EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

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'')

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The European Union has taken a number of actions to increase resilience and enhance its cybersecurity preparedness. The first EU Cybersecurity Strategy[1] adopted in 2013 set out strategic objectives and concrete actions to achieve resilience, reduce cybercrime, develop cyberdefence policy and capabilities, develop industrial and technological resources and establish a coherent international cyberspace policy for the EU. In that context, important developments have taken place since then, including in particular the second mandate for the European Union Agency for Network and Information Security (ENISA)[2] and the adoption of the **Directive on security of network and information systems**[3] (the 'NIS Directive'), which form the basis for the present proposal.

Furthermore, in **2016 the European Commission adopted a Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry**[4], in which further measures were announced to step-up cooperation, information and knowledge sharing and to increase the EU's resilience and preparedness, also taking into account the prospect of large scale incidents and a possible pan-European cybersecurity crisis. In this context, the Commission announced that it would bring forward the **evaluation** and **review** of Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning ENISA and repealing Regulation (EC) No 460/2004 ("ENISA Regulation"). The evaluation process could lead to a possible reform of the Agency and an enhancement of its capabilities and capacities to support Member States in a sustainable manner. It would therefore give it a more operational and central role in achieving cybersecurity resilience and would acknowledge in its new mandate the Agency's new responsibilities under the NIS Directive.

The NIS Directive is a first essential step with a view to promoting a culture of risk management, by introducing security requirements as legal obligations for the key economic actors, notably operators providing essential services (Operators of Essential Services – OES) and suppliers of some key digital services (Digital Service Providers – DSPs). With security requirements being seen as essential to safeguard the benefits of the evolving digitalisation of society, and given the rapid proliferation of connected devices (the Internet of Things – IoT), the 2016 Communication also put forward the idea of establishing a framework for security certification for ICT products and services in order to increase trust and security in the digital single market. ICT cybersecurity certification becomes particularly relevant in view of the increased use of technologies which require a high level of cybersecurity, such as connected and automated cars, electronic health or industrial automation control systems (IACS).

---

1 Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013).

2 Regulation (EU) 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

3 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

4 Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

These policy measures and announcements were further reinforced by the 2016 **Council Conclusions**, which acknowledged that "cyber threats and vulnerabilities continue to evolve and intensify which will require continued and closer cooperation, especially in handling large-scale cross-border cybersecurity incidents". The conclusions reaffirmed that "the ENISA Regulation is one of the core elements of an EU cyber resilience framework"[5] and called upon the Commission to take further steps to address issue of certification at the European level.

The establishment of a certification system would require the setting-up of an appropriate governance system at EU level, including thorough expertise provided by an independent EU agency. In this respect, the present proposal identifies ENISA as the natural EU-level body competent on cybersecurity matters which should take up such role to bring together, and coordinate the work of, national competent bodies in the field of certification.

In its Communication on the **DSM Strategy Mid-term Review of May 2017**, the Commission further specified that by September 2017 it would review the mandate of ENISA. This in order to define its role in the changed cybersecurity ecosystem and develop measures on cybersecurity standards, certification and labelling to make ICT-based systems, including connected objects, more cyber-secure.[6] The **European Council conclusions** in June 2017[7] welcomed the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions before the end of 2017.

The proposed Regulation provides for a comprehensive set of measures that build on previous actions and fosters mutually reinforcing specific objectives:

- Increasing **capabilities and preparedness** of Member States and businesses;
- Improving **cooperation and coordination** across Member States and EU institutions, agencies and bodies;
- Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises;
- Increasing **awareness** of citizens and businesses on cybersecurity issues;
- Increasing the overall **transparency of cybersecurity assurance**[8] of ICT products and services to strengthen trust in the digital single market and in digital innovation; and
- Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across Member States and sectors.

The following part of the Explanatory Memorandum explains the rationale for the initiative with respect to the proposed actions for ENISA and cybersecurity certification in more detail.

---

5 Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

6 Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy - COM(2017) 228.

7 European Council meeting (22 and 23 June 2017) – Conclusions EUCO 8/17.

8 Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

ENISA

ENISA acts as a centre of expertise dedicated to enhancing network and information security in the Union and supporting capacity building of Members States.

ENISA was set up in 2004[9] to contribute to the overall goal of ensuring a high level of network and information security within the EU. In 2013, Regulation (EU) No 526/2013 established the new mandate of the Agency for a period of seven years, until 2020. The Agency has its offices in Greece, notably the administrative seat in Heraklion (Crete) and the core operations in Athens.

ENISA is a small agency with a low budget and number of staff compared to all EU agencies. It has a fixed-term mandate.

ENISA supports the European institutions, the Member States and the business community in **addressing, responding and especially in preventing network and information security problems**. It does so through a series of activities across five areas identified in its strategy[10]:

- Expertise: provision of information and expertise on key network and information security issues.
- Policy: support to policy making and implementation in the Union.
- Capacity: support for capacity building across the Union (e.g. through trainings, recommendations, awareness raising activities).
- Community: foster the network and information security community (e.g. support to the Computer Emergency Response Teams (CERTs), coordination of pan-European cyber exercises).
- Enabling (e.g. engagement with the stakeholders and international relations).

In the course of the negotiations of the NIS Directive, the EU co-legislators decided to attribute important roles to ENISA in the implementation of this Directive. In particular, the Agency provides the secretariat to the CSIRTs Network (established to promote swift and effective operational cooperation between Member States on specific cybersecurity incidents and sharing information about risks), and it is also called on to assist the Cooperation Group in the execution of its tasks. In addition, the Directive requires ENISA to assist Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practices.

In accordance with the ENISA Regulation, the Commission has carried out an evaluation of the Agency which includes an independent study as well as a public consultation. The evaluation assessed the relevance, impact, effectiveness, efficiency, coherence and EU added value of the Agency with regard to its performance, governance, internal organisational structure and working practices during the period 2013-2016.

The overall performance of ENISA was positively assessed by a majority of respondents[11] (74%) in the public consultation. A majority of respondents furthermore considered ENISA to

[9] Regulation (EC) n° 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1.

[10] https://www.enisa.europa.eu/publications/corporate/enisa-strategy

be achieving its different objectives (at least 63% for each of the objectives). ENISA's services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).

However, a large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate in addressing the current cybersecurity challenges. A large majority of respondents (98%) indicated that an EU body should address these needs, and among them ENISA was considered to be the right organisation to do so by 99% of the respondents. In addition, 67.5 % of respondents expressed the view that ENISA could play a role in establishing a harmonized framework for security certification of IT products and services.

The overall evaluation (based not only on the public consultation but also on a number of individual interviews, additional targeted surveys and workshops) reached the following conclusions:

- ENISA's objectives remain relevant today. In a context of fast technological developments and evolving threats and in view of the growing global cybersecurity risks, there is a clear need in the EU for fostering and further reinforcing high-level technical expertise on cybersecurity issues. Capacities need to be built in the Member States to understand and respond to threats and stakeholders need to cooperate across thematic fields and across institutions.
- Despite its small budget, the Agency has been operationally efficient in the use of its resources and in the implementation of its tasks. The location split between Athens and Heraklion has, however, also generated further administrative costs.
- In terms of effectiveness, ENISA partially met its objectives. The Agency successfully contributed to improving network and information security in Europe by offering capacity building in 28 Member States[12], enhancing cooperation between Member States and network and information security stakeholders, and by providing expertise, community building and support to the development of policies. Overall, ENISA diligently focused on the implementation of its work programme and acted as a trusted partner for its stakeholders, in a field which has only recently been recognised to have such strong cross-border relevance.
- ENISA managed to make an impact, at least to some extent, in the vast field of network and information security, but it has not fully succeeded in developing a strong brand name and gaining sufficient visibility to become recognised as "the"

---

11 90 stakeholders from 19 Member States replied to the consultation (88 responses and 2 position papers), including national authorities from 15 Member States and 8 umbrella organisations representing a significant number of European enterprises.

12 Respondents to the public consultation were asked to comment on what they perceived as ENISA's main achievements over 2013-2016. Respondents from all groups (in total 55, including 13 from national authorities, 20 from private sector and 22 from "other") perceived the following as ENISA's main achievements: 1) The coordination of the Cyber Europe exercises; 2) The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange; 3) ENISA's publications (guidelines and recommendations, threat landscape reports, strategies for incident reporting and crisis management etc.) that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners; 4) Assisting with the promotion of the NIS Directive; 5) Efforts to increase awareness on cybersecurity via the cybersecurity month.

centre of expertise in Europe. The explanation for this lies in the broad mandate of ENISA, which was not equipped with proportionally sufficient resources. Furthermore, ENISA remains the only EU agency with a fixed-term mandate, thus limiting its ability to develop a long-term vision and support its stakeholders in a sustainable manner. This also contrasts with the provisions of the NIS Directive, which entrust ENISA with tasks with no end date. Finally, the assessment found that this limited effectiveness can partly be explained by the high reliance on external expertise over in-house expertise, and by the difficulties in recruiting and retaining specialised staff.

- Last but not least, the evaluation concluded that ENISA's added value lies primarily in the Agency's ability to enhance cooperation mainly between Member States, and especially with related network and information security communities (in particular between CSIRTs). There is no other actor at EU level that supports such broad scope of network and information security stakeholders. However, due to the need to strictly prioritise its activities, ENISA's work programme is mostly guided by the needs of Member States. As a result, it does not sufficiently address the needs of other stakeholders, in particular the industry. It also made the Agency reactive to fulfilling the needs of its key stakeholders, preventing it from achieving a bigger impact. Therefore, the added value provided by the Agency varied according to the diverging needs of its stakeholders and to the extent to which the Agency was able to respond to them (e.g. large versus small Member States; Member States versus industry).

In summary, the results of the stakeholders' consultations and evaluation suggested that ENISA's resources and mandate need to be adapted so that it can play an adequate role in responding to present and future challenges.

In view of these findings, the present proposal reviews the current mandate of ENISA and lays down a renewed set of tasks and functions, with a view to effectively and efficiently supporting Member States, EU institutions and other stakeholders' efforts to ensure a secure cyberspace in the European Union. The new proposed mandate seeks to give the Agency a stronger and more central role, in particular by also supporting Member States in implementing the NIS Directive and to counter particular threats more actively (operational capacity) and by becoming a centre of expertise supporting Member States and the Commission on cybersecurity certification. Under this proposal:

- ENISA would be granted a permanent mandate and thus be put on a stable footing for the future. The mandate, objectives and tasks should still be subject to regular review.
- The proposed mandate further clarifies the role of ENISA as the EU agency for cybersecurity and as the reference point in the EU cybersecurity ecosystem, acting in close cooperation with all the other relevant bodies of such an ecosystem.
- The organisation and the governance of the Agency, which were positively judged in the course of the evaluation, would be moderately reviewed, in particular to make sure that the needs of the wider stakeholders' community are better reflected in the work of the Agency.
- The suggested scope of the mandate is delineated, strengthening those areas where the agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, in particular the NIS

Directive, the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification:

- **EU policy development and implementation:** ENISA would be tasked with proactively contributing to the development of policy in the area of network information security, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. energy, transport, finance). To this end, it would have a strong advisory role, which it could fulfil by providing independent opinions and preparatory work for the development and the update of policy and law. ENISA would also support the EU policy and law in the areas of electronic communications, electronic identity and trust services, with a view to promoting an enhanced level of cybersecurity. In the implementation phase, in particular in the context of the NIS Cooperation Group, ENISA would assist Member States in achieving a consistent approach on the implementation of the NIS Directive across borders and sectors, as well as in other relevant policies and laws. In order to support the regular review of policies and laws in the area of cybersecurity, ENISA would also provide regular reporting on the state of implementation of the EU legal framework.
- **Capacity building:** ENISA would be contributing to the improvement of EU and national public authorities' capabilities and expertise, including on incident response and on the supervision of cybersecurity related regulatory measures. The Agency would also be required to contribute to the establishment of Information Sharing and Analysis Centres (ISACS) in various sectors by providing best practices and guidance on available tools and procedures, as well as by appropriately addressing regulatory issues related to information sharing.
- **Knowledge and information, awareness raising:** ENISA would become the information hub of the EU. This would imply the promotion and sharing of best practices and initiatives across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies. The Agency would also make available advice, guidance and best practices on the security of critical infrastructures. In the aftermath of significant cross-border cybersecurity incidents, ENISA would furthermore compile reports with a view of providing guidance to businesses and citizens across the EU. This stream of work would also involve the regular organisation of awareness raising activities in coordination with Member States authorities.
- **Market related tasks (standardisation, cybersecurity certification):** ENISA would perform a number of functions specifically supporting the internal market and cover a cybersecurity 'market observatory', by analysing relevant trends in the cybersecurity market to better match demand and supply, and by supporting the EU policy development in the ICT standardisation and ICT cybersecurity certification areas. With regard to standardisation in particular, it would facilitate the establishment and uptake of cybersecurity standards. ENISA would also execute the tasks foreseen in the context of the future framework for certification (see below section).
- **Research and innovation:** ENISA would contribute its expertise by advising EU and national authorities on priority-setting in research and development, including in the context of the contractual public-private partnership on cybersecurity (cPPP). ENISA's advice on research would feed into the new

European Cybersecurity Research and Competence Centre under the next multi-annual financial framework. ENISA would also be involved, when asked to do so by the Commission, in the implementation of research and innovation EU funding programmes.

- **Operational cooperation and crisis management:** this stream of work should build on strengthening the existing preventive operational capabilities, in particular upgrading the pan-European cybersecurity exercises (Cyber Europe) by having them on a yearly basis, and on a supporting role in operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by ensuring, among others, the well-functioning of the CSIRTs Network IT infrastructure and communication channels. In this context, a structured cooperation with CERT-EU, European Cybercrime Centre (EC3) and other relevant EU bodies would be required. Furthermore, a structured cooperation with CERT-EU, in close physical proximity, should result in a function to provide technical assistance in case of significant incidents and to support incident analysis. Member States that would request it would receive assistance to handle incidents and support for the analysis of vulnerabilities, artefacts and incidents in order to strengthen their own preventive and response capability.
- ENISA would also play a role in **the EU cybersecurity blueprint** presented as part of this package and setting the Commission's recommendation to Member States for a coordinated response to large-scale cross-border cybersecurity incidents and crises at the EU level[13]. ENISA would facilitate the cooperation between individual Member States in dealing with emergency response by analysing and aggregating national situational reports based on information made available to the Agency on a voluntary basis by Member States and other entities.

- **Cybersecurity certification of ICT products and services**

In order to establish and preserve trust and security, ICT products and services need to directly incorporate security features in the early stages of their technical design and development (security by design). Moreover, customers and users need to be able to ascertain the level of security assurance of the products and services they procure or purchase.

Certification, which consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance, plays an important role in increasing trust and security in products and services. While security evaluations are quite a technical area, certification serves the purpose to inform and reassure purchasers and users about the security properties of the ICT products and services that they buy or use. As mentioned above, this is particularly relevant for new systems that make extensive use of digital technologies and which require a

[13] The "blueprint" will apply to cybersecurity incidents whose disruption is more extensive than any Member State can handle on its own or affects two or more Member States with such a wide-ranging and significant impact or political significance that they require timely policy coordination and response at Union political level.

high level of security, such as e.g. connected and automated cars, electronic health, industrial automation control systems (IACS)[14] or smart grids.

Currently, the landscape of cybersecurity certification of ICT products and services in the EU is quite patchy. There are a number of international initiatives, such as the so-called Common Criteria (CC) for Information Technology Security Evaluation (ISO 15408), which is an international standard for computer security evaluation. It is based on third party evaluation and envisages seven Evaluation Assurance Levels (EAL). The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA. However, within the current version of the CCRA only evaluations up to EAL 2 are mutually recognized. Moreover, only 13 Member States have signed the Arrangement.

The certification authorities from 12 Member States have concluded a mutual recognition agreement regarding the certificates issued in conformity with the agreement on the basis of the Common Criteria[15]. Moreover, a number of ICT certification initiatives currently exist or are being established in Member States. Even if important, these initiatives bear the risk of creating market fragmentation and interoperability issues. As a consequence, a company may need to undergo several certification procedures in various Member States to be able to offer its product on multiple markets. For example, a smart meter manufacturer who wants to sell its products in three Member States, e.g. Germany, France and UK, currently needs to comply with three different certification schemes. These are the Commercial Product Assurance (CPA) in the UK, Certification de Sécurité de Premier Niveau in France (CSPN) and a specific protection profile based on Common Criteria in Germany.

This situation leads to higher costs and constitutes a considerable administrative burden for companies operating in several Member States. While the cost of certification may vary significantly depending on the product/service concerned, the evaluation assurance level sought and/or other components, in general this tends to be quite considerable for businesses. For the BSI "Smart Meter Gateway" certificate, for example, the cost is more than EUR one million (highest level of test and assurance, concerns not only one product but the whole infrastructure around it as well). The cost for smart meters certification in the UK is almost EUR 150 000. In France, the cost is similar to the UK, about EUR 150 000 or more.

Key public and private stakeholders recognised that in the absence of an EU-wide cybersecurity certification scheme, companies in many circumstances have to be certified individually in each Member State, thus leading to market fragmentation. Most importantly, in the absence of EU harmonisation legislation for ICT products and services, differences in cybersecurity certification standards and practices in Member States are liable to create 28 separate security markets in the EU in practice, each one with its own technical requirements, testing methodologies and cybersecurity certification procedures. These divergent approaches at national level are liable to cause – should no adequate action be taken at EU level – a

---

[14] DG JRC has published a report that proposes an initial set of common European requirements and broad guidelines related to cybersecurity certification of IACS components. Available at: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] The Senior Officials Group on Information Systems Security (SOG-IS) includes 12 Member States plus Norway and has developed a few protection profiles on a limited number of products such as digital signature, digital tachograph and smart cards. Participants work together to coordinate the standardisation of CC protection profiles and coordinate the development of protection profiles. Member States often request SOG-IS certification for national public procurement tenders.

significant setback in the achievement of the digital single market, slowing down or preventing the connected positive effects in terms of growth and jobs.

Building on the above developments, the proposed Regulation establishes a European Cybersecurity Certification Framework (the "**Framework**") for ICT products and services and specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The present proposal lays down an overall framework of rules governing European cybersecurity certification schemes. The proposal does not introduce directly operational certification schemes, but rather create a system (framework) for the establishment of specific certification schemes for specific ICT products/services (the "European cybersecurity certification schemes"). The creation of European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.

The general purpose of a European cybersecurity certification scheme is to attest that the ICT products and services that have been certified in accordance with such scheme comply with specified cybersecurity requirements. This for instance would include their ability to protect data (whether stored, transmitted or otherwise processed) against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration. EU cybersecurity certification schemes would make use of existing standards in relation to the technical requirements and evaluation procedures that the products need to comply with and would not develop the technical standards themselves[16]. For instance, an EU-wide certification for products such as smart cards, which are currently tested against international CC standards under the multilateral SOG-IS scheme (and described previously), would mean making this scheme valid throughout the EU.

In addition to outlining a specific set of security objectives to be taken into account in the design of a specific European cybersecurity certification scheme, the proposal provides what the minimum content of such schemes should be. Such schemes will have to define, among others, a number of specific elements setting out the scope and object of the cybersecurity certification. This includes the identification of the categories of products and services covered, the detailed specification of the cybersecurity requirements (for example by reference to the relevant standards or technical specifications), the specific evaluation criteria and methods, and the level of assurance they are intended to ensure (i.e. basic, substantial or high).

European cybersecurity certification schemes will be prepared by ENISA, with the assistance, expert advice and close cooperation of the European Cybersecurity Certification Group (see below), and adopted by the Commission by means of implementing acts. When the need for a cybersecurity certification scheme is identified, the Commission will request ENISA to prepare a scheme for specific ICT products or services. ENISA will work on the scheme in close cooperation with national certification supervisory authorities represented in the Group. Member States and the Group may propose to the Commission that it requests ENISA to prepare a particular scheme.

Certification can be a very expensive process, which in turn could lead to higher prices for customers and consumers. The need to certify may also vary significantly according to the specific context of use of the products and services and fast pace of technological change.

[16] In the case of European standards, this is done through the European standardisation organisations and endorsed by the European Commission in the publication in the *Official Journal* (see Regulation 1025/2012).

Recourse to European cybersecurity certification should therefore remain voluntary, unless otherwise provided in Union legislation laying down security requirements of ICT products and services.

In order to ensure harmonisation and avoid fragmentation, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme will cease to apply from the date established in the implementing act adopting the scheme. Member States should furthermore not introduce new national cybersecurity certification schemes for the ICT products and services covered by an existing European cybersecurity certification scheme.

Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services will be able to submit an application for certification of their products or services to a conformity assessment body of their choice. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements. Accreditation will be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements. Accreditation bodies will revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met, or where actions taken by a conformity assessment body infringe this Regulation.

Under the proposal, the monitoring, supervisory and enforcement tasks lie with the Member States. Member States will have to provide for one certification supervisory authority. This authority will be tasked with supervising the compliance of conformity assessment bodies, as well as of certificates issued by conformity assessment bodies established in their territory, with the requirements of this Regulation and the relevant European cybersecurity certification schemes. National certification supervisory authorities will be competent to handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. To the appropriate extent, they will investigate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they will cooperate with other certification supervisory authorities or other public authorities, for instance by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or with the specific European cybersecurity certification schemes.

Finally, the proposal establishes the European Cybersecurity Certification Group (the 'Group'), consisting of national certification supervisory authorities of all Member States. The main task of the Group is to advise the Commission on issues concerning cybersecurity certification policy and to work with ENISA on the development of draft European cybersecurity certification schemes. ENISA will assist the Commission in providing the secretariat of the Group and maintain an updated public inventory of schemes approved under the European Cybersecurity Certification Framework. ENISA would also liaise with standardisation bodies to ensure the appropriateness of standards used in approved schemes and to identify areas in need of cybersecurity standards.

The European Cybersecurity Certification Framework ('Framework') will provide several benefits for citizens and for undertakings. In particular:

- The creation of EU-wide cybersecurity certification schemes for specific products or services will provide companies with a "one-stop-shop" for cybersecurity certification in the EU. Such companies will be able to certify their product only once and obtain a certificate valid in all Member States. They will not be obliged to re-certify their products under different national certification bodies. This will significantly reduce costs for companies, facilitate cross-border operations and

ultimately reduce and avoid a fragmentation of the internal market for the products concerned.

- The Framework establishes the primacy of European cybersecurity certification schemes over national schemes: under this rule, the adoption of a European cybersecurity certification scheme will supersede all existing parallel national schemes for the same ICT products or services at a given level of assurance. This will bring further clarity, reducing the current proliferation of overlapping and possibly conflicting national cybersecurity certification schemes.
- The proposal supports and complements the implementation of the NIS Directive by providing the undertakings subject to the Directive with a very useful tool to demonstrate compliance with the NIS requirements in the whole Union. In developing new cybersecurity certification schemes, the Commission and ENISA will pay particular attention to the need to ensure that the NIS requirements are reflected in the cybersecurity certification schemes.
- The proposal will support and facilitate the development of a European cybersecurity policy, by harmonising the conditions and substantive requirements for the cybersecurity certification of ICT products and services in the EU. European cybersecurity certification schemes will refer to common standards or criteria of evaluation and testing methodologies. This will contribute significantly, albeit indirectly, to the take-up of common security solutions in the EU, thereby also removing barriers to the internal market.
- The Framework is designed in such a way to ensure the necessary flexibility for cybersecurity certification schemes. Depending on the specific cybersecurity needs, a product or service may be certified against higher or lower levels of security. European cybersecurity certification schemes will be designed with this flexibility in mind and will therefore provide for different levels of assurance (i.e. basic, substantial or high) so that they may be used for different purposes or in different contexts.
- All the above elements will make the cybersecurity certification more attractive for businesses as an effective means to communicate the level of cybersecurity assurance of ICT products or services. To the extent that cybersecurity certification becomes less expensive, more effective and commercially attractive, businesses will have greater incentives to certify their products against cybersecurity risks, thereby contributing to the spread of better cybersecurity practices in the design of ICT products and services (cybersecurity by design).

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

Under the NIS Directive, operators in sectors which are vital for our economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure, as well as digital service providers (i.e. search engines, cloud computing services and online marketplaces) are required to take measures to appropriately manage security risks. The new rules of this proposal complement, and ensure consistency with the provisions of the NIS Directive, in order to pursue still further the cyber resilience of the EU through enhanced capabilities, cooperation, risk management and cyber awareness.

Moreover, the rules on cybersecurity certification provide an essential tool for companies subject to the NIS Directive, as they will be able to certify their ICT products and services

against cybersecurity risks on the basis of cybersecurity certification schemes valid and recognised throughout the EU. They will also be complementary to security requirements mentioned in the eIDAS Regulation[17] and the Radio Equipment Directive[18].

- **Consistency with other Union policies**

The Regulation (EU) 2016/679 (the General Data Protection Regulation, "**GDPR**")[19] lays down provisions to establish certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The present Regulation is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

The proposed Regulation will ensure compatibility with Regulation 765/2008 on accreditation and market surveillance requirements[20] by referring to the rules of that framework on national accreditation bodies and conformity assessment bodies. As far as supervisory authorities are concerned, the proposed Regulation will require Member States to designate national certification supervisory authorities with responsibilities for supervision, monitoring and enforcement of the rules. Those bodies will remain separate from conformity assessment bodies, as prescribed by Regulation 765/2008.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

- **Legal basis**

The legal basis for EU action is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which deals with the approximation of laws of the Member States in order to achieve the objectives of Article 26 TFEU, namely, the proper functioning of the internal market.

The internal market legal basis for establishing ENISA has been upheld by the Court of Justice (in case C-217/04 *United Kingdom vs. European Parliament and Council*) and was further confirmed by the 2013 Regulation which set the current mandate of the Agency. In addition, activities that would reflect the objectives to increase cooperation and coordination among Member States and those adding EU level capabilities to complement the action of Member States would fall under the category of "operational cooperation". This is specifically identified by the NIS Directive (for which Article 114 TFEU is the legal basis) as an objective to be pursued in the context of the CSIRTs Network where "ENISA shall provide the secretariat and shall actively support the cooperation" (Article 12(1)). In particular, Article

[17] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[18] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC

[19] 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) (OJ L 119, 4.5.2016, p. 1–88).

[20] Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

12(f) further outlines the identification of further forms of operational cooperation as task of the CSIRTs Network, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; and (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents.

- The current fragmentation of the certification schemes for ICT products and services is also a result of the lack of a common legally binding and effective framework process applicable to the Member States. This hinders the creation of an internal market for ICT products and services and hampers the competitiveness of the European industry in this sector. The present proposal aims to address the existing fragmentation and the related obstacles to the internal market by providing a common framework for the establishment of cybersecurity certification schemes valid across the EU.

Subsidiarity (for non-exclusive competence)

The subsidiarity principle requires the assessment of the necessity and the added value of the EU action. The respect of subsidiarity in this area was already recognised when adopting the current ENISA Regulation[21].

Cybersecurity is an issue of common interest of the Union. The interdependencies between networks and information systems are such that individual actors (public and private, including citizens) very often cannot face the threats, manage the risks and the possible impacts of cyber incidents in isolation. On the one hand, the interdependencies across Member States, including with regard to the operation of critical infrastructures (energy, transport, water, just to name a few) make public intervention at the European level not only beneficial, but also needed. On the other hand, EU intervention can bring a positive "spill over" effect due to the sharing of good practices across Member States, which can result in an enhanced cybersecurity of the Union.

In summary, in the current context and looking at the future scenarios, it appears that to **increase collective cyber-resilience** of the Union **individual actions by EU Member States and a fragmented approach to cybersecurity** will not be sufficient.

EU action is also deemed necessary to address the fragmentation of the current cybersecurity certification schemes. It would allow manufacturers to fully benefit from an internal market, with significant savings regarding testing and redesign costs. While the current Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA) has for instance achieved important results in this respect, it has also shown important limitations which stand in the way of its suitability in being able to provide a longer term sustainable solutions in fulfilling the full potential of the internal market.

The added value of acting at EU level, in particular to enhance cooperation between Member States, but also between network and information security communities, has been recognised by the 2016 Council Conclusions[22] and it also clearly emerges from the evaluation of ENISA.

---

21 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

22 Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

- **Proportionality**

The proposed measures do not go beyond what is necessary to achieve its policy objectives. Furthermore, the scope of EU intervention does not impede any further national actions in the field of national security matters. EU action is therefore justified on grounds of subsidiarity and proportionality.

- **Choice of the instrument**

The present proposal reviews Regulation (EU) No 526/2013 which sets the current mandate and tasks for ENISA. Furthermore, given ENISA's important role in the setting up and management of an EU cybersecurity certification framework, ENISA's new mandate and the said Framework are best established under one single legal instrument, using the instrument of a Regulation.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

Ex-post evaluations/fitness checks of existing legislation

The Commission, according to the evaluation roadmap[23], assessed the **relevance, impact, effectiveness, efficiency, coherence and the added value** of the Agency with regard to its performance, governance, internal organisational structure and working practices in the period 2013-2016. The main findings can be summarised as follows (for more see the Staff Working Document on the subject, accompanying the impact assessment).

- **Relevance:** In a context of technological developments and evolving threats and considering the significant need for increased cybersecurity in the EU, ENISA's objectives proved to be relevant. Indeed, Member States and EU bodies rely on its substantial expertise on cybersecurity matters. Moreover, capacities need to be built in the Member States to better understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Cybersecurity continues to be a key political priority of the EU to which ENISA is expected to respond; however, ENISA’s design as EU agency with a fixed-term mandate: (i) does not allow for long-term planning and sustainable support to Member States and EU institutions; (ii) may lead to a legal vacuum as the provisions of the NIS Directive entrusting ENISA with tasks are of a permanent nature[24]; (iii) lacks coherence with a vision linking ENISA to an enhanced EU cybersecurity ecosystem.
- **Effectiveness**: ENISA overall met its objectives and implemented its tasks. It made a contribution to increased network and information security in Europe through its main activities (capacity building, provision of expertise, community building, and support to policy). It, however, showed potential for improvement in relation to each. The evaluation concluded that ENISA has effectively created strong and trustful relationships with some of its stakeholders, notably with the Member States and the CSIRTs community. Interventions in the area of capacity building were perceived as effective in particular for less resourced Member States. Stimulating broad cooperation has been one of the highlights, with stakeholders widely agreeing on the

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Reference to Articles 7, 9, 11, 12, 19 of the Directive on Security of Network and Information Systems (NIS Directive).

positive role ENISA plays in bringing people together. However, ENISA faced difficulties to make a big impact in the vast field of network and information security. This was also due to the fact it had fairly limited human and financial resources to meet a very broad mandate. The evaluation also concluded that ENISA partially met the objective of providing expertise, linked to the problems in recruiting experts (see also below in the efficiency section).

- **Efficiency**: Despite its small budget – among the lowest compared to other EU agencies – the Agency has been able to contribute to targeted objectives, showing overall efficiency in the use of its resources. The evaluation concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. One of the main challenges to the Agency's efficiency relates to ENISA's difficulties in recruiting and retaining highly qualified experts. The findings show that this can be explained by a combination of factors, including the general difficulties across the public sector to compete with the private sector when trying to hire highly specialised experts, the type of contracts (fixed term) that the Agency could mostly offer and the somewhat low level of attractiveness related to ENISA's location, for example linked to difficulties encountered by spouses to find work. A location split between Athens and Heraklion required additional efforts of coordination and generated additional costs, but the move to Athens in 2013 of the core operations department increased the Agency's operational efficiency.
- **Coherence**: ENISA's activities have been generally coherent with the policies and activities of its stakeholders, at national and EU level, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and other EU bodies has not been fully utilised. The evolution in the EU legal and policy landscape make the current mandate less coherent today.
- **EU-added value**: ENISA's added value lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related network and information security communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on network and information security. The added value provided by the Agency varied according to the diverging needs and resources of its stakeholders (e.g. large versus small Member States; Member States versus industry) and the need for the Agency to prioritise its activities according to the work programme. The evaluation concluded that a potential discontinuation of ENISA would be a lost opportunity for all Member States. It will not be possible to ensure the same degree of community building and cooperation across the Member States in the field of cybersecurity. Without a more centralised EU agency the picture would be more fragmented, with bilateral or regional cooperation stepping in to fill a void left by ENISA.

With specific regard to ENISA's past performances and future, the main trends emerging from the 2017 consultation are the following[25]:

[25] 90 stakeholders from 19 Member States replied to the consultation (88 responses and 2 position papers), including national authorities from 15 Member States including France, Italy, Ireland and Greece and 8 umbrella organisations representing a significant number of European organisations, for example the European Banking Federation, Digital Europe (representing the digital technology industry in Europe), European Telecommunications Network Operators' Association (ETNO). The ENISA public consultation was complemented by several other sources, including; (i) in-depth interviews, with

- The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%). A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each of the objectives). ENISA's services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).
- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU, in particular the top five (in a list of 16) were: cooperation across Member States; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation across Member States in matters related to cyber security; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks.
- A large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these. A large majority of respondents (98%) indicated that an EU body should respond to these needs and among them ENISA was considered to be the right organisation to do so by 99%.

Stakeholder consultations

- The Commission organised a public consultation for the review of ENISA between 12 April and 5 July, 2016 and received 421 replies[26]. According to the results, 67.5 % of respondents expressed the view that ENISA could play a role in establishing a harmonised framework for security certification of IT products and services.

The results from the 2016 consultation on cybersecurity cPPP[27] on the section on certification show that:

- 50,4% (e.g. 121 out of 240) of respondents do not know whether national certification schemes are mutually recognised across EU Member States. 25.8% (62 out of 240) replied 'No', while 23.8% (57 out of 240) replied 'Yes'.
- 37,9% of respondents (91 out of 240) think that existing certification schemes do not support the needs of Europe's industry. On the other hand, 17, 5% (42 out of 240) – mainly global companies operating on the European market - expressed the opposite view.
- 49.6% (119 out of 240) of respondents says that it is not easy to demonstrate equivalence between standards, certification schemes, and labels. 37.9% (91 out of 240) replied 'I do not know', while only 12,5% (30 out of 240) replied 'Yes'.

approximatively 50 key players in the cybersecurity community; (ii) survey to the CSIRTs Network; (iii) survey to the ENISA Management Board, Executive Board, Permanent Stakeholder Group.

[26] 162 contributions from citizens, 33 from civil society and consumer organisations; 186 from industry and 40 from public authorities, including competent authorities enforcing the ePrivacy Directive.

[27] 240 stakeholders from national public administrations, large businesses, SMEs, microbusinesses and research bodies responded to the section on certification.

Collection and use of expertise

The Commission relied on the following external expert advice:

- Study on the Evaluation of ENISA (Ramboll/Carsa 2017; SMART no. 2016/0077),
- Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (PriceWaterhouseCoopers 2017; SMART no. 2016/0029).

Impact assessment

- The Impact Assessment report on this initiative identified the following main problems to be addressed:
- Fragmentation of policies and approaches to cybersecurity across Member States;
- Dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies; and
- Insufficient awareness and information of citizens and companies, coupled with the growing emergence of multiple national and sectoral certification schemes.

The report assessed the following possible options with regard to ENISA's mandate:

- preservation of the status quo, meaning an extended mandate still limited in time (baseline option);
- expiry of ENISA’s current mandate without renewal and termination of ENISA (no policy intervention);
- a 'reformed ENISA'; and
- an EU cybersecurity agency with full operational capabilities.

The report assessed the following possible options with regard to cybersecurity certification:

- no policy intervention (baseline option);
- non-legislative ("soft law") measures;
- an EU legislative act to create a mandatory system for all Member States based on the SOG-IS system; and
- an EU general ICT cybersecurity security certification framework.

The analysis led to the conclusion that a "reformed ENISA" in combination with an EU general ICT cybersecurity certification framework is the preferred option.

The preferred option has been assessed as the most effective for the EU to reach the identified objectives of: increasing cybersecurity capabilities, preparedness, cooperation, awareness, transparency and avoiding market fragmentation. It has also been assessed as the most coherent with policy priorities of the EU Cybersecurity Strategy and related policies (e.g. NIS Directive), and the Digital Single Market Strategy. In addition, from the consultation process, it emerged that the preferred option enjoys the support of the majority of stakeholders. Furthermore, the analysis conducted in the impact assessment showed that the preferred option would reach the objectives through a reasonable employment of resources.

The Commission’s Regulatory Scrutiny Board delivered initially a negative opinion on 24 July, then a positive opinion on 25 August 2017 upon resubmission. The amended Impact Assessment report included additional supporting evidence, the final conclusions of the

evaluation of ENISA and additional explanations on the policy options and their impact. Annex 1 to the final Impact Assessment report summarizes how the comments of the Board in the second opinion have been addressed. In particular, the report was updated to present in greater detail the EU cybersecurity context, including the measures that are included in the Joint Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", (JOIN(2017) 450) and have a special relevance for ENISA: the EU cybersecurity blueprint and the European Cybersecurity Research and Competence Centre, to which the Agency would link its advisories on EU research needs.

The report explains how the reform of the Agency, including the new tasks, the better conditions of employment and the structural cooperation with EU bodies in the field, would improve its attractiveness as employer and help tackle problems related to the recruitment of experts. Annex 6 to the report also presents a revised estimate of costs associated to the policy options for ENISA. With regard to the topic of certification, the report has been revised to provide a more detailed explanation, including graphic presentation, of the preferred option, as well as to provide estimates on the costs for Member States and the Commission related to the new certification framework. The rationale for the choice of ENISA as key actor in the framework has been further explained based on its expertise in the field and the fact that it is only EU level agency on cybersecurity. Finally, the sections on certification were reviewed to clarify aspects related to the difference between the current SOG-IS system, the benefits associated to the different policy options and explain that fact that the type of ICT product and service covered by a European certification scheme will be defined in the approved scheme itself.

Regulatory fitness and simplification

Not applicable

Impact on fundamental rights

Cybersecurity has an essential role in protecting the privacy and personal data of individuals in accordance with Articles 7 and 8 of the Charter of Fundamental Rights of the EU. In case of cyber incidents the privacy and the protection of our personal data are clearly exposed. Cybersecurity is thus a necessary condition for the respect of privacy and confidentiality of our personal data. Under this perspective, by aiming to reinforce cybersecurity in Europe, the proposal provides an important complement to the existing legislation protecting the fundamental right to privacy and personal data. Cybersecurity is also essential for protecting the confidentiality of our electronic communications and thus for exercising the freedom of expression and information and other related rights, such as the freedom of thought, conscience and religion.

4. BUDGETARY IMPLICATIONS

See financial fiche

5. OTHER ELEMENTS

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

The Commission will monitor the application of the Regulation and submit a report on its evaluation to the European Parliament and to the Council and the European Economic and

Social Committee every five years. These reports will be public and detail the effective application and enforcement of this Regulation.

- **Detailed explanation of the specific provisions of the proposal**

Title I of the Regulation contains the general provisions: the subject matter (Article 1), the definitions (Article 2), including references to relevant definitions from other EU instruments, such as the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), Regulation (EC) No 765/2008 of the European Parliament and of the Council setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, and Regulation (EU) No 1025/2012 of the European Parliament and of the Council on European standardisation.

Title II of the Regulation contains the key provisions related to the ENISA, the EU Cybersecurity Agency.

Chapter I under this Title outlines the mandate (Article 3), objectives (Article 4) and tasks of the Agency (Articles 5 to 11).

Chapter II outlines the organisation of ENISA and includes key provisions on its structure (Article 12). It addresses the composition, voting rules and functions of the Management Board (Section 1, Articles 13 to 17), Executive Board (Section 2, Article 18) and Executive Director (Section 3, Article 19). It also includes provisions on the composition and role of the Permanent Stakeholders' Group (Section 4, Article 20). Last but not least, Section 5 under this Chapter details the operational rules for the Agency, including in relation to programming its operations, conflict of interest, transparency, confidentiality and access to documents (Articles 21-25).

Chapter III concerns the establishment and structure of the Agency's budget (Articles 26 and 27), as well as rules guiding its implementation (Articles 28 and 29). It also includes the provisions facilitating the combating of fraud, corruption and other unlawful activities (Article 30).

Chapter IV relates to the staffing of the Agency. It includes general provisions on the Staff Regulations and the Conditions of Employment and rules guiding privileges and immunity (Article 31 and 32). It also details the rules of engagement and appointment of the Executive Director of the Agency (Article 33). Last but not least, it includes the provisions guiding the use of seconded national experts or other staff not employed by the Agency (Article 34).

Finally, Chapter V contains the general provisions related to the Agency. It outlines the legal status (Article 35) and includes provisions regulating the issues of liability, language arrangements, protection of personal data (Articles 36-38), as well as the security rules on the protection of classified and sensitive non-classified information (Article 40). It describes the rules guiding the Agency's cooperation with third countries and international organisations (Article 39). Last but not least, it also contains provisions regarding the Agency's headquarters and operating conditions, as well as administrative control by the Ombudsman (Articles 41 and 42).

Title III of the Regulation establishes the European cybersecurity certification framework (the "**Framework**") for ICT products and services as *lex generalis* (Article 1). It defines the general purpose of European cybersecurity certification schemes, i.e. to ensure that ICT products and services comply with specified cybersecurity requirements as regards their ability to resist, at a given level of assurance, action that compromise the availability,

authenticity, integrity or confidentiality of stored, transmitted or processed data or the related functions or of services (Article 43). Moreover, it lists the security objectives that European cybersecurity certification schemes shall aim to address (Article 45), such as among others the ability to protect data against accidental or unauthorised access or disclosure, destruction or alteration, and the content (i.e. elements) of European cybersecurity certification schemes, such as the detailed specification of their scope, the security objectives, evaluation criteria etc. (Article 47).

Title III also establishes the main legal effects of European cybersecurity certification schemes, namely (i) the obligation to implement the scheme at national level and the voluntary nature of certification; (ii) the invalidating effect of European cybersecurity certification schemes on national schemes for the same products or services (Articles 48 and 49).

This Title further lays down the procedure for the adoption of European cybersecurity certification schemes and the respective roles of the Commission, ENISA and the European Cybersecurity Certification Group – the 'Group' - (Article 44). Finally, this Title lays down the provisions governing conformity assessment bodies, including their requirements, powers and tasks, national certification supervisory authorities, as well as penalties.

The Group is also established in this Title as an essential body consisting of representatives of national certification supervisory authorities whose main function is to work with ENISA on the preparation of European cybersecurity certification schemes and to advise the Commission on general or specific issues concerning cybersecurity certification policy.

Title IV of the Regulation includes the final provisions describing the exercise of delegation, evaluation requirements, repeal and succession, as well as the entry into force.

2017/0225 (COD)

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'')

(Text with EEA relevance)

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 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[28],

Having regard to the opinion of the Committee of the Regions[29],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Network and information systems and telecommunications networks and services play a vital role for society and have become the backbone of economic growth. Information and communications technology underpins the complex systems which support societal activities, keep our economies running in key sectors such as health, energy, finance and transport, and in particular support the functioning of the internal market.

(2) The use of network and information systems by citizens, businesses and governments across the Union is now pervasive. Digitisation and connectivity are becoming core features in an ever growing number of products and services and with the advent of the Internet of Things (IoT) millions, if not billions, of connected digital devices are expected to be deployed across the EU during the next decade. While an increasing number of devices are connected to the Internet, security and resilience are not sufficiently built in by design, leading to insufficient cybersecurity. In this context, the limited use of certification leads to insufficient information for organisational and individual users about the cybersecurity features of ICT products and services, undermining trust in digital solutions.

(3) Increased digitisation and connectivity lead to increased cybersecurity risks, thus making society at large more vulnerable to cyber threats and exacerbating dangers faced by individuals, including vulnerable persons such as children. In order to

[28] OJ C , , p. .
[29] OJ C , , p. .

mitigate this risk to society, all necessary actions need to be taken to improve cybersecurity in the EU to better protect network and information systems, telecommunication networks, digital products, services and devices used by citizens, governments and business – from SMEs to operators of critical infrastructures – from cyber threats.

(4) Cyber-attacks are on the increase and a connected economy and society that is more vulnerable to cyber threats and attacks requires stronger defences. However, while cyber-attacks are often cross-border, policy responses by cybersecurity authorities and law enforcement competences are predominantly national. Large-scale cyber incidents could disrupt the provision of essential services across the EU. This requires effective EU level response and crisis management, building upon dedicated policies and wider instruments for European solidarity and mutual assistance. Moreover, a regular assessment of the state of cybersecurity and resilience in the Union, based on reliable Union data, as well as systematic forecast of future developments, challenges and threats, both at Union and global level, is therefore important for policy makers, industry and users.

(5) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and foster mutually reinforcing objectives. These include the need to further increase capabilities and preparedness of Member States and businesses, as well as to improve cooperation and coordination across Member States and EU institutions, agencies and bodies. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in the case of large scale cross-border cyber incidents and crises. Additional efforts are also needed to increase awareness of citizens and businesses on cybersecurity issues. Moreover, the trust in the digital single market should be further improved by offering transparent information on the level of security of ICT products and services. This can be facilitated by EU-wide certification providing common cybersecurity requirements and evaluation criteria across national markets and sectors.

(6) In 2004, the European Parliament and the Council adopted Regulation (EC) No 460/2004[30] establishing ENISA with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union, and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations. In 2008, the European Parliament and the Council adopted Regulation (EC) No 1007/2008[31] extending the mandate of the Agency until March 2012. Regulation (EC) No 580/2011[32] extended further the mandate of the Agency until 13 September 2013. In 2013, the European Parliament and the Council adopted Regulation (EU) No 526/2013[33] concerning ENISA and

---

30 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).

31 Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 293, 31.10.2008, p. 1).

32 Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (OJ L 165, 24.6.2011, p. 3).

33 Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p.41).

repealing Regulation (EC)No 460/2004, which extended the Agency's mandate until June 2020.

(7) The Union has already taken important steps to ensure cybersecurity and increase trust in digital technologies. In 2013, an EU Cybersecurity Strategy was adopted to guide the Union's policy response to cybersecurity threats and risks. In its effort to better protect Europeans online, in 2016 the Union adopted the first legislative act in the area of cybersecurity, the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"). The NIS Directive put in place requirements concerning national capabilities in the area of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for economy and society such as energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers (search engines, cloud computing services and online marketplaces). A key role was attributed to ENISA in supporting implementation of this Directive. In addition, effective fight against cybercrime is an important priority in the European Agenda on Security, contributing to the overall aim of achieving a high level of cybersecurity.

(8) It is recognised that, since the adoption of the 2013 EU Cybersecurity Strategy and the last revision of the Agency's mandate, the overall policy context has changed significantly, also in relation to a more uncertain and less secure global environment. In this context and within the framework of the new Union cybersecurity policy, it is necessary to review the mandate of ENISA to define its role in the changed cybersecurity ecosystem and ensure it contributes effectively to the Union's response to cybersecurity challenges emanating from this radically transformed threat landscape, for which, as recognised by the evaluation of the Agency, the current mandate is not sufficient.

(9) The Agency established by this Regulation should succeed ENISA as established by Regulation (EU) No 526/2013. The Agency should carry out the tasks conferred on it by this Regulation and legal acts of the Union in the field of cybersecurity by, among other things, providing expertise and advice and acting as a Union centre of information and knowledge. It should promote the exchange of best practices between Member States and private stakeholders, offering policy suggestions to the European Commission and Member States, acting as a reference point for Union sectoral policy initiatives with regard to cybersecurity matters, fostering operational cooperation between the Member States and between the Member States and the European institutions, agencies and bodies.

(10) Within the framework of Decision 2004/97/EC, Euratom, adopted at the meeting of the European Council on 13 December 2003, the representatives of the Member States decided that ENISA would have its seat in a town in Greece to be determined by the Greek Government. The Agency’s host Member State should ensure the best possible conditions for the smooth and efficient operation of the Agency. It is imperative for the proper and efficient performance of its tasks, for staff recruitment and retention and to enhance the efficiency of networking activities that the Agency be based in an appropriate location, among other things providing appropriate transport connections and facilities for spouses and children accompanying members of staff of the Agency. The necessary arrangements should be laid down in an agreement between the Agency

and the host Member State concluded after obtaining the approval of the Management Board of the Agency.

(11) Given the increasing cybersecurity challenges the Union is facing, the financial and human resources allocated to the Agency should be increased to reflect its enhanced role and tasks, and its critical position in the ecosystem of organisations defending the European digital ecosystem.

(12) The Agency should develop and maintain a high level of expertise and operate as a point of reference establishing trust and confidence in the single market by virtue of its independence, the quality of the advice it delivers and the information it disseminates, the transparency of its procedures and methods of operation, and its diligence in carrying out its tasks. The Agency should proactively contribute to national and Union efforts while carrying out its tasks in full cooperation with the Union institutions, bodies, offices and agencies and the Member States. In addition, the Agency should build on input from and cooperation with the private sector as well as other relevant stakeholders. A set of tasks should establish how the Agency is to accomplish its objectives while allowing flexibility in its operations.

(13) The Agency should assist the Commission by means of advice, opinions and analyses on all the Union matters related to policy and law development, update and review in the area of cybersecurity, including critical infrastructure protection and cyber resilience. The Agency should act as a reference point of advice and expertise for Union sector-specific policy and law initiatives where matters related to cybersecurity are involved.

(14) The underlying task of the Agency is to promote the consistent implementation of the relevant legal framework, in particular the effective implementation of the NIS Directive, which is essential in order to increase cyber resilience. In view of the fast evolving cybersecurity threat landscape, it is clear that Member States must be supported by more comprehensive, cross-policy approach to building cyber resilience.

(15) The Agency should assist the Member States and Union institutions, bodies, offices and agencies in their efforts to build and enhance capabilities and preparedness to prevent, detect and respond to cybersecurity problems and incidents and in relation to the security of network and information systems. In particular, the Agency should support the development and enhancement of national CSIRTs, with a view of achieving a high common level of their maturity in the Union. The Agency should also assist with the development and update of Union and Member States strategies on the security of network and information systems, in particular on cybersecurity, promote their dissemination and track progress of their implementation. The Agency should also offer trainings and training material to public bodies, and where appropriate "train the trainers" with a view to assisting Member States in developing their own training capabilities.

(16) The Agency should assist the Cooperation Group established in the NIS Directive in the execution of its tasks, in particular by providing expertise, advice and facilitate the exchange of best practices, notably with regard to the identification of operators of essential services by Member States, including in relation to cross-border dependencies, regarding risks and incidents.

(17) With a view to stimulating cooperation between public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, the Agency should facilitate the establishment of sectoral Information Sharing and

Analysis Centres (ISACs) by providing best practices and guidance on available tools, procedure, as well as providing guidance on how to address regulatory issues related to information sharing.

(18) The Agency should aggregate and analyse national reports from CSIRTs and CERT-EU, setting up common rules, language and terminology for exchange of information. The Agency should also involve the private sector, within the framework of the NIS Directive which laid down the grounds for voluntary technical information exchange at the operational level with the creation of the CSIRTs Network.

(19) The Agency should contribute to an EU level response in case of large-scale cross-border cybersecurity incidents and crises. This function should include gathering relevant information and acting as facilitator between the CSIRTs Network and the technical community as well as decision makers responsible for crisis management. Furthermore, the Agency could support the handling of incidents from a technical perspective by facilitating relevant technical exchange of solutions between Member States and by providing input into public communications. The Agency should support the process by testing modalities of such cooperation through yearly cybersecurity exercises.

(20) To perform its operational tasks, the Agency should make use of the available expertise of CERT-EU through a structured cooperation, in close physical proximity. The structured cooperation will facilitate the necessary synergies and build-up of ENISA's expertise. Where appropriate, dedicated arrangements between the two organisations should be established to define the practical implementation of such cooperation.

(21) In compliance with its operational tasks, the Agency should be able to provide support to Member States, such as by providing advice or technical assistance, or ensuring analyses of threats and incidents. The Commission's Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises recommends that Member States cooperate in good faith and share amongst themselves and with ENISA information on large-scale cybersecurity incidents and crises without undue delay. Such information should further help ENISA in performing its operational tasks.

(22) As part of the regular cooperation at technical level to support Union situational awareness, the Agency should on regular basis prepare the EU Cybersecurity Technical Situation Report on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact, European Cybercrime Centre (EC3) at Europol, CERT-EU and, where appropriate, European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission, the High Representative of the Union for Foreign Affairs and Security Policy and the CSIRTs Network.

(23) Ex-post technical enquiries into incidents with significant impact in more than one Member State supported or undertaken by the Agency upon request or with the agreement of the concerned Member States should be focused on the prevention of future incidents and be carried out without prejudice to any judicial or administrative proceedings to apportion blame or liability.

(24) The Member States concerned should provide the necessary information and assistance to the Agency, for the purposes of the enquiry without prejudice to Article

346 of the Treaty on the Functioning of the European Union or other public policy reasons.

(25) Member States may invite undertakings concerned by the incident to cooperate by providing necessary information and assistance to the Agency without prejudice to their right to protect commercially sensitive information.

(26) To understand better the challenges in the field of cybersecurity, and with a view to providing strategic long term advice to Member States and Union institutions, the Agency needs to analyse current and emerging risks. For that purpose, the Agency should, in cooperation with Member States and, as appropriate, with statistical bodies and others, collect relevant information and perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on network and information security, in particular cybersecurity. The Agency should furthermore support Member States and Union institutions, agencies and bodies in identifying emerging trends and preventing problems related to cybersecurity, by performing analyses of threats and incidents.

(27) In order to increase the resilience of the Union, the Agency should develop excellence on the subject of security of internet infrastructure and of the critical infrastructures, by providing advice, guidance and best practices. With a view to ensuring easier access to better structured information on cybersecurity risks and potential remedies, the Agency should develop and maintain the "information hub" of the Union, a one-stop-shop portal providing the public with information on cybersecurity deriving from the EU and national institutions, agencies and bodies.

(28) The Agency should contribute towards raising the awareness of the public about risks related to cybersecurity and provide guidance on good practices for individual users aimed at citizens and organisations. The Agency should also contribute to promote best practices and solutions at the level of individuals and organisations by collecting and analysing publicly available information regarding significant incidents, and by compiling reports with a view to providing guidance to businesses and citizens and improving the overall level of preparedness and resilience. The Agency should furthermore organise, in cooperation with the Member States and the Union institutions, bodies, offices and agencies regular outreach and public education campaigns directed to end-users, aiming at promoting safer individual online behaviour and raising awareness of potential threats in cyberspace, including cybercrimes such as phishing attacks, botnets, financial and banking fraud, as well as promoting basic authentication and data protection advice. The Agency should play a central role in accelerating end-user awareness on security of devices.

(29) In order to support the businesses operating in the cybersecurity sector, as well as the users of cybersecurity solutions, the Agency should develop and maintain a "market observatory" by performing regular analyses and dissemination of the main trends in the cybersecurity market, both on the demand and supply side.

(30) To ensure that it fully achieves its objectives, the Agency should liaise with relevant institutions, agencies and bodies, including CERT-EU, European Cybercrime Centre (EC3) at Europol, European Defence Agency (EDA), European Agency for the operational management of large-scale IT systems (eu-LISA), European Aviation Safety Agency (EASA) and any other EU Agency that is involved in cybersecurity. It should also liaise with authorities dealing with data protection in order to exchange know-how and best practices and provide advice on cybersecurity aspects that might

have an impact on their work. Representatives of national and Union law enforcement and data protection authorities should be eligible to be represented in the Agency's Permanent Stakeholders Group. In liaising with law enforcement bodies regarding network and information security aspects that might have an impact on their work, the Agency should respect existing channels of information and established networks.

(31) The Agency, as a Member which furthermore provides the Secretariat of the CSIRTs Network, should support Member State CSIRTs and the CERT-EU in operational cooperation further to all the relevant tasks of the CSIRTs Network, as defined by the NIS Directive. Furthermore, the Agency should promote and support cooperation between the relevant CSIRTs in the event of incidents, attacks or disruptions of networks or infrastructure managed or protected by the CSIRTs and involving or potentially involving at least two CERTs while taking due account of the Standard Operating Procedures of the CSIRTs Network.

(32) With a view to increasing Union preparedness in responding to cybersecurity incidents, the Agency should organise yearly cybersecurity exercises at Union level, and, at their request, support Member States and EU institutions, agencies and bodies in organising exercises.

(33) The Agency should further develop and maintain its expertise on cybersecurity certification with a view to supporting the Union policy in this field. The Agency should promote the uptake of cybersecurity certification within the Union, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthening trust in the digital internal market.

(34) Efficient cybersecurity policies should be based on well-developed risk assessment methods, both in the public and private sector. Risk assessment methods are used at different levels with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public- and private-sector organisations will increase the level of cybersecurity in the Union. To this end, the Agency should support cooperation between stakeholders at Union level, facilitating their efforts relating to the establishment and take-up of European and international standards for risk management and for measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.

(35) The Agency should encourage Member States and service providers to raise their general security standards so that all internet users can take the necessary steps to ensure their own personal cybersecurity. In particular, service providers and product manufacturers should withdraw or recycle products and services that do not meet cybersecurity standards. In cooperation with competent authorities, ENISA may disseminate information regarding the level of cybersecurity of the products and services offered in the internal market, and issue warnings targeting providers and manufacturers and requiring them to improve the security, including cybersecurity, of their products.

(36) The Agency should take full account of the ongoing research, development and technological assessment activities, in particular those carried out by the various Union research initiatives to advise the Union institutions, bodies, offices and agencies

and where relevant, the Member States, at their request, on research needs in the area of network and information security, in particular cybersecurity.

(37) Cybersecurity problems are global issues. There is a need for closer international cooperation to improve security standards, including the definition of common norms of behaviour, and information sharing, promoting swifter international collaboration in response to, as well as a common global approach to, network and information security issues. To that end, the Agency should support further Union involvement and cooperation with third countries and international organisations by providing, where appropriate, the necessary expertise and analysis to the relevant Union institutions, bodies, offices and agencies.

(38) The Agency should be able to respond to ad hoc requests for advice and assistance by Member States and EU institutions, agencies and bodies falling within the Agency's objectives.

(39) It is necessary to implement certain principles regarding the governance of the Agency in order to comply with the Joint Statement and Common Approach agreed upon in July 2012 by the Inter-Institutional Working Group on EU decentralised agencies, the purpose of which statement and approach is to streamline the activities of agencies and improve their performance. The Joint Statement and Common Approach should also be reflected, as appropriate, in the Agency's Work Programmes, evaluations of the Agency, and the Agency's reporting and administrative practice.

(40) The Management Board, composed of the Member States and the Commission, should define the general direction of the Agency's operations and ensure that it carries out its tasks in accordance with this Regulation. The Management 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 Agency, adopt the Agency's Single Programming Document, adopt its own 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.

(41) In order for the Agency to function properly and effectively, the Commission and the Member States should ensure that persons to be appointed to the Management 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 Management Board in order to ensure continuity in its work.

(42) The smooth functioning of the Agency 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. The Executive Director should prepare a proposal for the Agency's work programme, after prior consultation with the Commission, and take all necessary steps to ensure the proper execution of the work programme of the Agency. The Executive Director should prepare an annual report to be submitted to the Management Board, draw up a draft statement of estimates of revenue and expenditure for the Agency, and implement the budget. Furthermore, the Executive Director should have the option of setting up ad hoc Working Groups to address specific matters, in particular of a scientific, technical, legal or socioeconomic nature. The Executive Director should ensure that the ad hoc Working Groups' members are selected according to the highest standards of expertise, taking due account of a representative balance, as appropriate according to

the specific issues in question, between the public administrations of the Member States, the Union institutions and the private sector, including industry, users, and academic experts in network and information security.

(43) The Executive Board should contribute to the effective functioning of the Management Board. As part of its preparatory work related to Management Board decisions, it should examine in detail relevant information and explore available options and offer advice and solutions to prepare relevant decisions of the Management Board.

(44) The Agency should have a Permanent Stakeholders' Group as an advisory body, to ensure regular dialogue with the private sector, consumers' organisations and other relevant stakeholders. The Permanent Stakeholders' Group, set up by the Management Board on a proposal by the Executive Director, should focus on issues relevant to stakeholders and bring them to the attention of the Agency. The composition of the Permanent Stakeholders Group and the tasks assigned to this Group, to be consulted in particular regarding the draft Work Programme, should ensure sufficient representation of stakeholders in the work of the Agency.

(45) The Agency should have in place rules regarding the prevention and the management of conflict of interest. The Agency 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[34]. Processing of personal data by the Agency should be subject to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[35]. The Agency 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.

(46) In order to guarantee the full autonomy and independence of the Agency and to enable it to perform additional and new tasks, including unforeseen emergency tasks, the Agency should be granted a sufficient and autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. The majority of the Agency staff should be directly engaged in the operational implementation of the Agency's mandate. The host Member State, or any other Member State, should be allowed to make voluntary contributions to the revenue of the Agency. The Union's budgetary procedure should remain applicable as far as any subsidies chargeable to the general budget of the Union are concerned. Moreover, the Court of Auditors should audit the Agency's accounts to ensure transparency and accountability.

(47) Conformity assessment is the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled. For the purposes of this Regulation, certification should be considered as a type of conformity assessment regarding the cybersecurity features of a product, process, service, system, or a combination of those ("ICT products and services") by an independent third party, other than the product manufacturer or service provider.

---

34 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).

35 OJ L 8, 12.1.2001, p. 1.

Certification cannot guarantee per se that certified ICT products and services are cyber secure. It is rather a procedure and technical methodology to attest that ICT products and services have been tested and that they comply with certain cybersecurity requirements laid down elsewhere, for example as specified in technical standards.

(48) Cybersecurity certification plays an important role in increasing trust and security in ICT products and services. The digital single market, and particularly the data economy and the Internet of Things, can only thrive if there is general public trust that such products and services provide a certain level of cybersecurity assurance. Connected and automated cars, electronic medical devices, industrial automation control systems or smart grids are only some examples of sectors in which certification is already widely used or is likely to be used in the near future. The sectors regulated by the NIS Directive are also sectors in which cybersecurity certification is critical.

(49) In the 2016 Communication "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", the Commission outlined the need for high-quality, affordable and interoperable cybersecurity products and solutions. The supply of ICT products and services within the single market remains very fragmented geographically. This is because the cybersecurity industry in Europe has developed largely on the basis of national governmental demand. In addition, the lack of interoperable solutions (technical standards), practices and EU-wide mechanisms of certification are among the other gaps affecting the single market in cybersecurity. On the one hand, this makes it difficult for European companies to compete at national, European and global level. On the other, it reduces the choice of viable and usable cybersecurity technologies that individuals and enterprises have access to. Similarly, in the Mid-Term Review on the implementation of the Digital Single Market Strategy, the Commission highlighted the need for safe connected products and systems, and indicated that the creation of a European ICT security framework setting rules on how to organise ICT security certification in the Union could both preserve trust in the internet and tackle the current fragmentation of the cybersecurity market.

(50) Currently, the cybersecurity certification of ICT products and services is used only to a limited extent. When it exists, it mostly occurs at Member State level or in the framework of industry driven schemes. In this context, a certificate issued by one national cybersecurity authority is not in principle recognised by other Member States. Companies thus may have to certify their products and services in several Member States where they operate, for example with a view to participating in national procurement procedures. Moreover, while new schemes are emerging, there seems to be no coherent and holistic approach with regard to horizontal cybersecurity issues, for instance in the field of the Internet of Things. Existing schemes present significant shortcomings and differences in terms of product coverage, levels of assurance, substantive criteria and actual utilisation.

(51) Some efforts have been made in the past in order to lead to a mutual recognition of certificates in Europe. However, they have been only partly successful. The most important example in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). While it represents the most important model for cooperation and mutual recognition in the field of security certification, SOG-IS MRA presents some significant shortcomings related to its high costs and limited scope. So far only a few protection profiles on digital products have been developed, such as digital signature, digital tachograph and smart cards. Most

importantly, SOG-IS includes only part of the Union Member States. This has limited the effectiveness of SOG-IS MRA from the point of view of the internal market.

(52) In view of the above, it is necessary to establish a European cybersecurity certification framework laying down the main horizontal requirements for European cybersecurity certification schemes to be developed and allowing certificates for ICT products and services to be recognised and used in all Member States. The European framework should have a twofold purpose: on the one hand, it should help increase trust in ICT products and services that have been certified according to such schemes. On the other hand, it should avoid the multiplication of conflicting or overlapping national cybersecurity certifications and thus reduce costs for undertakings operating in the digital single market. The schemes should be non-discriminatory and based on international and / or Union standards, unless those standards are ineffective or inappropriate to fulfil the EU's legitimate objectives in that regard.

(53) The Commission should be empowered to adopt European cybersecurity certification schemes concerning specific groups of ICT products and services. These schemes should be implemented and supervised by national certification supervisory authorities and certificates issued within these schemes should be valid and recognised throughout the Union. Certification schemes operated by the industry or other private organisations should fall outside the scope of the Regulation. However, the bodies operating such schemes may propose to the Commission to consider such schemes as a basis for approving them as a European scheme.

(54) The provisions of this Regulation should be without prejudice to Union legislation providing specific rules on certification of ICT products and services. In particular, the General Data Protection Regulation (GDPR) lays down provisions for the establishment of certification mechanisms and data protection seals and marks for the purpose of demonstrating compliance with that Regulation of processing operations by controllers and processors. Such certification mechanisms and data protection seals and marks should allow data subjects to quickly assess the level of data protection of relevant products and services. The present Regulation is without prejudice to the certification of data processing operations, including when such operations are embedded in products and services, under the GDPR.

(55) The purpose of European cybersecurity certification schemes should be to ensure that ICT products and services certified under such a scheme comply with specified requirements. Such requirements concern the ability to resist, at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems within the meaning of this Regulation. It is not possible to set out in detail in this Regulation the cybersecurity requirements relating to all ICT products and services. ICT products and services and related cybersecurity needs are so diverse that it is very difficult to come up with general cybersecurity requirements valid across the board. It is, therefore necessary to adopt a broad and general notion of cybersecurity for the purpose of certification, complemented by a set of specific cybersecurity objectives that need to be taken into account when designing European cybersecurity certification schemes. The modalities with which such objectives will be achieved in specific ICT products and services should then be further specified in detail at the level of the individual certification scheme adopted by the Commission, for example by reference to standards or technical specifications.

(56) The Commission should be empowered to request ENISA to prepare candidate schemes for specific ICT products or services. The Commission, based on the candidate scheme proposed by ENISA, should then be empowered to adopt the European cybersecurity certification scheme by means of implementing acts. Taking account of the general purpose and security objectives identified in this Regulation, European cybersecurity certification schemes adopted by the Commission should specify a minimum set of elements concerning the subject-matter, the scope and functioning of the individual scheme. These should include among others the scope and object of the cybersecurity certification, including the categories of ICT products and services covered, the detailed specification of the cybersecurity requirements, for example by reference to standards or technical specifications, the specific evaluation criteria and evaluation methods, as well as the intended level of assurance: basic, substantial and/or high.

(57) Recourse to European cybersecurity certification should remain voluntary, unless otherwise provided in Union or national legislation. However, with a view to achieving the objectives of this Regulation and avoiding the fragmentation of the internal market, national cybersecurity certification schemes or procedures for the ICT products and services covered by a European cybersecurity certification scheme should cease to produce effects from the date established by the Commission by means of the implementing act. Moreover, Member States should not introduce new national certification schemes providing cybersecurity certification schemes for ICT products and services already covered by an existing European cybersecurity certification scheme.

(58) Once a European cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services should be able to submit an application for certification of their products or services to a conformity assessment body of their choice. Conformity assessment bodies should be accredited by an accreditation body if they comply with certain specified requirements set out in this Regulation. Accreditation should be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements. Accreditation bodies should revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.

(59) It is necessary to require all Member States to designate one cybersecurity certification supervisory authority to supervise compliance of conformity assessment bodies and of certificates issued by conformity assessment bodies established in their territory with the requirements of this Regulation and of the relevant cybersecurity certification schemes. National certification supervisory authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories, investigate to the extent appropriate the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable time period. Moreover, they should cooperate with other national certification supervisory authorities or other public authority, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

(60) With a view to ensuring the consistent application of the European cybersecurity certification framework, a European Cybersecurity Certification Group (the 'Group') consisting of national certification supervisory authorities should be established. The

main tasks of the Group should be to advise and assist the Commission in its work to ensure a consistent implementation and application of the European cybersecurity certification framework; to assist and closely cooperate with the Agency in the preparation of candidate cybersecurity certification schemes; recommend that the Commission request the Agency to prepare a candidate European cybersecurity certification scheme; and to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes.

(61) In order to raise awareness and facilitate the acceptance of future EU cyber security schemes, the European Commission may issue general or sector-specific cyber security guidelines, e.g. on good cyber security practices or responsible cyber security behaviour highlighting the positive effect of the use of certified ICT products and services.

(62) The Agency's support to cybersecurity certification should also include liaising with the Council Security Committee and the relevant national body, regarding the cryptographic approval of products to be used in classified networks.

(63) In order to specify further the criteria for the accreditation of conformity assessment bodies, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission. The Commission should carry out appropriate consultations during its preparatory work, including at expert level. Those consultations should be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council should receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(64) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011.

(65) The examination procedure should be used for the adoption of implementing acts on European cybersecurity certification schemes for ICT products and services; on modalities of carrying enquiries by the Agency; as well as on the circumstances, formats and procedures of notifications of accredited conformity assessment bodies by the national certification supervisory authorities to the Commission.

(66) The Agency’s operations should be evaluated independently. The evaluation should have regard to the Agency achieving its objectives, its working practices and the relevance of its tasks. The evaluation should also assess the impact, effectiveness and efficiency of the European cybersecurity certification framework.

(67) Regulation (EU) No 526/2013 should be repealed.

(68) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather 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:

TITLE I
GENERAL PROVISIONS

Article 1
Subject matter and scope

With a view to ensuring the proper functioning of the internal market while aiming at a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation:

(a) lays down the objectives, tasks and organisational aspects of ENISA, the "EU Cybersecurity Agency", hereinafter 'the Agency'; and

(b) lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union. Such framework shall apply without prejudice to specific provisions regarding voluntary or mandatory certification in other Union acts.

Article 2
Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'cybersecurity' comprises all activities necessary to protect network and information systems, their users, and affected persons from cyber threats;

(2) 'network and information system' means a system within the meaning of point (1) of Article 4 of Directive (EU) 2016/1148;

(3) 'national strategy on the security of network and information systems' means a framework within the meaning of point (3) of Article 4 of Directive (EU) 2016/1148;

(4) 'operator of essential services' means a public or private entity as defined in point (4) of Article 4 of Directive (EU) 2016/1148;

(5) 'digital service provider' means any legal person that provides a digital service as defined in point (6) of Article 4 of Directive (EU) 2016/1148

(6) 'incident' means any event as defined in point (7) of Article 4 of Directive (EU) 2016/1148;

(7) 'incident handling' means any procedure as defined in point (8) of Article 4 of Directive (EU) 2016/1148;

(8) 'cyber threat' means any potential circumstance or event that may adversely impact network and information systems, their users and affected persons.

(9) 'European cybersecurity certification scheme' means the comprehensive set of rules, technical requirements, standards and procedures defined at Union level applying to the certification of Information and Communication Technology (ICT) products and services falling under the scope of that specific scheme;

(10) 'European cybersecurity certificate' means a document issued by a conformity assessment body attesting that a given ICT product or service fulfils the specific requirements laid down in a European cybersecurity certification scheme;

(11) ‘ICT product and service’ means any element or group of elements of network and information systems;

(12) ‘accreditation’ means accreditation as defined in point (10), Article 2 of Regulation (EC) No 765/2008;

(13) ‘national accreditation body’ means a national accreditation body as defined in point (11), Article 2 of Regulation (EC) No 765/2008;

(14) ‘conformity assessment’ means conformity assessment as defined in point (12), Article 2 of Regulation (EC) No 765/2008;

(15) ‘conformity assessment body’ means conformity assessment body as defined in point (13), Article 2 of Regulation (EC) No 765/2008;

(16) ‘standard’ means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012.

TITLE II
ENISA – the "EU Cybersecurity Agency"

CHAPTER I
MANDATE, OBJECTIVES AND TASKS

Article 3
Mandate

1. The Agency shall undertake the tasks assigned to it by this Regulation for the purpose of contributing to a high level of cybersecurity within the Union.
2. The Agency shall carry out tasks conferred upon it by Union acts setting out measures for approximating the laws, regulations and administrative provisions of the Member States which are related to cybersecurity.
3. The objectives and the tasks of the Agency shall be without prejudice to the competences of the Member States regarding cybersecurity, and in any case, without prejudice to activities concerning public security, defence, national security and the activities of the state in areas of criminal law.

Article 4
Objectives

1. The Agency shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers and the information it provides, the transparency of its operating procedures and methods of operation, and its diligence in carrying out its tasks.
2. The Agency shall assist the Union institutions, agencies and bodies, as well as Member States, in developing and implementing policies related to cybersecurity.
3. The Agency shall support capacity building and preparedness across the Union, by assisting the Union, Member States and public and private stakeholders in order to increase the protection of their network and information systems, develop skills and competencies in the field of cybersecurity, and achieve cyber resilience.
4. The Agency shall promote cooperation and coordination at Union level among Member States, Union institutions, agencies and bodies, and relevant stakeholders, including the private sector, on matters related to cybersecurity.
5. The Agency shall increase cybersecurity capabilities at Union level in order to complement the action of Member States in preventing and responding to cyber threats, notably in the event of cross-border incidents.
6. The Agency shall promote the use of certification, including by contributing to the establishment and maintenance of a cybersecurity certification framework at Union level in accordance with Title III of this Regulation, with a view to increasing transparency of cybersecurity assurance of ICT products and services and thus strengthen trust in the digital internal market.

7. The Agency shall promote a high level of awareness of citizens and businesses on issues related to the cybersecurity.

Article 5

Tasks relating to the development and implementation of Union policy and law

The Agency shall contribute to the development and implementation of Union policy and law, by:

1. assisting and advising, in particular by providing its independent opinion and supplying preparatory work, on the development and review of Union policy and law in the area of cybersecurity, as well as sector-specific policy and law initiatives where matters related to cybersecurity are involved;

2. assisting Member States to implement consistently the Union policy and law regarding cybersecurity notably in relation to Directive (EU) 2016/1148, including by means of opinions, guidelines, advice and best practices on topics such as risk management, incident reporting and information sharing, as well as facilitating the exchange of best practices between competent authorities in this regard;

3. contributing to the work of the Cooperation Group pursuant to Article 11 of Directive (EU) 2016/1148, by providing its expertise and assistance;

4. supporting:

   (1) the development and implementation of Union policy in the area of electronic identity and trust services, in particular by providing advice and technical guidelines, as well as facilitating the exchange of best practices between competent authorities;

   (2) the promotion of an enhanced level of security of electronic communications, including by providing expertise and advice, as well as facilitating the exchange of best practices between competent authorities;

5. supporting the regular review of Union policy activities by providing an annual report on the state of implementation of the respective legal framework regarding:

   (a) Member States' incident notifications provided by the single point of contacts to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148;

   (b) notifications of breach of security and loss of integrity regarding the trust service providers, provided by the supervisory bodies to the Agency, pursuant to Article 19(3) of Regulation (EU) 910/2014;

   (c) notifications of breach of security transmitted by the undertakings providing public communications networks or publicly available electronic communications services, provided by the competent authorities to Agency, pursuant to Article 40 of [Directive establishing the European Electronic Communications Code].

Article 6

Tasks relating to capacity building

1. The Agency shall assist:

(a) Member States in their efforts to improve the prevention, detection and analysis, and the capacity to respond to, cybersecurity problems and incidents by providing them with the necessary knowledge and expertise;

(b) Union institutions, bodies, offices and agencies, in their efforts to improve the prevention, detection and analysis of and the capability to respond to cybersecurity problems and incidents through appropriate support for the CERT for the Union institutions, agencies and bodies (CERT-EU);

(c) Member States, at their request, in developing national Computer Security Incident Response Teams (CSIRTs) pursuant to Article 9(5) of Directive (EU) 2016/1148;

(d) Member States, at their request, in developing national strategies on the security of network and information systems, pursuant to Article 7(2) of Directive (EU) 2016/1148; the Agency shall also promote dissemination and track progress of implementation of those strategies across the Union in order to promote best practices;

(e) Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking progress of their implementation;

(f) national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CSIRT meets a common set of minimum capabilities and operates according to best practices;

(g) the Member States by organising yearly large-scale cybersecurity exercises at the Union level referred to in Article 7(6) and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them;

(h) relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders;

(i) the Cooperation Group, by exchanging of best practices, in particular with regard to the identification of operators of essential services by Member States, including in relation to cross-border dependencies, regarding risks and incidents, pursuant to Article 11(3)(l) of Directive (EU) 2016/1148.

2. The Agency shall facilitate the establishment of and continuously support sectoral Information Sharing and Analysis Centres (ISACs), in particular in the sectors listed in Annex II of Directive (EU) 2016/1148, by providing best practices and guidance on available tools, procedure, as well as on how to address regulatory issues related to information sharing.

Article 7

Tasks relating to operational cooperation at Union level

1. The Agency shall support operational cooperation among competent public bodies, and between stakeholders.

2. The Agency shall cooperate at operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, those services dealing with cybercrime and supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern, including:

   (a) the exchange of know-how and best practices;

   (b) the provision of advice and guidelines on relevant issues related to cybersecurity;

   (c) the establishment, upon consultation of the Commission, of practical arrangements for the execution of specific tasks.

3. The Agency shall provide the secretariat of the CSIRTs network, pursuant to Article 12(2) of Directive (EU) 2016/1148 and shall actively facilitate the information sharing and the cooperation among its members.

4. The Agency shall contribute to the operational cooperation within the CSIRTs Network providing support to Member States by:

   (a) advising on how to improve their capabilities to prevent, detect and respond to incidents;

   (b) providing, at their request, technical assistance in case of incidents having a significant or substantial impact;

   (c) analysing vulnerabilities, artefacts and incidents.

In performing these tasks, the Agency and CERT-EU shall engage in a structured cooperation in order to benefit from synergies, in particular regarding operational aspects.

5. Upon a request by two or more Member States concerned, and with the sole purpose of providing advice for the prevention of future incidents, the Agency shall provide support to or carry out an ex-post technical enquiry following notifications by affected undertakings of incidents having a significant or substantial impact pursuant to Directive (EU) 2016/1148. The Agency shall also carry out such an enquiry upon a duly justified request from the Commission in agreement with the concerned Member States in case of such incidents affecting more than two Member States.

   The scope of the enquiry and the procedure to be followed in conducting such enquiry shall be agreed by the concerned Member States and the Agency and is without prejudice to any on-going criminal investigation concerning the same incident. The enquiry shall be concluded by a final technical report compiled by the Agency in particular on the basis of information and comments provided by the concerned Member States and undertaking(s) and agreed with the concerned Member States. A summary of the report focussing on the recommendations for the prevention of future incidents will be shared with the CSIRTs network.

6. The Agency shall organise annual cybersecurity exercises at Union level, and support Member States and EU institutions, agencies and bodies in organising exercises following their request(s). Annual exercises at Union level shall include

technical, operational and strategic elements and help to prepare the cooperative response at the Union level to large-scale cross-border cybersecurity incidents. The Agency shall also contribute to and help organise, where appropriate, sectoral cybersecurity exercises together with relevant ISACs and permit ISACs to participate also to Union level cybersecurity exercises.

7. The Agency shall prepare a regular EU Cybersecurity Technical Situation Report on incidents and threats based on open source information, its own analysis, and reports shared by, among others: Member States' CSIRTs (on a voluntary basis) or NIS Directive Single Points of Contact (in accordance with NIS Directive Article 14 (5)); European Cybercrime Centre (EC3) at Europol, CERT-EU.

8. The Agency shall contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to cybersecurity, mainly by:

   (a) aggregating reports from national sources with a view to contribute to establishing common situational awareness;

   (b) ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs Network and the technical and political decision-makers at Union level;

   (c) supporting the technical handling of an incident or crisis, including facilitating the sharing of technical solutions between Member States;

   (d) supporting public communication around the incident or crisis;

   (e) testing the cooperation plans to respond to such incidents or crises.

Article 8

Tasks relating to the market, cybersecurity certification, and standardisation

The Agency shall:

(a) support and promote the development and implementation of the Union policy on cybersecurity certification of ICT products and services, as established in Title III of this Regulation, by:

   (1) preparing candidate European cybersecurity certification schemes for ICT products and services in accordance with Article 44 of this Regulation;

   (2) assisting the Commission in providing the secretariat to the European Cybersecurity Certification Group pursuant to Article 53 of this Regulation;

   (3) compiling and publishing guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services, in cooperation with national certification supervisory authorities and the industry;

(b) facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products and services, as well as draw up, in collaboration with Member States, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards,

including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148;

(c) perform and disseminate regular analyses of the main trends in the cybersecurity market both on the demand and supply side, with a view of fostering the cybersecurity market in the Union.

Article 9

Tasks relating to knowledge, information and awareness raising

The Agency shall:

(a) perform analyses of emerging technologies and provide topic-specific assessments on expected societal, legal, economic and regulatory impacts of technological innovations on cybersecurity;

(b) perform long-term strategic analyses of cybersecurity threats and incidents in order to identify emerging trends and help prevent problems related to cybersecurity;

(c) provide, in cooperation with experts from Member States authorities, advice, guidance and best practices for the security of network and information systems, in particular for the security of the internet infrastructure and those infrastructures supporting the sectors listed in Annex II of Directive (EU) 2016/1148;

(d) pool, organise and make available to the public, through a dedicated portal, information on cybersecurity, provided by the Union institutions, agencies and bodies;

(e) raise awareness of the public about cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens and organisations;

(f) collect and analyse publicly available information regarding significant incidents and compiling reports with a view to providing guidance to businesses and citizens across the Union;

(g) organise, in cooperation with the Member States and Union institutions, bodies, offices and agencies regular outreach campaigns to increase cybersecurity and its visibility in the Union.

Article 10

Tasks relating to research and innovation

In relation to research and innovation, the Agency shall:

(a) advise the Union and the Member States on research needs and priorities in the area of cybersecurity, with a view to enabling effective responses to current and emerging risks and threats, including with respect to new and emerging information and communications technologies, and to using risk-prevention technologies effectively;

(b) participate, where the Commission has delegated the relevant powers to it, in the implementation phase of research and innovation funding programmes or as a beneficiary.

Article 11

Tasks relating to international cooperation

The Agency shall contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on issues related to cybersecurity, by:

(a) engaging, where appropriate, as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises;

(b) facilitating, upon the request of the Commission, the exchange of best practices between the relevant international organisations;

(c) providing, upon request, the Commission with expertise.

CHAPTER II
ORGANISATION OF THE AGENCY

Article 12

Structure

The administrative and management structure of the Agency shall be composed of the following:

(a) a Management Board which shall exercise the functions set out in Article 14;

(b) an Executive Board which shall exercise the functions set out in Article 18;

(c) an Executive Director who shall exercise the responsibilities set out in Article 19; and

(d) a Permanent Stakeholders' Group which shall exercise the functions set out in Article 20.

SECTION 1
MANAGEMENT BOARD

Article 13

Composition of the Management Board

1. The Management Board shall be composed of one representative of each Member State, and two representatives appointed by the Commission. All representatives shall have voting rights.

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

3. Members of the Management Board and their alternates shall be appointed in light of their knowledge in the field of cybersecurity, taking into account relevant managerial, administrative and budgetary skills. The Commission and Member States shall make efforts to limit the turnover of their representatives in the

Management Board, in order to ensure continuity of that Board's work. The Commission and Member States shall aim to achieve a balanced representation between men and women on the Management Board.

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

Article 14
Functions of the Management Board

1. The Management Board shall:

(a) define the general direction of the operation of the Agency and shall also ensure that the Agency works in accordance with the rules and principles laid down in this Regulation. It shall also ensure consistency of the Agency's work with activities conducted by the Member States as well as at Union level;

(b) adopt the Agency's draft single programming document referred to in Article 21, before its submission to the Commission for its opinion;

(c) adopt, taking into account the Commission opinion, the Agency's single programming document by a majority of two-thirds of members and in accordance with Article 17;

(d) adopt, by a majority of two-thirds of members, the annual budget of the Agency and exercise other functions in respect of the Agency's budget pursuant to Chapter III;

(e) assess and adopt the consolidated annual report on the Agency's activities and send both the report and its assessment by 1 July of the following year, to the European Parliament, the Council, the Commission and the Court of Auditors. The annual report shall include the accounts and describe how the Agency has met its performance indicators. The annual report shall be made public;

(f) adopt the financial rules applicable to the Agency in accordance with Article 29;

(g) 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;

(h) adopt rules for the prevention and management of conflicts of interest in respect of its members;

(i) ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-fraud Office (OLAF) and the various internal or external audit reports and evaluations;

(j) adopt its rules of procedure;

(k) in accordance with paragraph 2, exercise, with respect to the staff of the Agency, the powers conferred by the Staff Regulations of Officials on the Appointing Authority and the Conditions of Employment of Other Servants of the European Union on the Authority Empowered to Conclude a Contract of Employment ("the appointing authority powers");

(l) adopt rules implementing the Staff Regulations and the Conditions of Employment of Other Servants in accordance with the procedure provided for in Article 110 of the Staff Regulations;

(m) appoint the Executive Director and where relevant extend his term of office or remove him from office in accordance with Article 33 of this Regulation;

(n) appoint an Accounting Officer, who may be the Commission's Accounting Officer, who shall be totally independent in the performance of his/her duties;

(o) take all decisions on the establishment of the Agency's internal structures and, where necessary, their modification, taking into consideration the Agency's activity needs and having regard to sound budgetary management;

(p) authorise the conclusion of working arrangements in accordance with Articles 7 and 39.

2. The Management 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 of Other Servants, delegating relevant appointing authority powers to the Executive Director and defining the conditions under which this delegation of powers can be suspended. The Executive Director shall be authorised to sub-delegate those powers.

3. Where exceptional circumstances so require, the Management Board may by way of a decision temporarily suspend the delegation of the appointing authority powers to the Executive Director and those sub-delegated by the latter and exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.

Article 15

Chairperson of the Management Board

The Management Board shall elect by a majority of two-thirds of members its Chairperson and a Deputy Chairperson from among its members for a period of four years, which shall be renewable once. If, however, their membership of the Management 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.

Article 16

Meetings of the Management Board

1. Meetings of the Management Board shall be convened by its Chairperson.

2. The Management Board shall hold at least two ordinary meetings a year. It shall also hold extraordinary meetings at the request of the Chairperson, at the request of the Commission, or at the request of at least a third of its members.

3. The Executive Director shall take part, without voting rights, in the meetings of the Management Board.

4. Members of the Permanent Stakeholder Group may take part, upon invitation from the Chairperson, in the meetings of the Management Board, without voting rights.

5. The members of the Management Board and their alternates may, subject to its Rules of Procedure, be assisted at the meetings by advisers or experts.

6. The Agency shall provide the secretariat for the Management Board.

Article 17
Voting rules of the Management Board

1. The Management Board shall take its decisions by majority of its members.

2. A two-thirds majority of all Management Board members shall be required for the single programming document, the annual budget, the appointment, extension of the term of office or removal of the Executive Director.

3. Each member shall have one vote. In the absence of a member, their alternate shall be entitled to exercise the right to vote.

4. The Chairperson shall take part in the voting.

5. The Executive Director shall not take part in the voting.

6. The Management Board's rules of procedures shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.

SECTION 2
EXECUTIVE BOARD

Article 18
Executive Board

1. The Management Board shall be assisted by an Executive Board.

2. The Executive Board shall:

   (a) prepare decisions to be adopted by the Management Board;

   (b) ensure, together with the Management Board, the adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations;

   (c) without prejudice to the responsibilities of the Executive Director, as set out in Article 19, assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 19.

3. The Executive Board shall be composed of five members appointed from among the members of the Management Board amongst whom the Chairperson of the Management Board, who may also chair the Executive Board, and one of the representatives of the Commission. The Executive Director shall take part in the meetings of the Executive Board, but shall not have the right to vote.

4. The term of office of the members of the Executive Board shall be four years. That term shall be renewable.

5. The Executive Board shall meet at least once every three months. The chairperson of the Executive Board shall convene additional meetings at the request of its members.

6. The Management Board shall lay down the rules of procedure of the Executive Board.

7. When necessary, because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters.

SECTION 3
EXECUTIVE DIRECTOR

Article 19
Responsibilities of the Executive Director

1. The Agency shall be managed by its Executive Director, who shall be independent in the performance of his or her duties. The Executive Director shall be accountable to the Management Board.

2. The Executive Director shall report to the European Parliament on the performance of his or her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.

3. The Executive Director shall be responsible for:

   (a) the day-to-day administration of the Agency;

   (b) implementing the decisions adopted by the Management Board;

   (c) preparing the draft single programming document and submitting it to the Management Board for approval before its submission to the Commission;

   (d) implementing the single programming document and reporting to the Management Board thereon;

   (e) preparing the consolidated annual report on the Agency's activities and presenting it to the Management Board for assessment and adoption;

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

   (g) preparing an action plan following-up conclusions of internal or external audit reports, as well as investigations by the European Ant-fraud Office (OLAF) and reporting on progress twice a year to the Commission and regularly to the Management Board;

   (h) preparing draft financial rules applicable to the Agency

   (i) preparing the Agency's draft statement of estimates of revenue and expenditure and implementing its budget;

   (j) protecting 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;

(k) preparing an anti-fraud strategy for the Agency and presenting it to the Management Board for approval;

(l) developing and maintaining contact with the business community and consumers' organisations to ensure regular dialogue with relevant stakeholders;

(m) other tasks assigned to the Executive Director by this Regulation.

4. Where necessary and within the Agency's mandate, and in accordance with the Agency's objectives and tasks, the Executive Director may set up ad hoc Working Groups composed of experts, including from the Member States' competent authorities. The Management Board shall be informed in advance. The procedures regarding in particular the composition of the Working Groups, the appointment of the experts of the Working Groups by the Executive Director and the operation of the Working Groups shall be specified in the Agency's internal rules of operation.

5. The Executive Director shall decide whether it is necessary to locate members of staff in one or more Member States for the purpose of carrying out the Agency's tasks in an efficient and effective manner. Before deciding to establish a local office the Executive Director shall obtain the prior consent of the Commission, the Management Board and the Member State(s) concerned. The decision shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and duplication of administrative functions of the Agency. An agreement with the Member State(s) concerned shall be reached, where appropriate or required.

SECTION 4
PERMANENT STAKEHOLDERS' GROUP

Article 20
Permanent Stakeholders' Group

1. The Management Board, acting on a proposal by the Executive Director, shall set up a Permanent Stakeholders' Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, consumer groups, academic experts in the cybersecurity, and representatives of competent authorities notified under [Directive establishing the European Electronic Communications Code] as well as of law enforcement and data protection supervisory authorities.

2. Procedures for the Permanent Stakeholders' Group, in particular regarding the number, composition, and the appointment of its members by the Management Board, the proposal by the Executive Director and the operation of the Group, shall be specified in the Agency's internal rules of operation and shall be made public.

3. The Permanent Stakeholders' Group shall be chaired by the Executive Director or by any person the Executive Director appoints on a case-by-case basis.

4. The term of office of the Permanent Stakeholders' Group's members shall be two-and-a-half years. Members of the Management Board may not be members of the Permanent Stakeholders' Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the Permanent Stakeholders' Group and to participate in its work. Representatives of other bodies deemed relevant by the Executive Director, who are not members of the Permanent Stakeholders' Group, may be invited to attend the meetings of the Permanent Stakeholders' Group and to participate in its work.

5. The Permanent Stakeholders' Group shall advise the Agency in respect of the performance of its activities. It shall in particular advise the Executive Director on drawing up a proposal for the Agency's work programme, and on ensuring communication with the relevant stakeholders on all issues related to the work programme.

SECTION 5
OPERATION

Article 21
Single Programming Document

1. The Agency shall carry out its operations in accordance with a single programming document containing its multiannual and annual programming, which shall include all of its planned activities.

2. Each year, the Executive Director shall draw up a draft single programming document containing multiannual and annual programming with the corresponding human and financial resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) No 1271/2013[36] and taking into account guidelines set by the Commission.

3. By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1 and forward it to the European Parliament, the Council and the Commission no later than 31 January of the following year, as well as any later updated version of that document.

4. The single programming document shall become definitive after final adoption of the general budget of the Union and, if necessary, shall be adjusted accordingly.

5. The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multi-annual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.

---

36 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)

6. The Management Board shall amend the adopted annual work programme when a new task is given to the Agency. Any substantial amendment to the annual work programme shall be adopted by the same procedure as the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.

7. The multi-annual work programme shall set out overall strategic programming including objectives, expected results and performance indicators. It shall also set out resource programming including multi-annual budget and staff.

8. The resource programming shall be updated annually. The strategic programming shall be updated wherever appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 56.

Article 22
Declaration of interest

1. Members of the Management Board, the Executive Director and officials seconded by Member States on a temporary basis shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered prejudicial to their independence. The declarations shall be accurate and complete, made annually in writing and updated whenever necessary.

2. Members of the Management Board, the Executive Director, and external experts participating in ad hoc Working Groups shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting upon such points.

3. The Agency shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.

Article 23
Transparency

1. The Agency shall carry out its activities with a high level of transparency and in accordance with Article 25.

2. The Agency 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 22.

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

4. The Agency shall lay down, in its internal rules of operation, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.

Article 24
Confidentiality

1. Without prejudice to Article 25, the Agency 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 Management Board, the Executive Director, the members of the Permanent Stakeholders Group, external experts participating in ad hoc Working Groups, and members of the staff of the Agency including officials seconded by Member States on a temporary basis shall comply with the confidentiality requirements under Article 339 of the Treaty on the Functioning of the European Union (TFEU), even after their duties have ceased.

3. The Agency shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.

4. If required for the performance of the Agency's tasks, the Management Board shall decide to allow the Agency to handle classified information. In that case the Management Board shall, in agreement with the Commission services, adopt internal rules of operation applying the security principles set out in Commission Decisions (EU, Euratom) 2015/443[37] and 2015/444[38]. Those rules shall include provisions for the exchange, processing and storage of classified information.

Article 25
Access to documents

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

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

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

CHAPTER III
ESTABLISHMENT AND STRUCTURE OF THE BUDGET

Article 26
Establishment of the budget

1. Each year, the Executive Director shall draw up a draft statement of estimates of the Agency's revenue and expenditure for the following financial year, and shall forward

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

[38] 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).

it to the Management Board, together with a draft establishment plan. Revenue and expenditure shall be in balance.

2. Each year, the Management 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 Agency for the following financial year.

3. The Management 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 and the third countries with which the Union has concluded agreements in accordance with Article 39.

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 Agency.

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

7. Together with the single programming document, the Management Board shall adopt the Agency's budget. It shall become final following definitive adoption of the general budget of the Union. Where appropriate, the Management Board shall adjust the Agency's budget and single programming document in accordance with the general budget of the Union.

Article 27
Structure of the budget

1. Without prejudice to other resources, the Agency's revenue shall be composed of:

   (a) a contribution from the Union budget;

   (b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 29;

   (c) Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 29 and with the provisions of the relevant instruments supporting the policies of the Union;

   (d) contributions from third countries participating in the work of the Agency as provided for in Article 39;

   (e) any voluntary contributions from Member States in money or in kind; Member States that provide voluntary contributions may not claim any specific right or service as a result thereof.

2. The expenditure of the Agency shall include staff, administrative and technical support, infrastructure and operational expenses, and expenses resulting from contracts entered into with third parties.

Article 28

Implementation of the budget

1. The Executive Director shall be responsible for the implementation of the Agency's budget.
2. The Commission's internal auditor shall exercise the same powers over the Agency as over Commission departments.
3. By 1 March following each financial year (1 March of year N + 1), the Agency's accounting officer shall send the provisional accounts to the Commission's accounting officer and to the Court of Auditors.
4. Upon receipts of the Court of Auditors' observations on the Agency's provisional accounts, the Agency's accounting officer shall draw up the Agency's final accounts under his or her responsibility.
5. The Executive Director shall submit the final accounts to the Management Board for an opinion.
6. The Executive Director shall send, by 31 March of year N + 1, the report on the budgetary and financial management to the European Parliament, the Council, the Commission and the Court of Auditors.
7. The accounting officer shall, by 1 July of year N + 1, transmit the final accounts to the European Parliament, the Council, the accounting officer of the Commission and the Court of Auditors, together with the Management Board's opinion.
8. At the same date as the transmission of his or her final accounts, the accounting officer shall also send to the Court of Auditors a representation letter covering those final accounts, with a copy to the accounting officer of the Commission.
9. The Executive Director shall publish the final accounts by 15 November of the following year.
10. The Executive Director shall send the Court of Auditors a reply to its observations by 30 September of year N + 1 and shall also send a copy of that reply to the Management Board and to the Commission.
11. The Executive Director shall submit to the European Parliament, at the latter's request, all the information necessary for the smooth application of the discharge procedure for the financial year in question, as laid down in Article 165(3) of the Financial Regulation.
12. The European Parliament, acting on a recommendation from the Council, shall, before 15 May of year N + 2, give a discharge to the Executive Director in respect of the implementation of the budget for the year N.

Article 29

Financial Rules

The financial rules applicable to the Agency shall be adopted by the Management Board after consulting the Commission. They shall not depart from Regulation (EU) 1271/2013 unless such a departure is specifically required for the Agency's operation and the Commission has given its prior consent.

Article 30
Combating fraud

1. In order to facilitate the combating of fraud, corruption and other unlawful activities under Regulation (EC) 883/2013 of the European Parliament and of the Council[39], the Agency shall, within six months from the day it becomes operational, accede to the Interinstitutional Agreement of 25 May, 1999 concerning internal investigations by the European Anti-fraud Office (OLAF) and shall adopt the appropriate provisions applicable to all the employees of the Agency, using the template set out in the Annex to that Agreement.

2. 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 Agency.

3. 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 2185/96[40] 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 Agency.

4. Without prejudice to paragraphs 1, 2 and 3, cooperation agreements with third countries and international organisations, contracts, grant agreements and grant decisions of the Agency shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competences.

CHAPTER IV
AGENCY STAFF

Article 31
General provisions

The Staff Regulations and the Conditions of Employment of Other Servants and the rules adopted by agreement between the Union institutions for giving effect to those Staff Regulations shall apply to the staff of the Agency.

---

39 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).

40 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).

Article 32

Privileges and immunity

Protocol No 7 on the Privileges and Immunities of the European Union annexed to the Treaty on European Union and to the TFEU shall apply to the Agency and its staff.

Article 33

Executive Director

1. The Executive Director shall be engaged as a temporary agent of the Agency under Article 2(a) of the Conditions of Employment of Other Servants.
2. The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.
3. For the purpose of concluding the contract of the Executive Director, the Agency shall be represented by the Chairperson of the Management Board.
4. Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.
5. The term of office of the Executive Director shall be five 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 Agency's future tasks and challenges.
6. The Management Board shall reach decisions on appointment, extension of the term of office or removal from office of the Executive Director on the basis of a two-thirds majority of its members with voting rights.
7. The Management 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 five years.
8. The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within three months before any such extension, the Executive Director shall, if invited, make a statement before the relevant committee of the European Parliament and answer Members' questions.
9. An Executive Director whose term of office has been extended may not participate in another selection procedure for the same post.
10. The Executive Director may be removed from office only by decision of the Management Board, acting on a proposal from the Commission.

Article 34

Seconded national experts and other staff

1. The Agency may make use of seconded national experts or other staff not employed by the Agency. The Staff Regulations and the Conditions of Employment of Other Servants shall not apply to such staff.
2. The Management Board shall adopt a decision laying down rules on the secondment to the agency of national experts.

CHAPTER V
GENERAL PROVISIONS

Article 35
***Legal status* of the Agency**

1. The Agency shall be a body of the Union and shall have legal personality.
2. In each Member State, the Agency shall enjoy the most extensive legal capacity accorded to legal persons under national law. It may, in particular, acquire or dispose of movable and immovable property and may be a party to legal proceedings, or both.
3. The Agency shall be represented by its Executive Director.

Article 36
Liability of the Agency

1. The contractual liability of the Agency shall be governed by the law applicable to the contract in question.
2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by the Agency.
3. In the case of non-contractual liability, the Agency shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by it or its servants in the performance of their duties.
4. The Court of Justice of the European Union shall have jurisdiction in any dispute relating to compensation for such damage.
5. The personal liability of its servants towards the Agency shall be governed by the relevant conditions applying to the staff of the Agency.

Article 37
Language arrangements

1. Council Regulation No 1 shall apply to the Agency[41].The Member States and the other bodies appointed by them may address the Agency and receive a reply in the official language of the institutions of the Union of their choice.
2. The translation services required for the functioning of the Agency shall be provided by the Translation Centre for the Bodies of the European Union.

[41] Regulation No 1 determining the languages to be used by the European Atomic Energy Community (OJ 17, 6.10.1958, p. 401).

Article 38

Protection of personal data

1. The processing of personal data by the Agency shall be subject to Regulation EC) No 45/2001 of the European Parliament and of the Council[42].

2. The Management Board shall adopt implementing measures referred to in Article 24(8) of Regulation (EC) No 45/2001. The Management Board may adopt additional measures necessary for the application of Regulation (EC) No 45/2001 by the Agency.

Article 39

Cooperation with third countries and international organisations

1. In so far as is necessary in order to achieve the objectives set out in this Regulation, the Agency may cooperate with the competent authorities of third countries or with international organisations or both. To this end, the Agency may, subject to prior approval by the Commission, establish working arrangements with the authorities of third countries and international organisations. These arrangements shall not create legal obligations incumbent on the Union and its Member States.

2. The Agency shall be open to the participation of third countries that have entered into agreements with the Union to this effect. Under the relevant provisions of these agreements, arrangements shall be made specifying in particular the nature, extent and manner in which those countries will participate in the Agency's work, including provisions relating to participation in the initiatives undertaken by the Agency, financial contributions and staff. As regards staff matters, those arrangements shall, in any event, comply with the Staff Regulations.

3. The Management Board shall adopt a strategy for relations with third countries or international organisations concerning matters for which the Agency is competent. The Commission shall ensure that the agency operates within its mandate and the existing institutional framework by concluding an appropriate working arrangement with the agency's Executive Director.

Article 40

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

In consultation with the Commission, the Agency shall adopt its security rules applying the security principles contained in the Commission's security rules for protecting European Union Classified Information (EUCI) and sensitive non-classified information, as set out in Commission Decisions (EU, Euratom) 2015/443 and 2015/444. This shall cover, inter alia, provisions for the exchange, processing and storage of such information.

Article 41

Headquarters Agreement and operating conditions

1. The necessary arrangements concerning the accommodation to be provided for the Agency in the host Member State and the facilities to be made available by that

[42] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, Agency staff and members of their families shall be laid down in a Headquarters Agreement between the Agency and Member State where the seat is located, concluded after obtaining the approval of the Management Board and no later than [2 years after the entry into force of this Regulation].

2. The Agency's host Member State shall provide the best possible conditions to ensure the proper functioning of the Agency, including the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses.

Article 42
Administrative control

The operations of the Agency shall be supervised by the Ombudsman in accordance with Article 228 TFEU.

TITLE III
CYBERSECURITY CERTIFICATION FRAMEWORK

Article 43

European cybersecurity certification schemes

A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems.

Article 44

Preparation and adoption of a European Cybersecurity Certification Scheme

1. Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission.
2. When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary.
3. ENISA shall transmit the candidate European cybersecurity certification scheme prepared in accordance with paragraph 2 of this Article to the Commission.
4. The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation.
5. ENISA shall maintain a dedicated website providing information on, and publicity of, European cybersecurity certification schemes.

Article 45

Security objectives of European cybersecurity certification schemes

A European cybersecurity certification scheme shall be so designed to take into account, as applicable, the following security objectives:

(a) protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access or disclosure;

(b) protect data stored, transmitted or otherwise processed against accidental or unauthorised destruction, accidental loss or alteration;

(c) ensure that authorised persons, programmes or machines can access exclusively the data, services or functions to which their access rights refer;

(d) record which data, functions or services have been communicated, at what times and by whom;

(e) ensure that it is possible to check which data, services or functions have been accessed or used, at what times and by whom;

(f) restore the availability and access to data, services and functions in a timely manner in the event of physical or technical incident;

(g) ensure that ICT products and services are provided with up to date software that does not contain known vulnerabilities, and are provided mechanisms for secure software updates.

Article 46

Assurance levels of European cybersecurity certification schemes

1. A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ICT products and services issued under that scheme.

2. The assurance levels basic, substantial and high shall meet the following criteria respectively:

(a) assurance level basic shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of cybersecurity incidents;

(b) assurance level substantial shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a substantial degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of cybersecurity incidents;

(c) assurance level high shall refer to a certificate issued in the context of a European cybersecurity certification scheme, which provides a higher degree of confidence in the claimed or asserted cybersecurity qualities of an ICT product or service than certificates with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent cybersecurity incidents.

Article 47

Elements of European cybersecurity certification schemes

1. A European cybersecurity certification scheme shall include the following elements:

(a) subject-matter and scope of the certification, including the type or categories of ICT products and services covered;

(b) detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by reference to Union or international standards or technical specifications;

(c) where applicable, one or more assurance levels;

(d) specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved;

(e) information to be supplied to the conformity assessment bodies by an applicant which is necessary for certification;

(f) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;

(g) where surveillance is part of the scheme, the rules for monitoring compliance with the requirements of the certificates, including mechanisms to demonstrate the continued compliance with the specified cybersecurity requirements;

(h) conditions for granting, maintaining, continuing, extending and reducing the scope of certification;

(i) rules concerning the consequences of non-conformity of certified ICT products and services with the certification requirements;

(j) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products and services are to be reported and dealt with;

(k) rules concerning the retention of records by conformity assessment bodies;

(l) identification of national cybersecurity certification schemes covering the same type or categories of ICT products and services;

(m) the content of the issued certificate.

2. The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.

3. Where a specific Union act so provides, certification under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that act.

4. In the absence of harmonised Union legislation, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

Article 48

Cybersecurity certification

1. ICT products and services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 44 shall be presumed to be compliant with the requirements of such scheme.

2. The certification shall be voluntary, unless otherwise specified in Union law.

3. A European cybersecurity certificate pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44.

4. By the way of derogation from paragraph 3, in duly justified cases a particular European cybersecurity scheme may provide that a European cybersecurity certificate resulting from that scheme can only be issued by a public body. Such public body shall be one of the following:

   (a) a national certification supervisory authority referred to in Article 50(1)

   (b) a body that is accredited as conformity assessment body pursuant to Article 51(1) or

   (c) a body established under laws, statutory instruments, or other official administrative procedures of a Member State concerned and meeting the requirements for bodies certifying products, processes and services further to ISO/IEC 17065:2012.

5. The natural or legal person which submits its ICT products or services to the certification mechanism shall provide the conformity assessment body referred to in Article 51 with all information necessary to conduct the certification procedure.

6. Certificates shall be issued for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met.

7. A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.

Article 49

National cybersecurity certification schemes and certificates

1. Without prejudice to paragraph 3, national cybersecurity certification schemes and the related procedures for the ICT products and services covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant Article 44(4). Existing national cybersecurity certification schemes and the related procedures for the ICT products and services not covered by a European cybersecurity certification scheme shall continue to exist.

2. Member States shall not introduce new national cybersecurity certification schemes for ICT products and services covered by a European cybersecurity certification scheme in force.

3. Existing certificates issued under national cybersecurity certification schemes shall remain valid until their expiry date.

Article 50

National certification supervisory authorities

1. Each Member State shall appoint a national certification supervisory authority.

2. Each Member State shall inform the Commission of the identity of the authority appointed.

3. Each national certification supervisory authority shall, in its organisation, funding decisions, legal structure and decision-making, be independent of the entities they supervise.

4. Member States shall ensure that national certification supervisory authorities have adequate resources to exercise their powers and to carry out, in an effective and efficient manner, the tasks assigned to them.

5. For the effective implementation of the regulation, it is appropriate that these authorities participate in the European Cybersecurity Certification Group established pursuant to Article 53 in an active, effective, efficient and secure manner.

6. National certification supervisory authorities shall:

   (a) monitor and enforce the application of the provisions under this Title at national level and supervise compliance of the certificates that have been issued by conformity assessment bodies established in their respective territories with the requirements set out in this Title and in the corresponding European cybersecurity certification scheme;

   (b) monitor and supervise the activities of conformity assessment bodies for the purpose of this Regulation, including in relation to the notification of conformity assessment bodies and the related tasks set out in Article 52 of this Regulation;

   (c) handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories, investigate, to the extent appropriate, the subject matter of the complaint, and inform the complainant of the progress and the outcome of the investigation within a reasonable time period;

   (d) cooperate with other national certification supervisory authorities or other public authorities, including by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific European cybersecurity certification schemes;

   (e) monitor relevant developments in the field of cybersecurity certification.

7. Each national certification supervisory authority shall have at least the following powers:

   (a) to request conformity assessment bodies and European cybersecurity certificate holders to provide any information it requires for the performance of its task;

   (b) to carry out investigations, in the form of audits, of conformity assessment bodies and European cybersecurity certificates' holders, for the purpose of verifying compliance with the provisions under Title III;

   (c) to take appropriate measures, in accordance with national law, in order to ensure that conformity assessment bodies or certificate holders comply with this Regulation or with a European cybersecurity certification scheme;

   (d) to obtain access to any premises of conformity assessment bodies and European cybersecurity certificates' holders for the purpose of carrying out investigations in accordance with Union or Member State procedural law;

(e) to withdraw, in accordance with national law, certificates that are not compliant with this Regulation or a European cybersecurity certification scheme;

(f) to impose penalties, as provided for in Article 54, in accordance with national law, and to require the immediate cessation of the breaches of obligations set out in this Regulation.

8. National certification supervisory authorities shall cooperate amongst each other and the Commission and, in particular, exchange information, experiences and good practices as regards cybersecurity certification and technical issues concerning cybersecurity of ICT products and services.

Article 51
Conformity assessment bodies

1. The conformity assessment bodies shall be accredited by the national accreditation body named pursuant to Regulation (EC) No 765/2008 only when they meet the requirements set out in the Annex to this Regulation.

2. Accreditation shall be issued for a maximum of five years and may be renewed on the same conditions provided that the conformity assessment body meets the requirements set out in this Article. Accreditation bodies shall revoke an accreditation of a conformity assessment body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.

Article 52
Notification

1. For each European cybersecurity certification scheme adopted pursuant Article 44, national certification supervisory authorities shall notify the Commission of the accredited conformity assessment bodies accredited to issue certificates at specified assurance levels as referred to in Article 46 and, without undue delay, of any subsequent changes thereto.

2. One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of notified conformity assessment bodies in the Official Journal.

3. If the Commission receives a notification after the expiry of the period referred to in paragraph 1, it shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within two months from the date of receipt of that notification.

4. A national certification supervisory authority may submit to the Commission a request to remove a conformity assessment body notified by that Member State from the list referred to in paragraph 2 of this Article. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the national certification supervisory authority’s request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 55(2).

Article 53
European Cybersecurity Certification Group

1. The European Cybersecurity Certification Group (the 'Group') shall be established.
2. The Group shall be composed of national certification supervisory authorities. The authorities shall be represented by the heads or by other high level representatives of national certification supervisory authorities.
3. The Group shall have the following tasks:
   (a) to advise and assist the Commission in its work to ensure a consistent implementation and application of the present Title, in particular regarding cybersecurity certification policy issues, coordination of policy approaches, and the preparation of European cybersecurity certification schemes;
   (b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme in accordance with Article 44 of this Regulation;
   (c) to propose to the Commission that it requests the Agency to prepare a candidate European cybersecurity certification scheme in accordance with Article 44 of this Regulation;
   (d) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;
   (e) to examine the relevant developments in the field of cybersecurity certification and exchange good practices on cybersecurity certification schemes;
   (f) to facilitate the cooperation between national certification supervisory authorities under this Title through the exchange of information, in particular by establishing methods for the efficient exchange of information relating to all issues concerning cybersecurity certification.
4. The Commission shall chair the Group and provide the secretariat to it, with the assistance of ENISA as provided for in Article 8(a).

Article 54
Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Title and European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall [by …/without delay] notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.

TITLE IV
FINAL PROVISIONS

Article 55
Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No 182/2011 shall apply.

Article 56
Evaluation and review

1. Not later than five years after the date referred to in Article 58, and every five years thereafter, the Commission shall assess the impact, effectiveness and efficiency of the Agency and its working practices and the possible need to modify the mandate of the Agency and the financial implications of any such modification. The evaluation shall take into account any feedback made to the Agency in response to its activities. Where the Commission considers that the continuation of the Agency is no longer justified with regard to its assigned objectives, mandate and tasks, it may propose that this Regulation be amended with regard to the provisions related to the Agency.

2. The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products and services in the Union and improving the functioning of the internal market.

3. The Commission shall forward the evaluation report together with its conclusions to the European Parliament, the Council and the Management Board. The findings of the evaluation report shall be made public.

Article 57
Repeal and succession

1. Regulation (EC) No 526/2013 is repealed with effect from [….].

2. References to Regulation (EC) No 526/2013 and to ENISA shall be construed as references to this Regulation and to the Agency.

3. The Agency succeeds the Agency that was established by Regulation (EC) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All existing decisions of the Management Board and Executive Board remain valid, providing they are not in conflict with the provisions of this Regulation.

4. The Agency shall be established for an indefinite period of time starting from […]

5. The Executive Director appointed pursuant to Article 24(4) of Regulation (EC) No 526/2013 shall be the Executive Director of the Agency for the remaining part of his term of office.

6. The Members and their alternates of the Management Board appointed pursuant to Article 6 of Regulation (EC) No 526/2013 shall be the Members and their alternates of the Management Board of the Agency for the remaining part of their term of office.

Article 58

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

2. 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

Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Network and Information Security (ENISA, the "EU cybersecurity agency") and repealing Regulation (EU) 526/2013, and on Information and Communication Technology security certification ("Cybersecurity Act/Regulation")

1.2. Policy area(s) concerned

Policy area: 09 - Communications networks, content and technology

Activity: 09.02 digital single market

1.3. Nature of the proposal/initiative

☒ The proposal/initiative relates to **a new action (Title III – Certification)**

☐ The proposal/initiative relates to **a new action following a pilot project/preparatory action**[43]

☒The proposal/initiative relates to **the extension of an existing action** (**Title II – ENISA's mandate)**

☐ 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. Increase the resilience of the Member States, businesses and the EU as a whole

2. Ensure the proper functioning of the EU internal market for ICT products and services

3. Increase the global competitiveness of the EU companies operating in the ICT field.

4. Approximate the laws, regulations and administrative provisions of the Member States which require security of network and information systems [or cybersecurity]

1.4.2. Specific objective(s)

With the general objectives in mind, in the broader context of the reviewed Cybersecurity Strategy, the instrument, by delineating the scope and mandate of ENISA and establishing European certification framework for ICT products and services, intends to achieve the following specific objectives:

1. Increase **capabilities and preparedness** of Member States and businesses
2. Improve **cooperation and coordination** across Member States and EU, institutions, agencies and bodies.
3. Increase **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.
4. Increase **awareness** of citizens and businesses on cybersecurity issues.
5. Strengthen trust in the digital single market and in digital innovation through increasing the overall **transparency of cybersecurity assurance**[44] of ICT products

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

and services.

ENISA will contribute to achieving the above objectives through:

Enhanced policy making support – provide guidance and advice to the Commission and the Member States to update and develop a holistic normative framework in the field of cybersecurity as well as sector-specific policy and law initiatives where cybersecurity matters are involved; contribute to the work of the Cooperation Group (art. 11 of Directive (EU) 2016/1148) by providing expertise and assistance; support policy development and implementation in the area of electronic identity and trust services; promote exchange of best practices among competent authorities;

Enhanced capacity building support - provide support to Member States, the Union institutions, bodies, offices and agencies to develop and improve the prevention, detection, analysis as well as the capacity to respond to [cybersecurity] problems and incidents; assist Member States, upon their request, in developing national CSIRTs, national cybersecurity strategies; assist Union institutions in developing and reviewing of Union's cybersecurity strategies; providing cybersecurity trainings; assisting Member States through the Cooperation Group in exchanging best practices; facilitating the establishment of sectoral Information Sharing and Analysis Centres (ISACs).

Operational cooperation and crisis management support – support cooperation among competent public bodies and between stakeholders through establishing systematic cooperation with Union institutions, bodies, offices and agencies dealing with cybersecurity, cybercrime and the protection of privacy and personal data; providing the secretariat of the CSIRTs Network (art. 12(2) of Directive (EU) 2016/1148) as well as contribute to the operational cooperation within the Network by providing, in cooperation with CERT-EU, support to Member States, at their request; organise regular cybersecurity exercises; contribute to developing a cooperative response to the large scale cross-border cybersecurity incidents and crises; conduct, in cooperation with CSIRTs Network ex-post technical enquiries of significant incidents and issue follow-up recommendations;

Market related tasks (standardisation, certification) - perform a number of functions specifically supporting the internal market: cybersecurity 'market observatory', by analysing relevant trends in the cybersecurity market to better match demand and supply; support and promote the development and implementation of the Union policy on cybersecurity certification of ICT products and services through preparing candidate European cybersecurity certification schemes for ICT products and services, providing the secretariat to the Union Cybersecurity Certification Group, providing guidelines and good practices concerning security requirements of ICT products and services in cooperation with national certification supervisory authorities and the industry; **Enhanced knowledge, information and awareness raising support –** provide assistance and deliver advice to the Commission and the Member States to reach a high level of knowledge, throughout the Union, on issues related to NIS and its application to the industry stakeholders. This assumes also pooling, organizing and making available to the public, through a dedicated portal, information on security of network and information systems [or cybersecurity]. Another important element are awareness raising activities and outreach campaigns targeted at the general public about cybersecurity risks.

[44] Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

Enhanced research and innovation support - provide advice on research needs and priority-setting in cybersecurity area;

International cooperation support – support Union's efforts to cooperate with third countries and with international organisations to promote international cooperation on cybersecurity.

CERTIFICATION

Certification framework will contribute to achieving the objectives by increasing the overall transparency of cybersecurity assurance[45] of ICT products and services and thereby strengthening trust in the digital single market and in digital innovation. This should also help avoid fragmentation of certification schemes in the EU and related security requirement and evaluation criteria across Member States and sectors;

1.4.3. Expected result(s) and impact

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

A reinforced ENISA (supporting capabilities, prevention, cooperation and awareness at EU level, and therefore designed to increase overall EU cyber resilience), as well as supporting the EU certification framework of ICT products and services is expected to bring the following impacts (non-exhaustive list):

Overall impact:

- Overall positive impact on the internal market thanks to reduced market fragmentation and building trust in digital technologies through better cooperation, more harmonised approaches to EU cybersecurity policies and increased capabilities at EU level. This should result in a positive economic impact by helping to reduce the costs of cybersecurity/cybercrime incidents, for which the estimated economic impact in the Union stands at 0.41% of EU GDP (i.e. around EUR 55 billion).

Specific results:

Improved cybersecurity capabilities and preparedness of Member States and businesses

- Improved cybersecurity capabilities and preparedness of Member States (thanks to long-term strategic analysis of cyber threats and incidents, guidance and reports, brokerage of expertise and good practices, training and training materials availability, reinforced CyberEurope exercises)

- Improved capabilities of private actors thanks to the support to the establishment of Information Sharing and Analysis Centres (ISACs) in various sectors.

- Improved EU and Member States' cybersecurity preparedness thanks to the availability of a well-rehearsed and agreed plans in case of large scale cross-border cybersecurity incident tested in CyberEurope exercises;

Improved cooperation and coordination across Member States and EU institutions, agencies and bodies

- Improved cooperation both within and between public and private sectors;

[45] Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

- Improved consistency of approach to the NIS Directive implementation across borders and sectors

- Improved cooperation in the field of certification thanks to an institutional framework enabling the development of European cybersecurity certification schemes and the development of a common policy in the field.

Increased EU level capabilities to complement the action of Member States

- Improved "EU operational capacity" to complement the action of Member States and support them, upon request and in relation to limited and pre-identified services; These is expected to have a positive impact on the success of incident prevention, detection and response both at Member State and Union level;

Increased awareness of citizens and businesses on cybersecurity issues

- Improved general awareness of citizens and business on cybersecurity issues

- Improved ability to make informed purchase decisions related to ICT products and services thanks to cybersecurity certification

Strengthened trust in the digital single market and in digital innovation through increased transparency of cybersecurity assurance of ICT products and services

- Increased transparency of cybersecurity assurance[46] of ICT products and services thanks to simplification of procedures for security certification through an EU-wide framework

- Improved level of assurance of the security proprieties of ICT products and services

- Increased uptake of security certification incentivised by simplified procedures, reduced costs, and perspective of EU-wide business opportunities not hampered by market fragmentation

- Improved competitiveness within EU cybersecurity market due to reduced costs and administrative burden for SMEs and eliminating potential market-entry barriers caused by numerous national certification systems

Other

- No significant environmental impact is expected for any of the objectives.

- With regard to the EU budget, efficiency gains can be expected by increased cooperation and coordination of the activities between EU institutions, agencies and bodies.

1.4.4. Indicators of results and impact

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

(a)

Objective: Increasing capabilities and preparedness of Member States and businesses:

- Number of trainings organised by ENISA
- Geographical coverage (number of countries and areas) of the direct assistance

[46] Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

provided by ENISA

- Level of preparedness reached by Member States in terms of CSIRT maturity and supervision of cybersecurity related regulatory measures
- Number of EU-wide good practices for critical infrastructures provided by ENISA
- Number of EU-wide good practices for SMEs provided by ENISA
- Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA
- Regular contribution of ENISA to the work of cybersecurity working groups of the European Standardisation Organisations (ESOs).

Objective: Improving cooperation and coordination across Member States and EU, institutions, agencies and bodies:

- Number of Member States having made use of ENISA recommendations and opinions in their policy making process
- Number of EU institutions, agencies and bodies having made use of ENISA recommendations and opinions in their policy making process
- Regular implementation of CSIRTs Network work programme and well-functioning on the CSIRTs Network IT infrastructure and communication channels
- Number of technical reports made available to and used by the Cooperation Group
- Consistent approach to the NIS Directive implementation across borders and sectors
- Number of regulatory compliance assessments performed by ENISA
- Number of ISACS in place in different sectors, in particular for critical infrastructures
- Establishment and regular running of information platform disseminating cybersecurity information deriving from the EU institutions, agencies and bodies
- Regular contribution to the preparation of EU research and innovation work programmes
- Cooperation agreement between ENISA, EC3 and CERT-EU in place
- Number of certification schemes included and developed under the Framework

Objective: Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises:

- Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA
- Publication of aggregated information of incident reported under NIS Directive by ENISA
- Number of pan-European exercises coordinated by the Agency and number of Member States and organisations involved.
- Number of requests to support emergency response by Member States to ENISA and performed by the Agency

- Number of analyses of vulnerabilities, artefacts and incidents performed by ENISA in cooperation with CERT-EU.
- Availability of EU-wide situational reports based on information made available to ENISA by Member States and other entities in case of large scale cross-border cyber incident.

Objective: Increasing awareness of citizens and businesses on cybersecurity issues:

- Regular running of EU-wide and national awareness raising campaigns and regular update of the topics according to the emerging learning needs.
- Increase of cyber awareness among EU citizens
- Regular running of cybersecurity awareness quiz and increase over the time of the percentage of correct responses.
- Regular publication of cybersecurity and cyber hygiene good practices targeted to employees and organisations.

Objective: Strengthening trust in the digital single market and in digital innovation through increasing the overall transparency of cybersecurity assurance[47] of ICT products and services:

- Number of schemes that adhere to the EU framework
- Reduced cost of obtaining a certificate for ICT security.
- Number of conformity assessment bodies specialized in ICT certification, across Member States
- Set-up of the European Cybersecurity Certification Group and regular organisation of meetings
- Guidelines for certification according to the EU framework in place
- Regular publication of analyses of the main trends in the EU cybersecurity market
- Number of certified ICT products and services according to the rules of the European ICT security certification framework
- Increased number of end-users who are aware of security features of ICT products and services

(b)

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

In view of the regulatory requirements and fast evolving cybersecurity threat landscape, ENISA's mandate needs to be reviewed to lay down a renewed set of tasks and functions, with a view to effectively and efficiently supporting Member States, EU institutions and other stakeholders' efforts to ensure a secure cyberspace in the European Union. The suggested scope of the mandate is delineated, strengthening those areas where the agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, in particular the NIS Directive, the review of the EU Cybersecurity Strategy, the EU Cybersecurity Blueprint for cyber crisis

[47] Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

cooperation and ICT security certification. The new proposed mandate seeks to give the Agency stronger and more central role, in particular by also supporting Member States more actively to counter particular threats (operational capacity) and by becoming a centre of expertise supporting Member States and the Commission on cybersecurity certification.

At the same time the proposals establishes a European Cybersecurity Certification Framework for ICT products and services and specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The Framework lays down common provisions and procedures enabling the creation of EU-wide cybersecurity certification schemes for specific ICT products/services or cybersecurity risks. The creation of European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.

1.4.6. Added value of Union involvement

Cybersecurity is a truly global issue, which is cross-border by nature and is becoming increasingly cross-sector due to the interdependencies between networks and information systems. The number, complexity and scale of cybersecurity incidents and their impact on economy and society are growing over time and they are expected to further increase in parallel to technological developments, for example the proliferation of the internet of things. This implies that the need for increased common effort from Member States, EU institutions, private stakeholders to face cybersecurity threats cannot expected to decrease in the future.

Since its establishment in 2004, ENISA has aimed to foster cooperation between Member States and the NIS stakeholders, including supporting public-private cooperation. This support to cooperation included the technical work to provide an EU-wide picture of the threat landscape, the set-up of expert groups and the organisation of pan-European cyber incident and crisis management exercises for public and private sectors exercises (in particular "Cyber Europe"). The NIS Directive entrusted ENISA with additional tasks, including the role of the Secretariat of the CSIRTs Network for operational cooperation between Member States.

The added value of acting at EU level, in particular to enhance cooperation between Member States but also between NIS communities has been recognised by the 2016 Council Conclusions[48] and it also clearly emerges from the 2017 evaluation of ENISA, which shows that Agency's added value lies primarily in its ability to enhance cooperation among these stakeholders. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS.

ENISA's added value in bringing cybersecurity communities and stakeholders together is also valid in the field of certification. The rise of cybercrime and security threats has resulted in the emergence of national initiatives setting high-level cybersecurity and certification requirements for ICT components used in traditional infrastructure. Although important, these initiatives bear the risk of creating fragmentation of the single market and barriers for interoperability. An ICT vendor might need to undergo several certification processes to be able to sell in several Member States.The ineffectiveness/inefficiency of the current certification schemes is unlikely to be solved in the absence of EU intervention. In the absence of action, the market fragmentation is very likely to increase

[48] Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

in the short-medium term (next 5-10 years) with the emergence of new certification schemes. The lack of coordination and interoperability across such schemes is an element which decreases the potential of the digital single market. This proves the added value of establishing a European Cybersecurity Certification Framework for ICT products and services putting the right conditions in place for effectively addressing the problem related to the co-existence of multiple certification procedures in various Member States, reducing certification costs and thus making certification in the EU overall more attractive from a commercial and competitive perspective.

1.4.7. Lessons learned from similar experiences in the past

In accordance with the ENISA legal base, the Commission has carried out an evaluation of the Agency, which included an independent study as well as a public consultation. The evaluation came to a conclusion that ENISA's objectives remain relevant today. In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU, there is a need for technical expertise on the evolution of network and information security issues. Capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions.

The agency has been successfully contributing to increased NIS in Europe by offering capacity building in 28 Member States, enhancing cooperation between Member States and NIS stakeholders; provision of expertise, community building and support to policy.

While ENISA managed to make an impact, at least to some extent, in the vast field of NIS but it has not fully succeeded in developing a strong brand name and gaining sufficient visibility to become recognised as "the" centre of expertise in Europe. The explanation for this lies with the broad mandate of ENISA, which was not met with proportionally big resources. Furthermore, ENISA remains the only EU agency with a fixed-term mandate which limits its ability to develop a long term vision and support its stakeholders in a sustainable manner. This is also in contrast with the provisions of the NIS Directive, which entrust ENISA with tasks with no end date.

As far as cybersecurity certification for ICT products and services is concerned no European Framework exists at the moment. However, the rise of cybercrime and security threats has resulted in the emergence of national initiatives, which create the risk of fragmentation of the single market.

1.4.8. Compatibility and possible synergy with other appropriate instruments

The initiative is highly coherent with the existing policies, in particular in the area of the internal market. Indeed, it is designed according to the overall approach to cybersecurity, as defined by the review of the Digital Single Market Strategy, in order to complement a comprehensive set of measures, such as the review of the EU Cybersecurity Strategy, the blueprint for cyber crisis cooperation and the initiatives to fight cybercrime. It would ensure alignment with and build on the provisions of the existing cybersecurity legislation, in particular the NIS Directive, in order to pursue further the cyber resilience of the EU through enhanced capabilities, cooperation, risk management and cyber awareness.

The suggested certification measures should address the potential fragmentation caused by existing and emerging national certification schemes, therefore contributing to the development of the digital single market. The initiative also supports and complements the

implementation of the NIS Directive by providing the undertakings subject to the Directive with a tool to demonstrate compliance with the NIS requirements in the whole Union.

The European ICT cybersecurity certification framework as proposed, is without prejudice with the General Data Protection Regulation(GDPR)[49] and in particular with the relevant provisions on regarding certification[50] as they apply to the security of the processing of personal data. Last but not least, as much as possible the schemes proposed in the future European framework should rely on international standards as a way to avoid creating trade barriers and ensure coherence with international initiatives.

[49] Regulation (EU) 2016/679 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)

[50] Such as Articles 42 (Certification) and 43 (Certification Bodies) as well as Articles 57, 58, and 70 regarding respectively the relevant tasks and powers of the independent supervisory authorities and the tasks of the European Data Protection Board.

1.5. Duration and financial impact

☐ Proposal/initiative of **limited duration**

– ☐ Proposal/initiative in effect from [DD/MM]YYYY to [DD/MM]YYYY

– ☐ Financial impact from YYYY to YYYY

☒ Proposal/initiative of **unlimited duration**

– Implementation with a start-up period from 2019 to 2020,

– followed by full-scale operation.

1.6. Management mode(s) planned[51]

☒ **Direct management** by the Commission (Title III – Certification)

– ☐ executive agencies

☐ **Shared management** with the Member States

☒ **Indirect management** by entrusting budget implementation tasks to:

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

☐the EIB and the European Investment Fund;

☒ bodies referred to in Articles 208 and 209 (Title II – ENISA)

☐ 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.

Comments

The Regulation Covers:

- Title II of the proposed Regulation reviews the mandate of the European Union Agency for Network and Information Security (ENISA) giving it an important role in certification while

- Title III establishes a framework for the creation of European cybersecurity certification schemes of ICT products and services, in which ENISA plays a crucial role.

[51] Details of management modes and references to the Financial Regulation may be found on the BudgWeb site: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MANAGEMENT MEASURES

2.1. Monitoring and reporting rules

Specify frequency and conditions.

Monitoring will start right after the adoption of the legal instrument and it will focus on its application. The Commission will organise meetings with ENISA, Member States representatives (e.g. group of experts) and the relevant stakeholders in particular to facilitate the implementation of the rules concerning certification such as the establishment of the Board.

The first evaluation should take place 5 years after the entry into force of the legal instrument, provided sufficient data is available. An explicit evaluation and review clause [Art XXX], by which the Commission will conduct an independent evaluation, is included in the legal instrument. 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 Regulation and its added value. Further evaluations should take place every five years. The Commission Better Regulation methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholders consultations.

ENISA's Executive Director should present to the Management Board an ex-post evaluation of ENISA's activities every two years. The Agency should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Management Board should be responsible to vigilante on the adequate follow-up of such conclusions.

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

The data sources for planned monitoring would mostly be ENISA, the European Cyber-Certification Group, the Cooperation Group, the CSIRTs Network and the Member States' authorities. Besides the data deriving by the reports (including the annual activity reports) of ENISA, the European Cyber-Certification Group, the Cooperation Group and the CSIRTs Network, specific data gathering tools will be used when needed (for example surveys to national authorities, Eurobarometer and reports from Cybersecurity Month campaign and the pan-European exercises).

2.2. Management and control system

2.2.1. Risk(s) identified

The risks identified are limited: a Union agency exists already and its mandate will be delineated, strengthening those areas where the Agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, in particular the NIS Directive, the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification.

The proposal therefore details Agency's functions and leads to efficiency gains. The increase of operational competences and tasks does not represent a real risk as they would be complementing the action of Member States and supporting them, upon request and in relation to limited and pre-identified services.

Furthermore the proposed model of the agency, as per the Common Approach, ensures that there is a sufficient control in place to make sure that ENISA works towards its objectives. The operational and financial risks of the proposed changes seem to be limited.

At the same time, it is necessary to ensure adequate financial resources in order for ENISA to fulfil the tasks entrusted by the new mandate, including in the field of certification.

2.2.2. Control method(s) envisaged

The agency's accounts will be submitted for approval of the Court of Auditors and subject to the discharge procedure and audits are envisaged.

Also the operations of the agency are subject to the supervision of the Ombudsman in accordance with the provisions of Article 228 of the Treaty.

See also point 2.1 and point 2.2.1 above

2.3. Measures to prevent fraud and irregularities

Specify existing or envisaged prevention and protection measures.

The ENISA's prevention and protection measures would apply, specifically:

- Payments for any service or studies requested are checked by the agency's staff prior to payment, taking into account any contractual obligations, economic principles and good financial or management practice. Anti-fraud provisions (supervision, reporting requirements, etc.) will be included in all agreements and contracts concluded between the agency and recipients of any payments.

- In order to combat fraud, corruption and other unlawful activities the provisions of Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-fraud Office (OLAF) shall apply without restriction.

- The agency shall accede, within six months form the day of entry into force of this regulation, to the Inter-institutional Agreement of 25 May 1999 between the European Parliament and the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-fraud Office (OLAF) and shall issue, without delay, the appropriate provisions applicable to all the employees of the agency.

3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

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

- Existing budget lines

In order of multiannual financial framework headings and budget lines.

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
		Diff./Non-diff.[52]	from EFTA countries[53]	from candidate countries[54]	from third countries	within the meaning of Article 21(2)(b) of the Financial Regulation
1a Competitiveness for growth and employment	09.0203 European Union Agency for Network and Information Society and Information and communication Technology security certification	Diff	YES	NO	NO	NO
5 Administrative expenditure]	09.0101 Expenditure related to staff in active employment of Communications networks, content and technology 09.0102 Expenditure related to external staff in active employment of Communications	Non-diff.	NO	NO	NO	NO

[52] Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

[53] EFTA: European Free Trade Association.

[54] Candidate countries and, where applicable, potential candidates from the Western Balkans.

	networks, content and technology 09.010211 Other management expenditure					

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	1a	Competitiveness for growth and employment

ENISA			**Baseline** 2017 (31/12/2016)	**2019** *(from 01.07.2019)*	**2020**	**2021**	**2022**	**TOTAL**
Title 1: Staff Expenditure *(including also expenditure related to staff recruitment, training, socio-medical infrastructure and external services)*	Commitments	(1)	6.387	9.899	12.082	13.349	13.894	**49.224**
	Payments	(2)	6.387	9.899	12.082	13.349	13.894	**49.224**
Title 2: Infrastructure & operating expenditure	Commitments	(1a)	1.770	1.957	2.232	2.461	2.565	**9.215**
	Payments	(2a)	1.770	1.957	2.232	2.461	2.565	**9.215**
Title 3: Operational Expenditure	Commitments	(3a)	3.086	4.694	6.332	6.438	6.564	**24.028**
	Payments	(3b)	3.086	4.694	6.332	6.438	6.564	**24.028**
TOTAL appropriations for ENISA	Commitments	=1+1 a +3a	**11.244**	16.550	20.646	22.248	23.023	**82.467**
	Payments	=2+2 a +3b	**11.244**	**16.550**	**20.646**	**22.248**	**23.023**	**82.467**

Heading of multiannual financial framework	**5**	‘Administrative expenditure’

EUR million (to three decimal places)

		2019 *(from 01.07.2019)*	**2020**	**2021**	**2022**	**TOTAL**
DG: CNECT						
• Human Resources		0.216	0.846	0.846	0.846	**2.754**
• Other administrative expenditure		0.102	0.235	0.238	0.242	**0.817**
TOTAL DG CNECT	Appropriations	0.318	1.081	1.084	1.088	**3.571**

The staff costs were calculated according to the planned recruitment date (employment is envisaged starting from 01.07.2019).

The resources outlook beyond 2020 is indicative and without prejudice to the Commission proposals for the post-2020 multiannual financial framework

TOTAL appropriations under HEADING 5 of the multiannual financial framework	(Total commitments = Total payments)	0.318	1.081	1.084	1.088	**3.571**

EUR million (to three decimal places)

	2019	**2020**	**2021**	**2022**	**TOTAL**

TOTAL appropriations under HEADINGS 1 to 5 of the multiannual financial framework	Commitments	16.868	21.727	23.332	24.11	**86.038**
	Payments	16.868	21.727	23.332	24.11	**86.038**

3.2.2. Estimated impact on Agency's appropriations

– ☐ The proposal/initiative does not require the use of operational appropriations

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

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAL**
Increasing capabilities and preparedness of Member States and businesses	1.408	1.900	1.931	1.969	7.208
Improving cooperation and coordination across Member States and EU institutions, agencies and bodies.	0.939	1.266	1.288	1.313	4.806
Increasing EU level capabilities to complement the action of Member States, in particular in the case of cross-border cyber crises.	0.704	0.950	0.965	0.985	3.604
Increasing awareness of citizens and businesses on cybersecurity issues.	0.704	0.950	0.965	0.985	3.604
Strengthening trust in the digital single market and in digital innovation through increasing the overall transparency of cybersecurity assurance of ICT products and services.	0.939	1.266	1.288	1.313	4.806
TOTAL COST	4,694	6.332	6.437	6.565	24.028

[55] This table outlines only operational expenditure as per Title 3.

3.2.3. Estimated impact on Agency's human resources

3.2.3.1. Summary

– ☐ 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)

	Q3/4 2019	**2020**	**2021**	**2022**
Temporary Officials (AD Grades)	4.242	5.695	6.381	6.709
Temporary Officials (AST grades)	1.601	1.998	2.217	2.217
Contract Agents	2.041	2.041	2.041	2.041
Seconded National Experts	0.306	0.447	0.656	0.796
TOTAL	**8.190**	**10.181**	**11.295**	**11.763**

The staff costs were calculated according to the planned recruitment date (for current ENISA staff full employment was assumed as from 01.01.2019). For the new staff progressive employment was envisaged starting from 01.07.2019 and achieving full employment in 2022. The resources outlook beyond 2020 is indicative and without prejudice to the Commission proposals for the post-2020 multiannual financial framework.

Estimated impact on the staff (additional FTE) – establishment plan

Function group and grade	2017 **Current ENISA**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
AD Total	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST Total	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
AST/SC Total					
GRAND TOTAL	48	12	10	7	3

The tasks for additional AD/AST staff to achieve the objectives of the instrument as described in section 1.4.2:

Tasks	AD	AST	SNE	Total
Policy and capacity building	8	1		9
Operational cooperation	8	1	7	16
Certification (market related tasks)	9	3	2	14
Knowledge, information and awareness	1	1		2
TOTAL	26	6	9	41

Description of tasks to be carried out:

Tasks	**Additional resources required**
EU policy development and implementation & Capacity building	Tasks would include assisting the Cooperation Group, supporting consistent NIS implementation across borders, regular reporting on the state of implementation of the EU legal framework; advising and coordinating sectorial cybersecurity initiatives including in energy, transport (e.g. aviation/ road/ maritime/ connected vehicles), health, finance, providing support to the establishment of Information Sharing and Analysis Centres (ISACs) in various sectors.

Operational cooperation and crisis management	**The tasks would include:** Providing Secretariat to the CSIRT Network by ensuring, among others, the well-functioning of the CSIRTs Network IT infrastructure and communication channels. Ensure structured cooperation with CERT-EU, EC3 and other relevant EU bodies. Organising **Cyber Europe Exercises**[56] -tasks related to scaling up the exercise from a bi-annual to annual event and making sure the exercises look at incident from beginning to end. **Technical assistance -** tasks would include structured cooperation with CERT-EU to provide technical assistance in case of significant incidents and to support incident analysis. This would include providing to Member States assistance to handle incidents and analyse of vulnerabilities, artefacts and incidents. Facilitate cooperation between individual Member States in dealing with emergency response by analysing and aggregating national situational reports based on information made available to the Agency by Member States and other entities. **Blueprint for coordinated response to large-scale cross-border cyber incidents - t**he Agency will contribute to develop a cooperative response, at Union and Member States level, to large-scale cross-border incidents or crises related to the cybersecurity through a series of tasks from contributing to establish a situational awareness at Union level to testing the cooperation plans for incidents. **Ex post technical enquiries on incidents** - conduct or contribute to ex-post technical enquiries on incidents in cooperation with the CSIRTs Network with a view issuing recommendations and reinforcing capabilities in form of public reports to better prevent future incidents.
Market related tasks	The tasks would include actively supporting the

[56] Cyber Europe is the largest and most comprehensive EU cyber-security exercise to date involving more than 700 cyber-security professionals from all 28 Member States. It is held every second year. The evaluation of ENISA and the 2013 EU Cybersecurity Strategy point to the fact that many stakeholders advocate scaling up Cyber Europe to an annual event given the fast evolving nature of cyber threats. This is, however, not feasible at the moment in view of the limited resources of the Agency.

(standardisation, certification)	work undertaken within the Certification Framework, including providing technical expertise to prepare candidate European cybersecurity certification schemes. The tasks will also include support to Union policy development and implementation on standardisation, certification and Market Observatory- this will require facilitating the take-up of risk-management standards of electronic products, networks and services and advise operators of essential services and digital service providers on technical security requirements. The tasks will also include providing analysis of the main trends in the cybersecurity market.
Knowledge and information, awareness raising:	With a view of ensuring easier access to better structured information on cybersecurity risks and potential remedies, the proposal confers to the Agency a new task of developing and maintaining the "information hub" of the Union. The tasks would include pooling, organising and making available to the public, through a dedicated portal, information on security of network and information systems, in particular cybersecurity, provided by the EU institutions, agencies and bodies. The tasks would also include supporting ENISA's activities in the field of awareness raising to allow the Agency to scale up the effort.

3.2.3.2. Estimated requirements of human resources for the parent DG

– ☐ 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 amounts (or at most to one decimal place)

		Additional Staff			
	Baseline 2017	Q3/4 2019	2020	2021	2020
• **Establishment plan posts (officials and temporary staff)**					
09 01 01 01 (Headquarters and Commission's Representation Offices)	1	2	3		
• **External staff (in Full Time Equivalent unit: FTE)**[57]					
09 01 02 01 (AC, END, INT from the 'global envelope')	1	2			
TOTAL		**4**	**3**		

Description of tasks to be carried out:

Officials and temporary staff	Represent the Commission in the Management Board of the agency. Draw up Commission opinion on the ENISA single programming document and monitor its implementation. Supervise the preparation of the agency's budget and monitor its implementation. Assist the agency in developping its actitvities in line with the Union policies including by participating in relevant meetings. Supervise the implementation of the framework for European cybersecurity certification schemes of ICT products and services. Maintain contacts with Member States and other relevant stakeholders in relation to certification efforts. Cooperate with ENISA regarding candidate schemes. Preapre candidate European cybersecurity schemes.
External staff	As above

[57] AC = Contract Staff; AL = Local Staff; END = Seconded National Expert; INT = agency staff; JED = Junior Experts in Delegations.

3.2.4. Compatibility with the current multiannual financial framework

– ☐ The proposal/initiative is compatible the current multiannual financial framework.

– ☒ The proposal/initiative will entail reprogramming of the relevant heading in the multiannual financial framework.

The proposal will entail reprogramming of article 09 02 03 due to the revision of the ENISA's mandate, which confers the agency with new tasks related, among others, to the NIS Directive implementation and the European Cybersecurity Certification Framework. The corresponding amounts:

Year	Envisaged	Request
2019	10.739	16.550
2020	10.954	20.646
2021	N/A	22.248*
2022	N/A	23.023*

* This is an estimate. EU funding after 2020 will be examined in the context of a Commission-wide debate on all proposals for the post-2020 period. This means that once the Commission has made its proposal for the next multi-annual financial framework, the Commission will present an amended legislative financial statement taking into account the conclusions of the impact assessment[58].

– ☐ The proposal/initiative requires application of the flexibility instrument or revision of the multiannual financial framework[59].

3.2.5. Third-party contributions

– ☐ The proposal/initiative does not provide for co-financing by third parties.

– ☒ The proposal/initiative provides for the co-financing estimated below:

	Year **2019**	Year **2020**	Year **2021**	Year **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

58 Link to the page with impact assessment

59 See Articles 11 and 17 of Council Regulation (EU, Euratom) No 1311/2013 laying down the multiannual financial framework for the years 2014-2020.

60 The exact amount for the subsequent years will be known when the EFTA's proportionality factor will be fixed for the year concerned.

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 miscellaneous

EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

ANNEX 1

ANNEX

to the

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'')

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES

Conformity assessment bodies that wish to be accredited shall meet the following requirements:

1. A conformity assessment body shall be established under national law and have legal personality.

2. A conformity assessment body shall be a third-party body independent of the organisation or the ICT products or services it assesses.

3. A body belonging to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products or services which it assesses, may, on condition that its independence and the absence of any conflict of interest are demonstrated, be considered a conformity assessment body.

4. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall neither be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT product or service which is assessed, nor shall it be the authorised representative of any of those parties. This shall not preclude the use of assessed products that are necessary for the operations of the conformity assessment body or the use of such products for personal purposes.

5. A conformity assessment body, its top-level management and the personnel responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the marketing, installation, use or maintenance of those ICT products or services, or represent the parties engaged in those activities. They shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall apply, in particular, to consultancy services.

6. Conformity assessment bodies shall ensure that the activities of their subsidiaries or subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities.

7. Conformity assessment bodies and their personnel shall carry out the conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field and shall be free from all pressures and inducements, including of a financial nature, which might influence their judgement or the results of their conformity assessment activities, especially as regards persons or groups of persons with an interest in the results of those activities.

8. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility.

9. At all times and for each conformity assessment procedure and each kind, category or sub-category of ICT products or services, a conformity assessment body shall have at its disposal the necessary:

(a) personnel with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks;

(b) descriptions of procedures in accordance with which conformity assessment is carried out, ensuring the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a notified body and other activities;

(c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the ICT product or service technology in question and the mass or serial nature of the production process.

10. A conformity assessment body shall have the means necessary to perform the technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities.

11. The personnel responsible for carrying out conformity assessment activities shall have the following:

(a) sound technical and vocational training covering all the conformity assessment activities;

(b) satisfactory knowledge of the requirements of the assessments they carry out and adequate authority to carry out those assessments;

(c) appropriate knowledge and understanding of the applicable requirements and testing standards;

(d) the ability to draw up certificates, records and reports demonstrating that assessments have been carried out.

12. The impartiality of the conformity assessment bodies, of their top-level management and of the assessment personnel shall be guaranteed.

13. The remuneration of the top-level management and of the assessment personnel of a conformity assessment body shall not depend on the number of assessments carried out or on the results of those assessments.

14. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the State in accordance with national law, or the Member State itself is directly responsible for the conformity assessment.

15. The personnel of a conformity assessment body shall observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation or pursuant

to any provision of national law giving effect to it, except in relation to the competent authorities of the Member States in which its activities are carried out.

16. Conformity assessment bodies shall meet the requirements of standard EN ISO/IEC 17065:2012.

17. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of standard EN ISO/IEC 17025:2005.