecurity Industrial, Technology and Research Competence Centre's and the Network's activities every two years as set out in Article 17 of this proposal. The Executive

Director should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress every two years to the Commission. The Governing Board should be responsible to monitor the adequate follow-up of such conclusions, as set out by Article 16 of this proposal.

Alleged instances of maladministration in the activities of the legal body may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

2018/0328 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 173(3) and the first paragraph of Article 188 thereof,

Having regard to the proposal from the European Commission,

Having regard to the opinion of the European Economic and Social Committee[18],

Having regard to the opinion of the Committee of the Regions[19],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Our daily lives and economies become increasingly dependent on digital technologies, citizens become more and more exposed to serious cyber incidents. Future security depends, among others, on enhancing technological and industrial ability to protect the Union against cyber threats, as both civilian infrastructure and military capacities rely on secure digital systems.

(2) The Union has steadily increased its activities to address growing cybersecurity challenges following the 2013 Cybersecurity Strategy[20] aimed to foster a reliable, safe, and open cyber ecosystem. In 2016 the Union adopted the first measures in the area of

[18] OJ C , p. .

[19] OJ C , , p. .

[20] Joint Communication to the European Parliament and the Council:: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace JOIN(2013) 1 final.

cybersecurity through Directive (EU) 2016/1148 of the European Parliament and of the Council[21] on security of network and information systems.

(3) In September 2017, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a Joint Communication[22] on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" to further reinforce the Union's resilience, deterrence and response to cyber-attacks.

(4) The Heads of State and Government at the Tallinn Digital Summit, in September 2017, called for the Union to become "a global leader in cyber-security by 2025, in order to ensure trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."

(5) Substantial disruption of network and information systems can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal market. At the moment, the Union depends on non-European cybersecurity providers. However, it is in the Union's strategic interest to ensure that it retains and develops essential cybersecurity technological capacities to secure its Digital Single Market, and in particular to protect critical networks and information systems and to provide key cybersecurity services.

(6) A wealth of expertise and experience in cybersecurity research, technology and industrial development exists in the Union but the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness in this domain. These efforts and expertise need to be pooled, networked and used in an efficient manner to reinforce and complement existing research, technology and industrial capacities at Union and national levels.

(7) The Council Conclusions adopted in November 2017 called on the Commission to provide rapidly an impact assessment on the possible options to create a network of cybersecurity competence centres with the European Research and Competence Centre and propose by mid-2018 the relevant legal instrument.

(8) The Competence Centre should be the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Cybersecurity Competence Network. It should deliver cybersecurity-related financial support from the Horizon Europe and Digital Europe programmes, and should be open to the European Regional Development Fund and other programmes where appropriate. This approach should contribute to creating synergies and coordinating financial support related to cybersecurity research, innovation, technology and industrial development and avoiding duplication.

---

[21] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

[22] Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final.

(9) Taking into account that the objectives of this initiative can be best achieved if all Member States or as many Member States as possible participate, and as an incentive for Member States to take part, only Member States who contribute financially to the administrative and operational costs of the Competence Centre should hold voting rights.

(10) The participating Member States' financial participation should be commensurate to the Union's financial contribution to this initiative.

(11) The Competence Centre should facilitate and help coordinate the work of the Cybersecurity Competence Network ("the Network"), made up of National Coordination Centres in each Member State. National Coordination Centres should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out activities related to this Regulation.

(12) National Coordination Centres should be selected by Member States. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council[23], and the research community.

(13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements.

(14) Emerging technologies such as artificial intelligence, Internet of Things, high-performance computing (HPC) and quantum computing, blockchain and concepts such as secure digital identities create at the same time new challenges for cybersecurity as well as offer solutions. Assessing and validating the robustness of existing or future ICT systems will require testing security solutions against attacks run on HPC and quantum machines. The Competence Centre, the Network and the Cybersecurity Competence Community should help advance and disseminate the latest cybersecurity solutions. At the same time the Competence Centre and the Network should be at the service of developers and operators in critical sectors such as transport, energy, health, financial, government, telecom, manufacturing, defence, and space to help them solve their cybersecurity challenges.

(15) The Competence Centre should have several key functions. First, the Competence Centre should facilitate and help coordinate the work of the European Cybersecurity Competence Network and nurture the Cybersecurity Competence Community. The Centre should drive the cybersecurity technological agenda and facilitate access to the expertise gathered in the Network and the Cybersecurity Competence Community. Secondly, it should implement relevant parts of Digital Europe and Horizon Europe

[23] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

programmes by allocating grants, typically following a competitive call for proposals. Thirdly, the Competence Centre should facilitate joint investment by the Union, Member States and/or industry.

(16) The Competence Centre should stimulate and support the cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, and diverse group of actors involved in cybersecurity technology. That Community should include in particular research entities, supply-side industries, demand side industries, and the public sector. The Cybersecurity Competence Community should provide input to the activities and work plan of the Competence Centre and it should also benefit from the community-building activities of the Competence Centre and the Network, but otherwise should not be privileged with regard to calls for proposals or calls for tender.

(17) In order to respond to the needs of both demand and supply side industries, the Competence Centre's task to provide cybersecurity knowledge and technical assistance to industries should refer to both ICT products and services and all other industrial and technological products and solutions in which cybersecurity is to be embedded.

(18) Whereas the Competence Centre and the Network should strive to achieve synergies between the cybersecurity civilian and defence spheres, projects financed by the Horizon Europe Programme will be implemented in line with Regulation XXX [Horizon Europe Regulation], which provides that research and innovation activities carried out under Horizon Europe shall have a focus on civil applications.

(19) In order to ensure structured and sustainable collaboration, the relation between the Competence Centre and the National Coordination Centres should be based on a contractual agreement.

(20) Appropriate provisions should be made to guarantee the liability and transparency of the Competence Centre.

(21) In view of their respective expertise in cybersecurity, the Joint Research Centre of the Commission as well as the European Network and Information Security Agency (ENISA) should play an active part in the Cybersecurity Competence Community and the Industrial and Scientific Advisory Board.

(22) Where they receive a financial contribution from the general budget of the Union, the National Coordination Centres and the entities which are part of the Cybersecurity Competence Community should publicise the fact that the respective activities are undertaken in the context of the present initiative.

(23) The Union contribution to the Competence Centre should finance half of the costs arising from the establishment, administrative and coordination activities of the Competence Centre, In order to avoid double funding, those activities should not benefit simultaneously from a contribution from other Union programmes.

(24) The Governing Board of the Competence Centre, composed of the Member States and the Commission, should define the general direction of the Competence Centre’s operations, and ensure that it carries out its tasks in accordance with this Regulation. The Governing Board should be entrusted with the powers necessary to establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent

working procedures for decision making by the Competence Centre, adopt the Competence Centre's work plan and multiannual strategic plan reflecting the priorities in achieving the objectives and tasks of the Competence Centre, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof.

(25) In order for the Competence Centre to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Governing Board have appropriate professional expertise and experience in functional areas. The Commission and the Member States should also make efforts to limit the turnover of their respective Representatives on the Governing Board in order to ensure continuity in its work.

(26) The smooth functioning of the Competence Centre requires that its Executive Director be appointed on grounds of merit and documented administrative and managerial skills, as well as competence and experience relevant for cybersecurity, and that the duties of the Executive Director be carried out with complete independence.

(27) The Competence Centre should have an Industrial and Scientific Advisory Board as an advisory body to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Industrial and Scientific Advisory Board should focus on issues relevant to stakeholders and bring them to the attention of the Competence Centre's Governing Board. The composition of the Industrial and Scientific Advisory Board and the tasks assigned to it, such as being consulted regarding the work plan, should ensure sufficient representation of stakeholders in the work of the Competence Centre.

(28) The Competence Centre should benefit from the particular expertise and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity during the duration of Horizon2020, through its Industrial and Scientific Advisory Board.

(29) The Competence Centre should have in place rules regarding the prevention and the management of conflict of interest. The Competence Centre should also apply the relevant Union provisions concerning public access to documents as set out in Regulation (EC) No 1049/2001 of the European Parliament and of the Council[24]. Processing of personal data by the Competence Centre will be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council. The Competence Centre should comply with the provisions applicable to the Union institutions, and with national legislation regarding the handling of information, in particular sensitive non classified information and EU classified information.

(30) The financial interests of the Union and of the Member States should be protected by proportionate measures throughout the expenditure cycle, including the prevention, detection and investigation of irregularities, the recovery of lost, wrongly paid or incorrectly used funds and, where appropriate, the application of administrative and

[24] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

financial penalties in accordance with Regulation XXX (EU, Euratom) of the European Parliament and of the Council[25] [the Financial Regulation].

(31) The Competence Centre should operate in an open and transparent way providing all relevant information in a timely manner as well as promoting its activities, including information and dissemination activities to the wider public. The rules of procedure of the bodies of the Competence Centre should be made publicly available.

(32) The Commission's internal auditor should exercise the same powers over the Competence Centre as those exercised in respect of the Commission.

(33) The Commission, the Competence Centre, the Court of Auditors and the European Anti-Fraud Office should get access to all necessary information and the premises to conduct audits and investigations on the grants, contracts and agreement signed by the Competence Centre.

(34) Since the objectives of this Regulation, namely retaining and developing Union's cybersecurity technological and industrial capacities, increasing the competitiveness of the Union's cybersecurity industry and turning cybersecurity into a competitive advantage of other Union industries, cannot be sufficiently achieved by the Member States due the fact that existing, limited resources are dispersed as well as due to the scale of the investment necessary, but can rather by reason of avoiding unnecessary duplication of these efforts, helping to achieve critical mass of investment and ensuring that public financing is used in an optimal way be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS AND PRINCIPLES OF THE COMPETENCE CENTRE AND THE NETWORK

Article 1

Subject matter

1. This Regulation establishes the European Cybersecurity Industrial, Technology and Research Competence Centre (the 'Competence Centre'), as well as the Network of National Coordination Centres, and lays down rules for the nomination of National Coordination Centres as well as for the establishment of the Cybersecurity Competence Community.

[25] [add title and OJ reference]

2. The Competence Centre shall contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] thereof and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme].

3. The seat of the Competence Centre shall be located in [Brussels, Belgium.]

4. The Competence Centre shall have legal personality. In each Member State, it shall enjoy the most extensive legal capacity accorded to legal persons under the laws of that Member State. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings.

Article 2

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'cybersecurity' means the protection of network and information systems, their users, and other persons against cyber threats;

(2) 'cybersecurity products and solutions' means ICT products, services or process with the specific purpose of protecting network and information systems, their users and affected persons from cyber threats;

(3) 'public authority' means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person performing public administrative functions under national law, including specific duties;

(4) 'participating Member State' means a Member State which voluntarily contributes financially to the administrative and operational costs of the Competence Centre.

Article 3

Mission of the Centre and the Network

1. The Competence Centre and the Network shall help the Union to:

   (a) retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market;

   (b) increase the competitiveness of the Union's cybersecurity industry and turn cybersecurity into competitive advantage of other Union industries.

2. The Competence Centre shall undertake its tasks, where appropriate, in collaboration with the Network of National Coordination Centres and a Cybersecurity Competence Community.

Article 4

Objectives and Tasks of the Centre

The Competence Centre shall have the following objectives and related tasks:

1. facilitate and help coordinate the work of the National Coordination Centres Network ('the Network') referred to in Article 6 and the Cybersecurity Competence Community referred to in Article 8;

2. contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX[26] and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX[27] and in particular Section 2.2.6 of Pillar II of Annex I. of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation[ref. number of the Specific Programme]. and of other Union programmes when provided for in legal acts of the Union];

3. enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities, by carrying out the following tasks:

    (a) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services , acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;

    (b) having regard to the state-of-the-art cybersecurity industrial and research infrastructures and related services, providing support to other entities, including financially, to acquiring, upgrading, operating and making available such infrastructures and related services to a wide range of users across the Union from industry including SMEs, the public sector and the research and scientific community;

    (c) providing cybersecurity knowledge and technical assistance to industry and public authorities, in particular by supporting actions aimed at facilitating access to the expertise available in the Network and the Cybersecurity Competence Community;

4. contribute to the wide deployment of state-of-the-art cyber security products and solutions across the economy, by carrying out the following tasks:

---

26 [add full title and OJ reference]

27 [add full title and OJ reference]

(a) stimulating cybersecurity research, development and the uptake of Union cybersecurity products and solutions by public authorities and user industries;

(b) assisting public authorities, demand side industries and other users in adopting and integrating the latest cyber security solutions;

(c) supporting in particular public authorities in organising their public procurement, or carrying out procurement of state-of-the-art cybersecurity products and solutions on behalf of public authorities;

(d) providing financial support and technical assistance to cybersecurity start-ups and SMEs to connect to potential markets and to attract investment;

5. improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity by carrying out the following tasks:

(a) supporting further development of cybersecurity skills , where appropriate together with relevant EU agencies and bodies including ENISA.

6. contribute to the reinforcement of cybersecurity research and development in the Union by:

(a) providing financial support to cybersecurity research efforts based on a common, continuously evaluated and improved multiannual strategic, industrial, technology and research agenda;

(b) support large-scale research and demonstration projects in next generation cybersecurity technological capabilities, in collaboration with the industry and the Network;

(c) support research and innovation for standardisation in cybersecurity technology

7. enhance cooperation between the civil and defence spheres with regard to dual use technologies and applications in cybersecurity, by carrying out the following tasks:

(a) supporting Member States and industrial and research stakeholders with regard to research, development and deployment;

(b) contributing to cooperation between Member States by supporting education, training and exercises ;

(c) bringing together stakeholders, to foster synergies between civil and defence cyber security research and markets;

8. enhance synergies between the civil and defence dimensions of cybersecurity in relation to the European Defence Fund by carrying out the following tasks:

(a) providing advice, sharing expertise and facilitating collaboration among relevant stakeholders;

(b) managing multinational cyber defence projects, when requested by Member States, and thus acting as a project manager within the meaning of Regulation XXX [Regulation establishing the European Defence Fund].

Article 5

Investment in and use of infrastructures, capabilities, products or solutions

1. Where the Competence Centre provides funding for infrastructures, capabilities, products or solutions pursuant to Article 4(3) and (4) in the form of a grant or a prize, the work plan of the Competence Centre may specify in particular:

   (a) rules governing the operation of an infrastructure or capability, including where relevant entrusting the operation to a hosting entity based on criteria that the Competence Centre shall define;

   (b) rules governing access to and use of an infrastructure or capability.

2. The Competence Centre may be responsible for the overall execution of relevant joint procurement actions including pre-commercial procurements on behalf of members of the Network, members of the cybersecurity Competence Community, or other third parties representing the users of cybersecurity products and solutions. For this purpose, the Competence Centre may be assisted by one or more National Coordination Centres or members of the Cybersecurity Competence Community.

Article 6

Nomination of National Coordination Centres

1. By [date], each Member State shall nominate the entity to act as the National Coordination Centre for the purposes of this Regulation and notify it to the Commission.

2. On the basis of an assessment concerning the compliance of that entity with the criteria laid down in paragraph 4, the Commission shall issue a decision within 6 months from the nomination transmitted by the Member State providing for the accreditation of the entity as a National Coordination Centre or rejecting the nomination. The list of National Coordination Centres shall be published by the Commission.

3. Member States may at any time nominate a new entity as the National Coordination Centre for the purposes of this Regulation. Paragraphs 1 and 2 shall apply to nomination of any new entity.

4. The nominated National Coordination Centre shall have the capability to support the Competence Centre and the Network in fulfilling their mission laid out in Article 3

of this Regulation. They shall possess or have direct access to technological expertise in cybersecurity and be in a position to effectively engage and coordinate with industry, the public sector and the research community.

5. The relationship between the Competence Centre and the National Coordination Centres shall be based on a contractual agreement signed between the Competence Centre and each of the National Coordination Centres. The agreement shall provide for the rules governing the relationship and division of tasks between the Competence Centre and each National Coordination Centre.

6. The National Coordination Centres Network shall be composed of all the National Coordination Centres nominated by the Member States.

Article 7

Tasks of the National Coordination Centres

1. The National Coordination Centres shall have the following tasks:

   (a) supporting the Competence Centre in achieving its objectives and in particular in coordinating the Cybersecurity Competence Community;

   (b) facilitating the participation of industry and other actors at the Member State level in cross-border projects;

   (c) contributing, together with the Competence Centre, to identifying and addressing sector-specific cyber security industrial challenges;

   (d) acting as contact point at the national level for the Cybersecurity Competence Community and the Competence Centre;

   (e) seeking to establish synergies with relevant activities at the national and regional level;

   (f) implementing specific actions for which grants have been awarded by the Competence Centre, including through provision of financial support to third parties in line with Article 204 of Regulation XXX [new Financial Regulation] under conditions specified in the concerned grant agreements.

   (g) promoting and disseminating the relevant outcomes of the work by the Network, the Cybersecurity Competence Community and the Competence Centre at national or regional level;

   (h) assessing requests by entities established in the same Member State as the Coordination Centre for becoming part of the Cybersecurity Competence Community.

2. For the purposes of point (f), the financial support to third parties may be provided in any of the forms specified in Article 125 of Regulation XXX [new Financial Regulation] including in the form of lump sums.

3. National Coordination Centres may receive a grant from the Union in accordance with Article 195 (d) of Regulation XXX [new Financial Regulation] in relation to carrying out the tasks laid down in this Article.

4. National Coordination Centres shall, where relevant, cooperate through the Network for the purpose of implementing tasks referred to in points (a), (b), (c), (e) and (g) of paragraph 1.

Article 8

The Cybersecurity Competence Community

1. The Cybersecurity Competence Community shall contribute to the mission of the Competence Centre as laid down in Article 3 and enhance and disseminate cybersecurity expertise across the Union.

2. The Cybersecurity Competence Community shall consist of industry, academic and non-profit research organisations, and associations as well as public entities and other entities dealing with operational and technical matters. It shall bring together the main stakeholders with regard to cybersecurity technological and industrial capacities in the Union. It shall involve National Coordination Centres as well as Union institutions and bodies with relevant expertise..

3. Only entities which are established within the Union may be accredited as members of the Cybersecurity Competence Community. They shall demonstrate that they have cybersecurity expertise with regard to at least one of the following domains:

   (a) research;

   (b) industrial development;

   (c) training and education.

4. The Competence Centre shall accredit entities established under national law as members of the Cybersecurity Competence Community after an assessment made by the National Coordination Centre of the Member State where the entity is established, on whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it or the relevant National Coordination Centre considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].

5. The Competence Centre shall accredit relevant bodies, agencies and offices of the Union as members of the Cybersecurity Competence Community after carrying out an assessment whether that entity meets the criteria provided for in paragraph 3. An accreditation shall not be limited in time but may be revoked by the Competence Centre at any time if it considers that the entity does not fulfil the criteria set out in paragraph 3 or it falls under the relevant provisions set out in Article 136 of Regulation XXX [new financial regulation].

6. The representatives of the Commission may participate in the work of the Community.

Article 9

Tasks of the members of the Cybersecurity Competence Community

The members of the Cybersecurity Competence Community shall:

(1) support the Competence Centre in achieving the mission and the objectives laid down in Articles 3 and 4 and, for this purpose, work closely with the Competence Centre and the relevant National Coordinating Centres;

(2) participate in activities promoted by the Competence Centre and National Coordination Centres;

(3) where relevant, participate in working groups established by the Governing Board of the Competence Centre to carry out specific activities as provided by the Competence Centre's work plan;

(4) where relevant, support the Competence Centre and the National Coordination Centres in promoting specific projects;

(5) promote and disseminate the relevant outcomes of the activities and projects carried out within the community.

Article 10

Cooperation of the Competence Centre with Union institutions, bodies, offices and agencies

1. The Competence Centre shall cooperate with relevant Union institutions, bodies, offices and agencies including the European Union Agency for Network and Information Security, the Computer Emergency Response Team (CERT-EU), the European External Action Service, the Joint Research Centre of the Commission, the Research Executive Agency, Innovation and Networks Executive Agency, European Cybercrime Centre at Europol as well as the European Defence Agency.

2. Such cooperation shall take place within the framework of working arrangements. Those arrangements shall be submitted to the prior approval of the Commission.

CHAPTER II

ORGANISATION OF THE COMPETENCE CENTRE

Article 11

Membership and structure

1. The members of the Competence Centre shall be the Union, represented by the Commission, and the Member States.

2. The structure of the Competence Centre shall comprise:

   (a) a Governing Board which shall exercise the tasks set out in Article 13;

   (b) an Executive Director who shall exercise the tasks set out in Article 16;

   (c) an Industrial and Scientific Advisory Board which shall exercise the functions set out in Article 20.

SECTION I

GOVERNING BOARD

Article 12

Composition of the Governing Board

1. The Governing Board shall be composed of one representative of each Member State, and five representatives of the Commission, on behalf of the Union.

2. Each member of the Governing Board shall have an alternate to represent them in their absence.

3. Members of the Governing Board and their alternates shall be appointed in light of their knowledge in the field of technology as well as of relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives in the Governing Board, in order to ensure continuity of the Board's work. The Commission and the Member States shall aim to achieve a balanced representation between men and women on the Governing Board.

4. The term of office of members of the Governing Board and of their alternates shall be four years. That term shall be renewable.

5. The Governing Board members shall act in the interest of the Competence Centre, safeguarding its goals and mission, identity, autonomy and coherence, in an independent and transparent way.

6. The Commission may invite observers, including representatives of relevant Union bodies, offices and agencies, to take part in the meetings of the Governing Board as appropriate.

7. The European Agency for Network and Information Security (ENISA) shall be a permanent observer in the Governing Board.

Article 13

Tasks of the Governing Board

1. The Governing Board shall have the overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities.

2. The Governing Board shall adopt its rules of procedure. These rules shall include specific procedures for identifying and avoiding conflicts of interest and ensure the confidentiality of any sensitive information.

3. The Governing Board shall take the necessary strategic decisions, in particular:

   (a) adopt a multi-annual strategic plan, containing a statement of the major priorities and planned initiatives of the Competence Centre, including an estimate of financing needs and sources;

   (b) adopt the Competence Centre's work plan, annual accounts and balance sheet and annual activity report, on the basis of a proposal from the Executive Director;

   (c) adopt the specific financial rules of the Competence Centre in accordance with [Article 70 of the FR];

   (d) adopt a procedure for appointing the Executive Director;

   (e) adopt the criteria and procedures for assessing and accrediting the entities as members of the Cybersecurity Competence Community;

   (f) appoint, dismiss, extend the term of office of, provide guidance to and monitor the performance of the Executive Director, and appoint the Accounting Officer;

   (g) adopt the annual budget of the Competence Centre, including the corresponding staff establishment plan indicating the number of temporary posts by function group and by grade, the number of contract staff and seconded national experts expressed in full-time equivalents

   (h) adopt rules regarding conflicts of interest;

   (i) establish working groups with members of the Cybersecurity Competence Community;

   (j) appoint members of the Industrial and Scientific Advisory Board;

   (k) set up an Internal Auditing Function in accordance with Commission Delegated Regulation (EU) No 1271/2013[28];

   (l) promote the Competence Centre globally, so as to raise its attractiveness and make it a world-class body for excellence in cybersecurity;

[28] Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).

(m) establish the Competence Centre's communications policy upon recommendation by the Executive Director;

(n) be responsible to monitor the adequate follow-up of the conclusions of retrospective evaluations.

(o) where appropriate, establish implementing rules to the Staff Regulations and the Conditions of Employment in accordance with Article 31(3);

(p) where appropriate, lay down rules on the secondment of national experts to the Competence Centre and on the use of trainees in accordance with Article 32(2);

(q) adopt security rules for the Competence Centre;

(r) adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented;

(s) adopt the methodology to calculate the financial contribution from Member States;

(t) be responsible for any task that is not specifically allocated to a particular body of the Competence Centre; it may assign such tasks to anybody of the Competence Centre;

Article 14

Chairperson and Meetings of the Governing Board

1. The Governing Board shall elect a Chairperson and a Deputy Chairperson from among the members with voting rights, for a period of two years. The mandate of the Chairperson and the Deputy Chairperson may be extended once, following a decision by the Governing Board. If, however, their membership of the Governing Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chairperson shall *ex officio* replace the Chairperson if the latter is unable to attend to his or her duties. The Chairperson shall take part in the voting.

2. The Governing Board shall hold its ordinary meetings at least three times a year. It may hold extraordinary meetings at the request of the Commission, at the request of one third of all its members, at the request of the chair, or at the request of the Executive Director in the fulfilment of his/her tasks.

3. The Executive Director shall take part in the deliberations, unless decided otherwise by the Governing Board, but shall have no voting rights. The Governing Board may invite, on a case-by-case basis, other persons to attend its meetings as observers.

4. Members of the Industrial and Scientific Advisory Board may take part, upon invitation from the Chairperson, in the meetings of the Governing Board, without voting rights.

5. The members of the Governing Board and their alternates may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.

6. The Competence Centre shall provide the secretariat for the Governing Board.

Article 15

Voting rules of the Governing Board

1. The Union shall hold 50 % of the voting rights. The voting rights of the Union shall be indivisible.

2. Every participating Member State shall hold one vote.

3. The Governing Board shall take its decisions by a majority of at least 75% of all votes, including the votes of the members who are absent, representing at least 75% of the total financial contributions to the Competence Centre. The financial contribution will be calculated based on the estimated expenditures proposed by the Member States referred to in point c of Article 17(2) and based on the report on the value of the contributions of the participating Member States referred to in Article 22(5).

4. Only the representatives of the Commission and the representatives of the participating Member States shall hold voting rights.

5. The Chairperson shall take part in the voting.

SECTION II

EXECUTIVE DIRECTOR

Article 16

Appointment, dismissal or extension of the term of office of the Executive Director

1. The Executive Director shall be a person with expertise and high reputation in the areas where the Competence Centre operates.

2. The Executive Director shall be engaged as a temporary agent of the Competence Centre under Article 2(a) of the Conditions of Employment of Other Servants.

3. The Executive Director shall be appointed by the Governing Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.

4. For the purpose of concluding the contract of the Executive Director, the Competence Centre shall be represented by the Chairperson of the Governing Board.

5. The term of office of the Executive Director shall be four years. By the end of that period, the Commission shall carry out an assessment which takes into account the evaluation of the performance of the Executive Director and the Competence Centre's future tasks and challenges.

6. The Governing Board may, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, extend once the term of office of the Executive Director for no more than four years.

7. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.

8. The Executive Director shall be removed from office only by decision of the Governing Board, acting on a proposal from the Commission.

Article 17

Tasks of the Executive Director

1. The Executive Director shall be responsible for operations and for the day-to-day management of the Competence Centre and shall be its legal representative. The Executive Director shall be accountable to the Governing Board and perform his or her duties with complete independence within the powers assigned to him or her.

2. The Executive Director shall in particular carry out the following tasks in an independent manner:

   (a) implement the decisions adopted by the Governing Board;

   (b) support the Governing Board its work, provide the secretariat for their meetings and supply all information necessary for the performance of their duties;

   (c) after consultation with the Governing Board and the Commission, prepare and submit for adoption to the Governing Board the draft multiannual strategic plan and the draft annual work plan of the Competence Centre including the scope of the calls for proposals, calls for expressions of interest and calls for tenders needed to implement the work plan and the corresponding expenditure estimates as proposed by the Member States and the Commission;

   (d) prepare and submit for adoption to the Governing Board the draft annual budget, including the corresponding staff establishment plan indicating the number of temporary posts in each grade and function group and the number of contract staff and seconded national experts expressed in full-time equivalents;

   (e) implement the work plan and report to the Governing Board thereon;

   (f) prepare the draft annual activity report on the Competence Centre, including the information on corresponding expenditure;

   (g) ensure the implementation of effective monitoring and evaluation procedures relating to the performance of the Competence Centre;

   (h) prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission

(i) prepare, negotiate and conclude the agreements with the National Coordination Centres;

(j) be responsible for administrative, financial and staff matters, including the implementation of the Competence Centre budget, taking due account of advice received from the Internal Auditing Function, within the limits of the delegation by the Governing Board;

(k) approve and manage the launch of calls for proposals, in accordance with the work plan and administer the grant agreements and decisions;

(l) approve the list of actions selected for funding on the basis of the ranking list established by a panel of independent experts;

(m) approve and manage the launch of calls for tenders, in accordance with the work plan and administer the contracts;

(n) approve the tenders selected for funding;

(o) submit the draft annual accounts and balance sheet to the Internal Auditing Function, and subsequently to the Governing Board,

(p) ensure that risk assessment and risk management are performed;

(q) sign individual grant agreements, decisions and contracts;

(r) sign procurement contracts;

(s) prepare an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Anti-Fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Governing Board;

(t) prepare draft financial rules applicable to the Competence Centre;

(u) establish and ensure the functioning of an effective and efficient internal control system and report any significant change to it to the Governing Board;

(v) ensure effective communication with the Union's institutions;

(w) take any other measures needed to assess the progress of the Competence Centre towards its mission and objectives as set out in Articles 3 and 4 of this Regulation;

(x) perform any other tasks entrusted or delegated to him or her by the Governing Board.

SECTION III

INDUSTRIAL AND SCIENTIFIC ADVISORY BOARD

Article 18

Composition of the Industrial and Scientific Advisory Board

1. The Industrial and Scientific Advisory Board shall consist of no more than 16 members. The members shall be appointed by the Governing Board from among the representatives of the entities of the Cybersecurity Competence Community.

2. Members of the Industrial and Scientific Advisory Board shall have expertise either with regard to cybersecurity research, industrial development, professional services or the deployment thereof. The requirements for such expertise shall be further specified by the Governing Board.

3. Procedures concerning the appointment of its members by the Governing Board and the operation of the Advisory Board, shall be specified in the Competence Centre's rules of procedure and shall be made public.

4. The term of office of members of the Industrial and Scientific Advisory Board shall be three years. That term shall be renewable.

5. Representatives of the Commission and of the European Network and Information Security Agency may participate in and support the works of the Industrial and Scientific Advisory Board.

Article 19

Functioning of the Industrial and Scientific Advisory Board

1. The Industrial and Scientific Advisory Board shall meet at least twice a year.

2. The Industrial and Scientific Advisory Board may advise the Governing Board on the establishment of working groups on specific issues relevant to the work of the Competence Centre where necessary under the overall coordination of one or more members of the Industrial and Scientific Advisory Board.

3. The Industrial and Scientific Advisory Board shall elect its chair.

4. The Industrial and Scientific Advisory Board shall adopt its rules of procedure, including the nomination of the representatives that shall represent the Advisory Board where relevant and the duration of their nomination.

Article 20

Tasks of the Industrial and Scientific Advisory Board

The Industrial and Scientific Advisory Board shall advise the Competence Centre in respect of the performance of its activities and shall:

(1) provide to the Executive Director and the Governing Board strategic advice and input for drafting the work plan and multi-annual strategic plan within the deadlines set by the Governing Board;

(2) organise public consultations open to all public and private stakeholders having an interest in the field of cybersecurity, in order to collect input for the strategic advice referred to in paragraph 1;

(3) promote and collect feedback on the work plan and multi-annual strategic plan of the Competence Centre.

CHAPTER III

FINANCIAL PROVISIONS

Article 21

Union financial contribution

1. The Union's contribution to the Competence Centre to cover administrative costs and operational costs shall comprise the following:

   (a) EUR 1 981 668 000 from the Digital Europe Programme, including up to EUR 23 746 000 for administrative costs;

   (b) An amount from the Horizon Europe Programme, including for administrative costs, to be determined taking into account the strategic planning process to be carried out pursuant to Article 6(6) of Regulation XXX [Horizon Europe Regulation].

2. The maximum Union contribution shall be paid from the appropriations in the general budget of the Union allocated to [Digital Europe Programme] and to the specific programme implementing Horizon Europe, established by Decision XXX.

3. The Competence Centre shall implement cybersecurity actions of [Digital Europe Programme] and [Horizon Europe Programme] in accordance with point (c) (iv) of Article 62 of Regulation (EU, Euratom) XXX[29] [the financial regulation].

4. The Union financial contribution shall not cover the tasks referred to in Article 4(8)(b)

Article 22

Contributions of participating Member States

1. The participating Member States shall make a total contribution to the operational and administrative costs of the Competence Centre of at least the same amounts as those in Article 21(1) of this Regulation.

2. For the purpose of assessing the contributions referred to in paragraph 1 and in point (b)ii of Article 23(3), the costs shall be determined in accordance with the usual cost accounting practices of the Member States concerned, the applicable accounting

[29] [add full title and OJ reference]

standards of the Member State, and the applicable International Accounting Standards and International Financial Reporting Standards. The costs shall be certified by an independent external auditor appointed by the Member State concerned. The valuation method may be verified by the Competence Centre should there be any uncertainty arising from the certification.

3. Should any participating Member State be in default of its commitments concerning its financial contribution, the Executive Director shall put this in writing and shall set a reasonable period within which such default shall be remedied. If the situation is not remedied within that period, the Executive Director shall convene a meeting of the Governing Board to decide whether the defaulting participating Member State's right to vote is to be revoked or whether any other measures are to be taken until its obligations have been met. The defaulting Member State's voting rights shall be suspended until the default of its commitments is remedied.

4. The Commission may terminate, proportionally reduce or suspend the Union's financial contribution to the Competence Centre if the participating Member States do not contribute, contribute only partially or contribute late with regard to the contributions referred to in paragraph 1.

5. The participating Member States shall report by 31 January each year to the Governing Board on the value of the contributions referred to in paragraphs 1 made in each of the previous financial year.

Article 23

Costs and resources of the Competence Centre

1. The Competence Centre shall be jointly funded by the Union and Member States through financial contributions paid in instalments and contributions consisting of costs incurred by National Coordination Centres and beneficiaries in implementing actions that are not reimbursed by the Competence Centre.

2. The administrative costs of the Competence Centre shall not exceed EUR [number] and shall be covered by means of financial contributions divided equally on an annual basis between the Union and the participating Member States. If part of the contribution for administrative costs is not used, it may be made available to cover the operational costs of the Competence Centre.

3. The operational costs of the Competence Centre shall be covered by means of:

   (a) the Union's financial contribution;

   (b) contributions from the participating Member States in the form of:

      (i) Financial contributions; and

      (ii) where relevant, in-kind contributions by the participating Member States of the costs incurred by National Coordination Centres and beneficiaries in implementing indirect actions less the contribution of

the Competence Centre and any other Union contribution to those costs;

4. The resources of the Competence Centre entered into its budget shall be composed of the following contributions:

   (a) participating Member States' financial contributions to the administrative costs;

   (b) participating Member States' financial contributions to the operational costs;

   (c) any revenue generated by Competence Centre;

   (d) any other financial contributions, resources and revenues.

5. Any interest yielded by the contributions paid to the Competence Centre by the participating Member States shall be considered to be its revenue.

6. All resources of the Competence Centre and its activities shall be aimed to achieve to the objectives set out in Article 4.

7. The Competence Centre shall own all assets generated by it or transferred to it for the fulfilment of its objectives.

8. Except when the Competence Centre is wound up, any excess revenue over expenditure shall not be paid to the participating members of the Competence Centre.

Article 24

Financial commitments

The financial commitments of the Competence Centre shall not exceed the amount of financial resources available or committed to its budget by its members.

Article 25

Financial year

The financial year shall run from 1 January to 31 December.

Article 26

Establishment of the budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of the Competence Centre’s revenue and expenditure for the following financial year, and shall forward it to the Governing Board, together with a draft establishment plan. Revenue and expenditure shall be in balance. The expenditure of the Competence Centre shall include the staff, administrative, infrastructure and operational expenses. Administrative expenses shall be kept to a minimum.

2. Each year, the Governing Board shall, on the basis of the draft statement of estimates of revenue and expenditure referred to in paragraph 1, produce a statement of estimates of revenue and expenditure for the Competence Centre for the following financial year.

3. The Governing Board shall, by 31 January each year, send the statement of estimates referred to in paragraph 2, which shall be part of the draft single programming document, to the Commission.

4. On the basis of that statement of estimates, the Commission shall enter in the draft budget of the Union the estimates it deems necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall submit to the European Parliament and the Council in accordance with Article 313 and 314 TFEU.

5. The European Parliament and the Council shall authorise the appropriations for the contribution to the Competence Centre.

6. The European Parliament and the Council shall adopt the establishment plan for the Competence Centre.

7. Together with the Work Plan, the Governing Board shall adopt the Centre's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Governing Board shall adjust the Competence Centre's budget and Work Plan in accordance with the general budget of the Union.

Article 27

Presentation of the Competence Centre's accounts and discharge

The presentation of the Competence Centre's provisional and final accounts and the discharge shall follow the rules and timetable of the Financial Regulation and of its financial rules adopted in accordance with Article 29.

Article 28

Operational and financial reporting

1. The Executive Director shall report annually to the Governing Board on the performance of his/her duties in accordance with the financial rules of the Competence Centre.

2. Within two months of the closure of each financial year, the Executive Director shall submit to the Governing Board for approval an annual activity report on the progress made by the Competence Centre in the previous calendar year, in particular in relation to the work plan for that year. That report shall include, inter alia, information on the following matters:

   (a) operational actions carried out and the corresponding expenditure;

(b) the actions submitted, including a breakdown by participant type, including SMEs, and by Member State;

(c) the actions selected for funding, including a breakdown by participant type, including SMEs, and by Member State and indicating the contribution of the Competence Centre to the individual participants and actions;

(d) progress towards the achievement of the objectives set out in Article 4 and proposals for further necessary work to achieve these objectives.

3. Once approved by the Governing Board, the annual activity report shall be made publicly available.

Article 29

Financial rules

The Competence Centre shall adopt its specific financial rules in accordance with Article 70 of Regulation XXX [new Financial Regulation].

Article 30

Protection of financial interests

1. The Competence Centre shall take appropriate measures to ensure that, when actions financed under this Regulation are implemented, the financial interests of the Union are protected by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative sanctions.

2. The Competence Centre shall grant Commission staff and other persons authorised by the Commission, as well as the Court of Auditors, access to its sites and premises and to all the information, including information in electronic format that is needed in order to conduct their audits.

3. The European Anti-Fraud Office (OLAF) may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Council Regulation (Euratom, EC) No 2185/96[30] and Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council[31] with a view to establishing whether there has been fraud, corruption or any other illegal activity

[30] Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

[31] Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

affecting the financial interests of the Union in connection with a grant agreement or a contract funded, directly or indirectly, in accordance with this Regulation.

4. Without prejudice to paragraphs 1, 2 and 3 of this Article, contracts and grant agreements resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct such audits and investigations in accordance with their respective competences. Where the implementation of an action is outsourced or sub-delegated, in whole or in part, or where it requires the award of a procurement contract or financial support to a third party, the contract, or grant agreement shall include the contractor's or beneficiary's obligation to impose on any third party involved explicit acceptance of those powers of the Commission, the Competence Centre, the Court of Auditors and OLAF.

CHAPTER IV

COMPETENCE CENTRE STAFF

Article 31

Staff

1. The Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Union as laid down by Council Regulation (EEC, Euratom, ECSC) No 259/68[32] ('Staff Regulations' and 'Conditions of Employment') and the rules adopted jointly by the institutions of the Union for the purpose of applying the Staff Regulations and Conditions of Employment shall apply to the staff of the Competence Centre.

2. The Governing Board shall exercise, with respect to the staff of the Competence Centre, the powers conferred by the Staff Regulations on the Appointing Authority and the powers conferred by the Conditions of Employment on the authority empowered to conclude contract ('the appointing authority powers').

3. The Governing Board shall adopt, in accordance with Article 110 of the Staff Regulations, a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment delegating the relevant appointing authority powers to the Executive Director and defining the conditions under which that delegation may be suspended. The Executive Director is authorised to sub-delegate those powers.

4. Where exceptional circumstances so require, the Governing Board may by decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and any sub-delegation made by the latter. In such a case the Governing Board shall exercise itself the appointing authority powers or delegate

[32] Regulation (EEC, Euratom, ECSC) No 259/68 of the Council of 29 February 1968 laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Communities and instituting special measures temporarily applicable to officials of the Commission (OJ L 56, 4.3.1968, p. 1).

them to one of its members or to a staff member of the Competence Centre other than the Executive Director.

5. The Governing Board shall adopt implementing rules as regards the Staff Regulations and the Conditions of Employment in accordance with Article 110 of the Staff Regulations.

6. The staff resources shall be determined in the staff establishment plan of the Competence Centre, indicating the number of temporary posts by function group and by grade and the number of contract staff expressed in full-time equivalents, in line with its annual budget.

7. The staff of the Competence Centre shall consist of temporary staff and contract staff.

8. All costs related to staff shall be borne by the Competence Centre.

Article 32

Seconded national experts and other staff

1. The Competence Centre may make use of seconded national experts or other staff not employed by the Competence Centre.

2. The Governing Board shall adopt a decision laying down rules on the secondment of national experts to the Competence Centre, in agreement with the Commission.

Article 33

Privileges and Immunities

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union shall apply to the Competence Centre and its staff.

CHAPTER V

COMMON PROVISIONS

Article 34

Security Rules

1. Article 12(7) Regulation (EU) No XXX [Digital Europe Programme] shall apply to participation in all actions funded by the Competence Centre.

2. The following specific security rules shall apply to actions funded from Horizon Europe:

(a) for the purposes of Article 34(1) [Ownership and protection] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, the grant of non-exclusive licenses may be limited to third parties established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States;

(b) for the purposes of Article 36(4)(b) [Transfer and licensing] of Regulation (EU) No XXX [Horizon Europe], the transfer or license to a legal entity established in an associated country or established in the Union but controlled from third countries shall also be a ground to object to transfers of ownership of results, or to grants of an exclusive license regarding results;

(c) for the purposes of Article 37(3)(a) [Access rights] of Regulation (EU) No XXX [Horizon Europe], when provided for in the Work plan, granting of access to results and background may be limited only to a legal entity established or deemed to be established in Members States and controlled by Member States and/or nationals of Member States.

Article 35

Transparency

1. The Competence Centre shall carry out its activities with a high level of transparency.

2. The Competence Centre shall ensure that the public and any interested parties are given appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 41.

3. The Governing Board, acting on a proposal from the Executive Director, may authorise interested parties to observe the proceedings of some of the Competence Centre's activities.

4. The Competence Centre shall lay down, in its rules of procedure, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2. For actions funded from Horizon Europe this will take due account of the provisions in Annex III of the Horizon Europe Regulation.

Article 36

Security rules on the protection of classified information and sensitive non-classified information

1. Without prejudice to Article 35, the Competence Centre shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment, in whole or in part, has been made.

2. Members of the Governing Board, the Executive Director, the members of the Industrial and Scientific Advisory Board, external experts participating in ad hoc

Working Groups, and members of the staff of the Centre shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union, even after their duties have ceased.

3. The Governing Board of the Competence Centre shall adopt the Competence Centre's security rules, following approval by the Commission, based on the principles and rules laid down in the Commission's security rules for protecting European Union classified information (EUCI) and sensitive non-classified information including inter alia provisions for the processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443[33] and 2015/444[34].

4. The Competence Centre may take all necessary measures to facilitate the exchange of information relevant to its tasks with the Commission and the Member States and where appropriate, the relevant Union agencies and bodies. Any administrative arrangement concluded to this end on sharing EUCI or, in the absence of such arrangement, any exceptional ad hoc release of EUCI shall have received the Commission's prior approval.

Article 37

Access to documents

1. Regulation (EC) No 1049/2001 shall apply to documents held by the Competence Centre.

2. The Governing Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 within six months of the establishment of the Competence Centre.

3. Decisions taken by the Competence Centre pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the Ombudsman under Article 228 of Treaty on the Functioning of the European Union or of an action before the Court of Justice of the European Union under Article 263 of Treaty on the Functioning of the European Union.

Article 38

Monitoring, evaluation and review

1. The Competence Centre shall ensure that its activities, including those managed through the National Coordination Centres and the Network, shall be subject to continuous and systematic monitoring and periodic evaluation. The Competence Centre shall ensure that the data for monitoring programme implementation and results are collected efficiently, effectively, and in timely manner and proportionate

[33] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).

[34] Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).

reporting requirements shall be imposed on recipients of Union funds and Member States. The outcomes of the evaluation shall be made public.

2. Once there is sufficient information available about the implementation of this Regulation, but no later than three and a half years after the start of the implementation of this Regulation, the Commission shall carry out an interim evaluation of the Competence Centre. The Commission shall prepare a report on that evaluation and shall submit that report to the European Parliament and to the Council by 31 December 2024. The Competence Centre and Member States shall provide the Commission with the information necessary for the preparation of that report.

3. The evaluation referred to in paragraph 2 shall include an assessment of the results achieved by the Competence Centre, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the Competence Centre is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Competence Centre set out in Article 46 be extended.

4. On the basis of the conclusions of the interim evaluation referred to in paragraph 2 the Commission may act in accordance with [Article 22(5)] or take any other appropriate actions.

5. The monitoring, evaluation, phasing out and renewal of the contribution from Horizon Europe will follow the provisions of articles 8, 45 and 47 and Annex III of the Horizon Europe Regulation and agreed implementation modalities.

6. The monitoring, reporting and evaluation of the contribution from Digital Europe will follow the provisions of articles 24, 25 of the Digital Europe programme.

7. In case of a winding up of the Competence Centre, the Commission shall conduct a final evaluation of the Competence Centre within six months after the winding-up of the Competence Centre, but no later than two years after the triggering of the winding-up procedure referred to in Article 46 of this Regulation. The results of that final evaluation shall be presented to the European Parliament and to the Council.

Article 39

Liability of the Competence Centre

1. The contractual liability of the Competence Centre shall be governed by the law applicable to the agreement, decision or contract in question.

2. In the case of non-contractual liability, the Competence Centre shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its staff in the performance of their duties.

3. Any payment by the Competence Centre in respect of the liability referred to in paragraphs 1 and 2 and the costs and expenses incurred in connection therewith shall be considered to be expenditure of the Competence Centre and shall be covered by its resources.

4. The Competence Centre shall be solely responsible for meeting its obligations.

Article 40

Jurisdiction of the Court of Justice of the European Union and applicable law

1. The Court of Justice of the European Union shall have jurisdiction:

   (1) pursuant to any arbitration clause contained in agreements, decisions or contracts concluded by the Competence Centre;

   (2) in disputes related to compensation for damage caused by the staff of the Competence Centre in the performance of their duties;

   (3) in any dispute between the Competence Centre and its staff within the limits and under the conditions laid down in the Staff Regulations.

2. Regarding any matter not covered by this Regulation or by other Union legal acts, the law of the Member State where the seat of the Competence Centre is located shall apply.

Article 41

Liability of members and insurance

1. The financial liability of the members for the debts of the Competence Centre shall be limited to their contribution already made for the administrative costs.

2. The Competence Centre shall take out and maintain appropriate insurance.

Article 42

Conflicts of interest

The Competence Centre Governing Board shall adopt rules for the prevention and management of conflicts of interest in respect of its members, bodies and staff. Those rules shall contain the provisions intended to avoid a conflict of interest in respect of the representatives of the members serving in the Governing Board as well as the Scientific and Industrial Advisory Board in accordance with Regulation XXX [new Financial Regulation].

Article 43

Protection of Personal Data

1. The processing of personal data by the Competence Centre shall be subject to Regulation (EU) No XXX/2018 of the European Parliament and of the Council.

2. The Governing Board shall adopt implementing measures referred to in Article xx(3) of Regulation (EU) No xxx/2018. The Governing Board may adopt additional

measures necessary for the application of Regulation (EU) No xxx/2018 by the Competence Centre.

Article 44

Support from the host Member State

An administrative agreement may be concluded between the Competence Centre and the Member State [Belgium] in which its seat is located concerning privileges and immunities and other support to be provided by that Member State to the Competence Centre.

CHAPTER VII

FINAL PROVISIONS

Article 45

Initial actions

1. The Commission shall be responsible for the establishment and initial operation of the Competence Centre until it has the operational capacity to implement its own budget. The Commission shall carry out, in accordance with Union law, all necessary actions with the involvement of the competent bodies of the Competence Centre.

2. For the purpose of paragraph 1, until the Executive Director takes up his duties following his/her appointment by the Governing Board in accordance with Article 16, the Commission may designate an interim Executive Director and exercise the duties assigned to the Executive Director who may be assisted by a limited number of Commission officials. The Commission may assign a limited number of its officials on an interim basis.

3. The interim Executive Director may authorise all payments covered by the appropriations provided in the annual budget of the Competence Centre once approved by the Governing Board and may conclude agreements, decisions and contracts, including staff contracts following the adoption of the Competence Centre's staff establishment plan.

4. The interim Executive Director shall determine, in common accord with the Executive Director of the Competence Centre and subject to the approval of the Governing Board, the date on which the Competence Centre will have the capacity to implement its own budget. From that date onwards, the Commission shall abstain from making commitments and executing payments for the activities of the Competence Centre.

Article 46

Duration

1. The Competence Centre shall be established for the period from 1 January 2021 to 31 December 2029.

2. At the end of this period, unless decided otherwise through a review of this Regulation, the winding-up procedure shall be triggered. The winding-up procedure shall be automatically triggered if the Union or all participating Member States withdraw from the Competence Centre.

3. For the purpose of conducting the proceedings to wind up the Competence Centre, the Governing Board shall appoint one or more liquidators, who shall comply with the decisions of the Governing Board.

4. When the Competence Centre is being wound up, its assets shall be used to cover its liabilities and the expenditure relating to its winding-up. Any surplus shall be distributed among the Union and the participating Member States in proportion to their financial contribution to the Competence Centre. Any such surplus distributed to the Union shall be returned to the Union budget.

Article 47

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

1.2. Policy area(s) concerned in the ABM/ABB structure

1.3. Nature of the proposal/initiative

1.4. Objective(s)

1.5. Grounds for the proposal/initiative

1.6. Duration and financial impact

1.7. Management mode(s) planned

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

2.2. Management and control system

2.3. Measures to prevent fraud and irregularities

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

3.2.2. Estimated impact on operational appropriations

3.2.3. Estimated impact on appropriations of an administrative nature

3.2.4. Compatibility with the current multiannual financial framework

3.2.5. Third-party contributions

3.3. Estimated impact on revenue

LEGISLATIVE FINANCIAL STATEMENT

1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

1.1. Title of the proposal/initiative

Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre

1.2. Policy area(s) concerned in the ABM/ABB structure[35]

Research and innovation European Strategic Investments

1.3. Nature of the proposal/initiative

☒The proposal/initiative relates to **a new action**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[36]

☐ The proposal/initiative relates to **the extension of an existing action**

☐ The proposal/initiative relates to **an action redirected towards a new action**

1.4. Objective(s)

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/initiative

1. A Connected Digital Single Market 2. A New Boost for Jobs, Growth and Investment

1.4.2. Specific objective(s) concerned

Specific objectives 1.3 The digital economy can develop to its full potential underpinned by initiatives enabling full growth of digital and data technologies. 2.1 Europe maintains its position as a world leader in the digital economy, where European companies can grow globally, drawing on strong digital entrepreneurship and performing start-ups and where industry and public services master the digital transformation.

[35] ABM: activity-based management; ABB: activity-based budgeting.

[36] As referred to in Article 54(2)(a) or (b) of the Financial Regulation.

2.2. Europe's research finds investment opportunities for potential technology breakthroughs and flagships, in particular the Horizon 2020/Horizon Europe programme and using Private Public Partnerships.

1.4.3. *Expected result(s) and impact*

Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.

The Competence Centre, together with the Network and the Community, will seek to achieve the following objectives:

(1) contribute to the implementation of the cybersecurity part of the Digital Europe Programme established by Regulation No XXX and in particular actions related to Article 6 of Regulation (EU) No XXX [Digital Europe Programme] and of the Horizon Europe Programme established by Regulation No XXX and in particular Section 2.2.6 of Annex I of Decision No XXX on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation, and of other Union programmes when provided for in legal acts of the Union]

(2) enhance cybersecurity capabilities, knowledge and infrastructures at the service of industries, the public sector and research communities,

(3) contribute to the wide deployment of the latest cyber security products and solutions across the economy,

(4) improve the understanding of cybersecurity and contribute to reducing skills gaps in the Union related to cybersecurity,

(5) contribute to the reinforcement of cybersecurity research and development in the Union,

(6) enhance collaboration between the civilian and defence spheres with regard to dual use technologies and applications,

(7) enhance synergies between the civilian and defence dimensions of cybersecurity,

(8) help coordinate and facilitate the work of the National Coordination Centres Network ('the Network') referred to in Article 10 and the Cybersecurity Competence Community referred to in Article 12.

1.4.4. *Indicators of results and impact*

Specify the indicators for monitoring implementation of the proposal/initiative.

· Number of cybersecurity infrastructure/tools jointly procured.

· Access to testing and experimentation time made possible for European researchers and industry across the Network and within the Centre. Whenever the facilities already exist, increased number of hours available for those communities in comparison to the hours currently available.

· The number of user communities served and number of researchers getting access to the European cybersecurity facilities increases when compared to the number of those having to look for such resources outside Europe.

· Competitiveness of European suppliers starts increasing, measured in terms of global market share (target 25% market share by 2027), and in terms of share of European R&D results taken up by industry.

· Contribution to next cybersecurity technologies, measured in terms of copyright, patents, scientific publications and commercial products.

· Number of cybersecurity skills curricula assessed and aligned, number of cybersecurity professional certification programmes assessed;

· Number of scientists, students, users (industrial and public administrations) trained.

1.5. Grounds for the proposal/initiative

1.5.1. Requirement(s) to be met in the short or long term

Achieve a critical mass of investment in cybersecurity technologic and industrial development, and to overcome the fragmentation of relevant capacities spread across the EU.

1.5.2. Added value of EU involvement

Cybersecurity is an issue of common interest of the Union, as confirmed by the Council Conclusions mentioned above. The scale and cross-border character of incidents such as WannaCry or NonPetya are a point in case. The nature and scale of the cybersecurity technological challenges, as well as insufficient coordination of efforts within and across the industry, public sector and research communities require the EU to further support coordination efforts both to pool a critical mass of resources and ensure better knowledge and assets management. This is needed in view of the resource requirements related to certain capabilities for cybersecurity research, development and deployment; the need to provide access to interdisciplinary cybersecurity know-how across different disciplines (often only partially available at the national level); the global nature of industrial value chains, as well as the activity of global competitors working across the markets.

This requires resources and expertise at a scale that can be hardly matched by the individual action of any Member State. For example, a pan-European quantum communication network could require EU investment in the order of EUR 900 million, depending on the investments by Member States (to be interconnected/complemented) and to what extent the technology will allow the reuse of existing infrastructures.

1.5.3. Lessons learned from similar experiences in the past

The interim evaluation of Horizon2020 amongst others confirmed the continued relevance of EU support to R&D and the societal challenges (amongst them "Secure Societies", from which cybersecurity R&D is supported). At the same time, the evaluation confirms that reinforcing industrial leadership remains a challenge and that there continues to be an innovation gap, with the EU lagging behind in breakthrough, market-creating innovation.

The Connecting Europe Facility (CEF) mid-term evaluation appears to confirm the added value of EU intervention beyond R&D, albeit cybersecurity under CEF had a somewhat different focus (on operational security) and intervention logic. At the same time, the majority of the recipients of CEF cybersecurity grants – the community of national CSIRTs – expressed their wish for a bespoke support programme under the next MFF.

The creation in 2016 of the Public-Private Partnership (cPPP) on cybersecurity in the EU was a solid first step bringing together the research, industry and public sector communities to facilitate research and innovation in cybersecurity and within the limits of the 2014-2020 financial framework should result in good, more focused outcomes in research and innovation. The cPPP allowed industrial partners to express commitment about their individual spending on areas defined in the partnership's Strategic Research and Innovation Agenda.

1.5.4. Compatibility and possible synergy with other appropriate instruments

The Cybersecurity competence network and the European Cybersecurity Industrial, Technology and Research Competence Centre will act as an additional support to existing cybersecurity policy provisions and actors. The mandate of the European Cybersecurity Industrial, Technology and Research Competence Centre will be complementary to ENISA's efforts but has a different focus and requires a different set of skills. While ENISA has a role to play in advising on cybersecurity research and innovation in the EU, its proposed mandate focuses first and foremost on other tasks crucial for strengthening cybersecurity resilience in the EU. The Centre should stimulate the development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level.

The European Cybersecurity Industrial, Technology and Research Competence Centre, together with the Cybersecurity competence network, will also work towards supporting research to facilitate and accelerate standardisation and certification processes, in particular those related to cybersecurity certification schemes in the meaning of the Cybersecurity Act.

The European Cybersecurity Industrial, Technology and Research Competence Centre will act as a single implementation mechanism for two European programmes supporting cybersecurity (Digital Europe Programme, Horizon Europe) and enhance coherence and synergies between them.

This initiative allows to complement the efforts of the Member States by providing appropriate input to education policy makers in order to enhance cybersecurity education (e.g. by developing cybersecurity curricula in civilian and military educational systems but also input for basic cybersecurity education). It would also allow supporting the alignment and continuous assessment of the professional cybersecurity certification programs - all necessary activities to help close the cybersecurity skills gap and facilitate industries' and other communities' access to cybersecurity specialists. Alignment of education and skills will help developing a qualified EU cybersecurity workforce – a key asset for cybersecurity companies as well as other industries with a stake in cybersecurity.

1.6. Duration and financial impact

☒ Proposal/initiative of **limited duration**

– ☒ Proposal/initiative in effect from 01/01/2021 to 31/12/2029

– ☒ Financial impact from 2021 to 2027 for commitment appropriations and from 2021 to 2031 for payment appropriations.

☐ Proposal/initiative of **unlimited duration**

– Implementation with a start-up period from YYYY to YYYY,

– followed by full-scale operation.

1.7. Management mode(s) planned[37]

☐ **Direct management** by the Commission

– ☐ by its departments, including by its staff in the Union delegations;

– ☐ by the executive agencies

☐ **Shared management** with the Member States

☒

Indirect management by entrusting budget implementation tasks to:

– ☐ third countries or the bodies they have designated;

– ☐ international organisations and their agencies (to be specified);

– ☐the EIB and the European Investment Fund;

– ☒ bodies referred to in Articles 70 and 71 of the Financial Regulation;

– ☐ public law bodies;

– ☐ bodies governed by private law with a public service mission to the extent that they provide adequate financial guarantees;

– ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that provide adequate financial guarantees;

– ☐ persons entrusted with the implementation of specific actions in the CFSP pursuant to Title V of the TEU, and identified in the relevant basic act.

– *If more than one management mode is indicated, please provide details in the 'Comments' section.*

[37] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

Article 28 contains detailed provisions on monitoring and reporting.

2.2. Management and control system

2.2.1. Risk(s) identified

To mitigate risks related to the operating of the Competence Centre following its setting-up and delays, the Commission will support the Competence Centre during this phase to ensure swift recruitment of key personnel and the setting up of an efficient internal control system and sound procedures.

2.2.2. Information concerning the internal control system set up

The Executive Director shall be responsible for operations and for the day-to-day management of the Competence Centre and shall be its legal representative. The Director shall be accountable to the Governing Board and report to it on an ongoing basis on the development of the Competence Centre activities. The Governing Board has an overall responsibility for the strategic orientation and the operations of the Competence Centre and shall supervise the implementation of its activities. The financial rules applicable to the Competence Centre shall be adopted by the Governing Board after consulting the Commission. They shall not depart from Regulation (EU) 1271/2013 unless such a departure is specifically required for the Competence Centre's operation and the Commission has given its prior consent. The Commission's internal auditor shall exercise the same powers over the Competence Centre as those exercised in respect of the Commission. The Court of Auditors shall have the power of audit, on the basis of documents and on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Competence Centre.

2.2.3. Estimate of the costs and benefits of the controls and assessment of the expected level of risk of error

Cost and benefits of controls The cost of control for the European Cybersecurity Industrial, Technology and Research Competence Centre are divided between the cost of oversight at Commission level and the cost operational controls at implementing body level. The cost of the controls at the level of the Competence centre is estimated to be around 1,19 % of the operational payment appropriations implemented at the level of the competence centre.

The cost of oversight at Commission level is estimated at 1,20% of the operational payment appropriations implemented at the level of the competence centre.

Under the assumption that the activities would be entirely managed by the Commission without the support of the implementing body, the cost of control would be substantially higher and could be around 7,7% of the payment appropriations.

The controls foreseen aim at ensuring a smooth and effective oversight of the implementing entities by the Commission and at ensuring the necessary degree of assurance at Commission level.

The benefits of the controls are the following:

- Avoiding the selection of weaker or inadequate proposals.
- Optimising the planning, and the use of EU funds, so as to preserve EU added value.
- Ensuring the quality of the grant agreements, avoiding errors in the identification of legal entities, ensuring the correct calculation of the EU Contributions and taking the necessary guarantees for a correct operation of the grants.
- Detection of ineligible costs at payment stage.
- Detection of errors affecting the legality and regularity of operations at audit stage.

Estimated level of error

The aim is to maintain the residual error rate under to the threshold of 2% for the whole Programme, while limiting the control burden for beneficiaries to achieve the right balance between the legality and regularity objective with other objectives such as the attractiveness of the Programme in particular for SMEs and the cost of controls.

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation 883/2013 of the European Parliament and of the Council and Council Regulation (Euratom, EC) No 2185/9640 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the Union' financial interests against fraud and other irregularities with a view to establishing whether there has

been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by the Competence Centre.

Agreements, decisions and contracts resulting from the implementation of this Regulation shall contain provisions expressly empowering the Commission, the Competence Centre, the Court of Auditors and OLAF to conduct audits and investigations, according to their respective competences.

The Competence Centre shall ensure that the financial interests of its members are adequately protected by carrying out or commissioning appropriate internal and external controls.

The Competence Centre shall accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF). The Competence Centre shall adopt the necessary measures to facilitate internal investigations conducted by OLAF.

The Competence Centre will adopt an anti-fraud strategy, based on a fraud risk analysis and cost-benefit considerations. It shall protect the financial interests of the Union by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

3.1. Heading of the multiannual financial framework and new expenditure budget line(s) proposed

- New budget lines requested

In order of multiannual financial framework headings and budget lines:

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.[38]	from EFTA countries[39]	from candidate countries[40]	from third countries	within the meaning of Article [21(2)(b)] of the Financial Regulation
Heading 1: Single Market, Innovation & Digital	01 02 XX XX Horizon Europe Cybersecurity Industrial, Technology and Research Competence Centre – support expenditure 01 02 XX XX Horizon Europe Cybersecurity Industrial, Technology and Research Competence Centre 02 06 01 XX Digital Europe programme Cybersecurity Industrial, Technology and Research Competence Centre – support expenditure 02 06 01 XX Digital Europe programme Cybersecurity Industrial, Technology and Research	Diff.	YES	YES (if specified in annual Work Programme)	YES (limited to some parts of the Programme)	NO

[38] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.
[39] EFTA: European Free Trade Association.
[40] Candidate countries and, where applicable, potential candidates from the Western Balkans.

	Competence Centre					

- The contributions to these budget lines is expected to come from:

EUR million (to three decimal places)

Budget line	Year 2021	Year 2022	Year 2023	Year 2024	Year 2025	Year 2026	Year 2027	**Total**
01 01 01 01 Expenditure related to research officials temporary agents – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 External personnel implementing research programmes – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Other management expenditure for research – Horizon Europe	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Global challenges and Industrial Competitiveness	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 administrative support – Digital Europe programme	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cybersecurity – Digital Europe programme	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1.957,922**
Total expenditure	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1.981,668**

The contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached. The proposal will be based on the outcome of the strategic planning process as defined in Article 6 (6) of Regulation XXX [Horizon Europe framework programme].

The above amounts do not include the contribution from Member States to the operational and administrative costs of the Competence Centre, commensurate to the Union financial contribution.

3.2. Estimated impact on expenditure

3.2.1. Summary of estimated impact on expenditure

EUR million (to three decimal places)

Heading of multiannual financial framework	**1**	Single Market Innovation & Digital

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Post 2027***	**TOTAL**
Title 1 (Staff expenditure)	Commitments = Payments	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Title 2 (Infrastructure & operating expenditures)	Commitments = Payments	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Title 3 (operational expenditure)	Commitments	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1.957,922**
	Payments	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1.061,715	**1.957,922**
TOTAL appropriations for the envelope	Commitments	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1.981,668**

[41] Staff appropriations are only accounted for half a year in 2021

of the programmes[42]	Payments	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1.061,715**	**1.981,668**

[42] The total appropriations set out only relate to the EU financial resources dedicated to cybersecurity under Digital Europe. The contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 5 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached. The proposal will be based on the outcome of the strategic planning process as defined in Article 6 (6) of Regulation XXX [Horizon Europe framework programme].

Heading of multiannual financial framework	7	'Administrative expenditure'

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTAL
Human resources		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Other administrative expenditure		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAL appropriations under HEADING 7 of the multiannual financial framework	(Total commitments = Total payments)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

EUR million (to three decimal places)

		2021	2022	2023	2024	2025	2026	2027	*Post 2027*	TOTAL
TOTAL appropriations across HEADINGS of the multiannual financial framework	Commitments	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2.005,637**
	Payments	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1.²061,715**	**2.005,637**

3.2.2. *Summary of estimated impact on appropriations of an administrative nature*

– ☐ The proposal/initiative does not require the use of appropriations of an administrative nature

– ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below:

EUR million (to three decimal places)

Years	2021	2022	2023	2024	2025	2026	2027	TOTAL
HEADING 7 of the multiannual financial framework								
Human resources	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Other administrative expenditure	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotal HEADING 7 of the multiannual financial framework	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Outside HEADING 7[43] of the multiannual financial framework								
Human resources								
Other expenditure of an administrative nature	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotal outside HEADING 7 of the multiannual financial framework	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
TOTAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

The above appropriations required for human resources and other expenditure of an administrative nature outside Heading 7 correspond to the amounts covered by the Union financial contribution from Digital Europe Programme.

[43] Technical and/or administrative assistance and expenditure in support of the implementation of EU programmes and/or actions (former 'BA' lines), indirect research, direct research.

The appropriations required for human resources and other expenditure of an administrative nature outside Heading 7 will be increased by the amounts covered by the Union financial contribution from Horizon Europe Programme, once the contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached.

The above amounts of appropriations required for human resources and other expenditure of an administrative nature outside Heading 7 do not include the contribution from Member States to the administrative costs of the Competence Centre, commensurate to the Union financial contribution.

3.2.2.1. Estimated requirements of human resources in the Commission

– ☐ The proposal/initiative does not require the use of human resources.

– ■ The proposal/initiative requires the use of human resources, as explained below:

Estimate to be expressed in full time equivalent units

Years		2021	2022	2023	2024	2025	2026	2027
• Establishment plan posts (officials and temporary staff)								
Headquarters and Commission's Representation Offices		20	21	21	21	21	21	22
Delegations								
Research								
• External staff (in Full Time Equivalent unit: FTE) - AC, AL, END, INT and JED [44] Heading 7								
Financed from HEADING 7 of the multiannual financial framework	- at Headquarters	3	3	3	3	3	3	3
	- in Delegations							
Financed from the envelope of the programme [45]	- at Headquarters							
	- in Delegations							
Research								
Other (specify)								
TOTAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

The human resources required will be met by staff from the DG who are already assigned to management of the action and/or have been redeployed within the DG, together if necessary with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

Description of tasks to be carried out:

Officials and temporary staff	Coordination, monitoring and steering of the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre, including support and coordination costs. Policy development and coordination in the field of Cybersecurity in relation to the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre, e.g. with regard to setting priorities for research and industrial policy, general cooperation between Member States and economic operators, consistency

[44] AC= Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JPD= Junior Professionals in Delegations.

[45] Sub-ceiling for external staff covered by operational appropriations (former 'BA' lines).

	with the future EU cybersecurity certification framework, work on liability and duty of care, or coordination with policies on HPC, AI, and digital skills. .
External staff	Coordination, monitoring and steering of the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre, including support and coordination costs. Policy development and coordination in the field of Cybersecurity in relation to the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre, e.g. with regard to setting priorities for research and industrial policy, general cooperation between Member States and economic operators, consistency with the future EU cybersecurity certification framework, work on liability and duty of care, or coordination with policies on HPC, AI, and digital skills. .

3.2.2.2. Estimated requirements of human resources in the Cybersecurity Industrial, Technology and Research Competence Centre

	2021	2022	2023	2024	2025	2026	2027
Commission Officials							
Of which AD							
Of which AST							
Of which AST-SC							
Temporary Agents							
Of which AD	10	11	13	13	13	13	13
Of which AST							
Of which AST-SC							
Contract Agents	26	32	39	39	39	39	39
SNEs	1	1	1	1	1	1	1
Total	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Description of tasks to be carried out:

Officials and temporary staff	Operational implementation of the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre pursuant to Article 4 of this Regulation, including support and coordination costs.
External staff	Operational implementation of the tasks entrusted to the European Cybersecurity Industrial, Technology and Research Competence Centre pursuant to Article 4 of this Regulation, including support and coordination costs.

The above estimated requirements of human resources in the Cybersecurity Industrial, Technology and Research Competence Centre correspond to the estimated requirements to implement the Union financial contribution under Digital Europe.

The above estimated requirements of human resources in the Cybersecurity Industrial, Technology and Research Competence Centre will be increased by the estimated requirements to implement the Union financial contribution under Horizon Europe, once the contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached.

3.2.2.3. Establishment plan of the Cybersecurity Industrial, Technology and Research Competence Centre

Function group and grade	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD Total	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST Total							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
AST/SC Total							
GRAND TOTAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Estimated impact on the staff (additional) – external personnel of the Cybersecurity Industrial, Technology and Research Competence Centre

Contract agents	2021	2022	2023	2024	2025	2026	2027
Function group IV	20	22	29	29	29	29	29
Function group III	2	4	4	4	4	4	4
Function group II	4	6	6	6	6	6	6
Function group I							
Total	**26**	**32**	**39**	**39**	**39**	**39**	**39**

In order to ensure headcount neutrality, the additional staffing in the Cybersecurity Industrial, Technology and Research Competence Centre will be partly offset by reduction in the number of officials and external staff (i.e. establishment plan and external personnel currently in place) in the relevant Commission services.
The staff numbers of the Cybersecurity Industrial, Technology and Research Competence Centre in points 3.2.2.2-4 will be compensated as follows[46]:

TOTAL	2021	2022	2023	2024	2025	2026	2027
Commission officials	5	5	6	6	6	6	6
Temporary agents							
Contract agents	14	17	20	20	20	20	20

[46] Subject to the final amount of the budget whose implementation will be delegated to the Competence Centre

SNEs							
Total FTEs	19	22	26	26	26	26	26
Headcount	19	22	26	26	26	26	26

The compensation of the human resources in the Cybersecurity Industrial, Technology and Research Competence Centre will be commensurate to the share of the Union financial contribution, i.e. 50%.

The above compensation relates to the estimated requirements of human resources in the Cybersecurity Industrial, Technology and Research Competence Centre for implementing the Union financial contribution from Digital Europe.

The above compensation will be increased by the estimated requirements to implement the Union financial contribution from Horizon Europe, once the contribution from the financial envelope of the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached.

3.2.3. *Third-party contributions*

The proposal/initiative:

– ☐ does not provide for co-financing by third parties

– ☒ provides for the co-financing by third parties[47] estimated below:

Appropriations in EUR million (to three decimal places)

Years	2021	2022	2023	2024	2025	2026	2027	TOTAL
Member States – contribution to staff expenditure	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Member States – contribution to Infrastructure & operating expenditures	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Member States – contribution to operational expenditure	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1.957,922**
TOTAL appropriations co-financed	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1.981,668**

The above third-party contribution only relates to the co-financing commensurate to the EU financial resources dedicated to cybersecurity under Digital Europe. The above third-party contribution will be increased once the financial contribution from the cluster 'Inclusive and Secure Society' of Pillar II 'Global Challenges and Industrial Competitiveness' of Horizon Europe (total envelope EUR 2 800 000 000) referred to in Article 21 (1) (b) will be proposed by the Commission during the legislative process and in any case before a political agreement is reached. The proposal will be based on the outcome of the strategic planning process as defined in Article 6 (6) of Regulation XXX [Horizon Europe framework programme].

3.3. Estimated impact on revenue

– ☒ The proposal/initiative has no financial impact on revenue.

– ☐ The proposal/initiative has the following financial impact:

☐ on own resources

☐ on other revenue

please indicate, if the revenue is assigned to expenditure lines ☐

EUR million (to three decimal places)

[47] Estimated in-kind contribution from Member States

Budget revenue line:	Impact of the proposal/initiative[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Article …….							

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

[48] As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20 % for collection costs.