Contribution ID: 166bff56-92c4-4f04-8246-b8224b2cb3bf
Date: 19/06/2025 20:28:44

The review of the Cybersecurity Act

Fields marked with * are mandatory.

Introduction

The 2025 Commission work programme has a strong focus on simplification to boost prosperity and resilience of the Union. This reflects the recommendation of the Draghi report, which underlined that the accumulation of rules, complexity and challenges in implementing the rules are having a significant impact on Europe's competitiveness, limiting our economic potential and our prosperity. In this sense the Commission will propose unprecedented simplification to boost prosperity and resilience, and to unleash opportunities, innovation and growth, launching a new drive to speed up, simplify and improve EU policies and laws, make rules clearer and easier to understand and faster to implement.

The revision of the Cybersecurity Act (Regulation (EU) 2019/881; the 'CSA'), which aims to achieve a high level of cybersecurity, cyber resilience and trust in the European Union, will be a cornerstone in this effort. In 2019, the CSA set a permanent mandate for the European Union Agency for Cybersecurity (ENISA) and established a European Cybersecurity Certification Framework (ECCF) for voluntary European cybersecurity certification schemes for information and communications technology (ICT) products, services and processes. From February 2025, the Cybersecurity Act, amended by Regulation (EU) 2025/37, offers a possibility to request development of a certification scheme for managed security services under the ECCF as well.

In addition to reviewing the current aspects of the CSA, the revision of the Cybersecurity Act will be the driver for simplification of cybersecurity legislation. This includes measures to ensure more straightforward and more agile means to facilitate multiple-purpose reporting to avoid duplications. It will also address other ways to simplify cybersecurity rules. In that way, it will contribute to the broader simplification agenda of the Commission.

The review will also focus on the revision of ENISA's mandate, taking into account that since 2019, ENISA has been allocated additional tasks, by new cybersecurity legislation such as the NIS2 Directive, the Cyber Resilience Act, the Cyber Solidarity Act (CSoA), the eIDAS Regulation (as amended), the Cybersecurity Regulation for EUIBAs or the Digital Operational Resilience Act (DORA), or for example by the European Action Plan on the cybersecurity of hospitals and healthcare providers. Similarly, the ECCF was tested in practice, as three

candidate schemes under the ECCF are presently in progress and the revision will look at an improved functioning of the ECCF. Considering lessons learnt from the functioning of ENISA and of the ECCF, the political commitment to simplification of EU legislation and current challenges in terms of cybersecurity that Member States, companies and organisations may face, this initiative aims to gather stakeholders' views on the following topics:

- **Section 1:** Mandate of ENISA.
- **Section 2:** European Cybersecurity Certification Framework.
- **Section 3:** Simplification of cybersecurity and incident reporting obligations.

This consultation is open to everybody: Member State competent authorities and regulators, cybersecurity organisations, EU bodies dealing with cybersecurity, trade associations and industry representatives, managed security service providers, researchers and academia, cybersecurity professionals, consumer organisations as well as non-governmental organisations and citizens.

You can upload a file with a more detailed contribution at the end of the questionnaire.

The consultation will remain open until 20th June 2025.

About you

* Language of my contribution

- ○ Bulgarian
- ○ Croatian
- ○ Czech
- ○ Danish
- ○ Dutch
- ◉ English
- ○ Estonian
- ○ Finnish
- ○ French
- ○ German
- ○ Greek
- ○ Hungarian
- ○ Irish
- ○ Italian

- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as
  - Academic/research institution
  - Business association
  - Company/business
  - Consumer organisation
  - EU citizen
  - Environmental organisation
  - Non-EU citizen
  - (●) Non-governmental organisation (NGO)
  - Public authority
  - Trade union
  - Other

* First name

Elizabeth

* Surname

Vish

* Email (this won't be published)

elizabeth@securityandtechnology.org

* Organisation name

255 character(s) maximum

Institute for Security and Technology

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

Check if your organisation is on the EU Transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

* Country of origin

Please add your country of origin, or that of your organisation.

This list does not represent the official position of the European institutions with regard to the legal status or policy of the entities mentioned. It is a harmonisation of often divergent lists and practices.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone

- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo

- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Cuba
- Curaçao
- Cyprus
- Czechia
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Türkiye
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- **United States**
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia

Democratic Republic of the Congo	Lesotho	Saint Kitts and Nevis	Zimbabwe
Denmark	Liberia	Saint Lucia	

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **Fo r the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* **Contribution publication privacy settings**

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- **Anonymous**
  Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.
- **Public**
  Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☑ I agree with the personal data protection provisions

Section 1: General questions on ENISA mandate

This section aims to introduce some general questions concerning the mandate of the European Union Agency for Cybersecurity (ENISA). The questions intend to gather information for the potential changes of the mandate and prioritization of tasks of ENISA, based on the related added value for stakeholders. The questions do not aim to assess ENISA's performance, which was subject to a previous evaluation exercise.

Current tasks of ENISA

Q1. Please provide your views regarding the importance of each of the current cybersecurity tasks entrusted to ENISA:

ENISA's task	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
* **Development and implementation of Union policy and law** (e.g., assisting Member States to implement Union policy and law, assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies, etc.)	○	○	○	○	◉
* **Building cybersecurity capacity** (e.g., assisting in activities aiming at bolstering cybersecurity across the EU, etc.)	○	○	○	○	◉
* **Operational cooperation at Union level** (e.g., ENISA support for operational cooperation among Member States, EUIBAs and stakeholders, providing the secretariat of CSIRTs, assisting at the request of one or more Member States, in the assessment of incidents, etc.)	○	○	○	○	◉
* **Market, cybersecurity certification, and standardisation** (e.g., support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes – monitoring developments, preparing candidate schemes, evaluating adopted schemes, standardisation and performing analyses of the main trends in the cybersecurity market, etc.)	○	○	○	○	◉
* **Knowledge and information** (e.g., perform analyses of emerging technologies, perform long-term strategic analyses of cyber threats and incidents, collect and analyse publicly available information about incidents, etc.)	○	○	○	○	◉

* **Awareness-raising and education** (e.g., raise public awareness of cybersecurity risks, organise regular outreach campaigns, promote cybersecurity education, etc.)	○	○	○	○	◉
* **Research and innovation** (e.g., contribute to the strategic research and innovation agenda)	○	○	○	○	◉
* **International cooperation** (e.g., contribute to the implementation of the Union's efforts when cooperating with third countries)	◉	○	○	○	○

Section 1.a. ENISA providing support in policy implementation

The following subsection aims to analyse a core task of the Agency, namely the support in cybersecurity policy implementation.

Q1. Where do you see the biggest added value of ENISA in the following suggestions:

ENISA's added value	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
* **Assisting Member States** to implement Union policy and law regarding cybersecurity consistently. Examples include: issuing opinions and guidelines, providing advice and best practices on topics such as the European Cybersecurity Certification Framework, risk management, incident reporting and information sharing, etc.	○	○	○	○	◉
* **Assisting the Commission** with evidence-based information on the development and review of Union policy in the area of cybersecurity.	○	○	○	○	◉
* **Support to industry (entities)** in the form of best practices and technical guidance through reports/studies and analysis.	○	○	○	○	◉

* ENISA's contribution to the Union's efforts to **cooperate with key international partners.**	○	○	○	○	◉

*** Q2. Do you see any other areas than those mentioned in Q1, where ENISA could bring big added value?**

Please, elaborate (with maximum 100 words):

No comment.

Section 1.b. ENISA providing technical support

Following the adoption of legislative acts such as the NIS2 Directive, Cyber Resilience Act, Cyber Solidarity Act, eIDAS Regulation on electronic identity and trust services, ENISA has received more specific technical tasks (establishing platforms, databases, templates, etc.) to support stakeholders in the implementation of EU law. ENISA will also establish a European Cybersecurity Support Centre for hospitals and healthcare providers, as set out in the recent Action Plan on the cybersecurity of hospitals and healthcare providers. This sub-section of the survey aims to gather more information on how the mandate of the Agency could address this set of specific services and their priority for stakeholders.

*** Q1. Do you consider that there should be additional technical tasks (apart from those included in the adopted legislative acts) that should be integrated in ENISA's mandate?**

- ○ Yes
- ○ No
- ◉ Do not know / no opinion

*** Q2. Do you consider that ENISA is performing well in providing technical tasks (e.g. maintenance of platforms, databases and tools)?**

- ○ Yes
- ○ No
- ◉ Do not know / no opinion

Section 1.c. ENISA's collaboration with other bodies

The cybersecurity ecosystem has evolved significantly since the last revision of ENISA's mandate in 2019. New actors are now part of the cyber fora and the relationship of the Agency with other stakeholders has evolved. This sub-section of the questionnaire aims to gather stakeholder views on ENISA's eventual involvement with other bodies.

* **Q1. Do you consider that ENISA's relationship and/or its partnership with other EU agencies, bodies, institutions etc. should be better specified in the founding act (the Cybersecurity Act)?**

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree
- ◉ Do not know / no opinion

Section 1.d. ENISA's support in situational awareness

The following subsection aims to analyse a core task of the Agency, namely the support of ENISA in operational cooperation and gather stakeholders' views on operational cooperation and the situational awareness picture.

* **Q1: Pursuant to the current Article 7 of the Cybersecurity Act, ENISA supports the operational cooperation at Union level by creating synergies with other Union entities, organising cybersecurity exercises, contributing to a cooperative response to large-scale cyber incidents by providing a secretariat role for the CSIRTs Network and, within its framework, supporting Member States in capacity building, information sharing, analysis of vulnerabilities and incidents and, upon request, providing support in relation to ex post technical inquiries regarding significant incidents.**

In which areas defined in Article 7 should ENISA further strengthen its role? Which tasks, roles are no longer relevant? What new tasks, roles are important for ENISA to cover in the new mandate?

Please elaborate (with maximum 500 words):

The most important approach is to maintain focus on the critical functions that are currently outlined for ENISA under Article 7, rather than expanding ENISA's mandate.

ENISA should continue to serve in the secretariat role for the CSIRTs Network and assist member states in capacity building and information sharing. Through collaborative work with Europol and other EU and Member State organizations, IST has identified information sharing - particularly between government authorities and the private sector, as well as between private sector entities - as foundational for building operational collaboration and ultimately combating cybercrime and other cyber threats.

CSIRTs can play a more central role in organizing and disseminating threat information in order to help combat cybercrime and other cyber threats. By focusing on its existing mandates, including its mandate as the Secretariat for the CSIRTs Network, ENISA could facilitate closer, more effective relationships between the CSIRTs Network, law enforcement organizations across the EU, and existing public-private partnerships across the cyber ecosystem.

ENISA also has the opportunity to continue to strengthen public-private partnerships in the operational context, through efforts such as the Collaborative Public-Private program. Closer collaboration between private and public entities can facilitate a more cohesive, response, and proactive approach to addressing cyber threats. One way ENISA could achieve this is through expanding the scope and effectiveness of "Common Exercises" to include critical infrastructure companies. Their inclusion would improve the realism of these exercises and foster stronger collaboration between key sectors.

Legal and regulatory burdens – either real or perceived – also continue to hamper information sharing. In its role fostering collaboration, including through organizing cybersecurity exercises, ENISA can help address concerns about information sharing held by both national and sub-national organizations. IST hears frequently from partners, both industry and government organizations, that cybersecurity exercises are an invaluable resource for building trust across diverse stakeholders. In addition to exercises and table tops, ENISA should also continue to invest in other capacity building efforts for EU Member States. ENISA can clarify existing mechanisms and processes across the EU regulatory landscape and invest in cross-institutional relationships and partnerships.

ENISA holds a unique position to drive EU-wide supply chain cybersecurity by addressing risks that cut across sectors, industries, and jurisdictions. Unlike individual Member States or private entities, ENISA can systematically identify and analyze chokepoints and concentration risks—whether in hardware, critical infrastructure, or widely used software—that threaten the resilience of the entire digital single market. This involves mapping dependencies across critical sectors, assessing the impact of disruptions, and supporting harmonized risk management practices.

ENISA should integrate supply chain scenarios into joint cyber exercises, enabling public and private actors to test and strengthen coordinated responses to complex, cross-border supply chain attacks. Deepening capacity around Threat Intelligence Platforms (TIPs) like MISP is essential for real-time threat visibility and information sharing, empowering both national authorities and industry partners. ENISA can also support collaborative cyber defense efforts, such as those under PESCO, by fostering cross-sectoral and cross-jurisdictional cooperation, sharing best practices, and aligning standards.

* **Q2: Should ENISA's role in supporting the constituency with capacity building be further strengthened (i.e. with specific support for ransomware prevention; sector specific support offered by ENISA; exercises organised by ENISA; challenges organised by ENISA)?**

- (●) Yes
- ( ) No
- ( ) Do not know / no opinion

* **Q3: Do you think ENISA has a role to play in building a shared EU situational awareness picture together with other Union entities by providing relevant technical information?**

- (●) Yes
- ( ) No
- ( ) Do not know / no opinion

Please elaborate (with max 100 words):

As the EU-wide "CERT," ENISA should have a prime role in enabling situational awareness for member state cyber defense agencies. Having a single point of contact for cybersecurity companies, rather than having to build connections with every CERTS in all 26 member states would be more efficient.

Section 1.e. ENISA and skills and awareness

The following subsection aims to analyse a core task of the Agency, namely the assistance of ENISA in awareness-raising and education, focusing more specifically on cyber skills.

Q1. To what extent do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* ENISA **should continue developing the European Cybersecurity Skills Framework** (ECSF)	( )	( )	( )	( )	(●)
* ENISA **should continue to coordinate EU-wide cyber awareness campaigns and challenges** (e.g. European Cybersecurity Month, the European Cybersecurity Challenge...) and to develop guidance and tools addressing cybersecurity education and cybersecurity awareness (e.g. AR-in-a-Box, CyberEducation Platform,	( )	( )	( )	( )	(●)

Cybersecurity Education Maturity Assessment, training material...)					
* ENISA **should continue leading the work on developing an attestation scheme for cybersecurity skills**, allowing ultimately for quality assurance and recognition of certifications in cybersecurity	○	○	○	○	◉

Section 2: Certification

This section is designed to explore key questions related to the European Cybersecurity Certification Framework (ECCF). The ECCF has a major role in strengthening cybersecurity to protect our industries, citizens and critical infrastructure against internal and external threats. Nevertheless, the evaluation of the Cybersecurity Act (CSA) has highlighted areas where improvements are needed, in particular as regards the adoption and governance process, the roles and responsibilities of the Member States, Commission and ENISA and the formalisation of the maintenance phase of the European cybersecurity certification schemes. Consequently, the questions in this section aim to collect insights to inform potential amendments to the ECCF, ensuring greater clarity, efficiency and stakeholder involvement.

Section 2.a. Scope, objectives, elements of schemes and harmonisation principle

Q1. What are the considerations, if any, that would encourage you to apply for a certificate under the European cybersecurity certification scheme?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* Certification as means to improve the security of products or services	○	○	○	○	◉
* Regulatory compliance, including presumption of conformity	○	○	○	○	◉
* International market access based on mutual recognition	○	○	○	○	◉
* Reduction of legal exposure and potential financial liabilities	○	○	○	○	◉
* Market or contractually required compliance	○	○	○	○	◉
* Customer trust and credibility	○	○	○	○	◉
* Reduction of administrative costs	○	○	○	○	◉

Please elaborate your answer and list other considerations that would encourage you to apply for a certificate (with maximum 200 words):

* **Q2. What technologies / services or other related aspects would benefit from European cybersecurity certification in the next 5 to 10 years (e.g. IoT, crypto, PQC, physical security)?**

Please elaborate your answer (with maximum 100 words):

IST recommends that ENISA's efforts under the ECCF focus on effectively implementing the existing certifications in line with existing requirements and authorities.

* **Q3. Do you consider that the scope, objectives and elements of the ECCF as expressed in the current CSA are clearly defined?**

- ○ Strongly agree
- ○ Agree
- ○ Disagree
- ○ Strongly disagree
- ◉ Do not know / no opinion

Please, elaborate your answer (with maximum 100 words):

* **Q4. Are there any elements that the European cybersecurity certification schemes should cover in addition to those currently foreseen in Article 54 of the Cybersecurity Act (i.e. assurance levels covered, evaluation criteria, vulnerability handling, content and format of certificates)?**

Please elaborate your answer (with maximum 100 words):

No comment.

* **Q5. Do you think there are elements of the European cybersecurity certification schemes that could and should be harmonised for all European cybersecurity certification schemes (i.e. vulnerability handling, peer review mechanism, mark and label, scheme maintenance)?**

- ◉ Yes
- ○ No
- ○ Do not know / no opinion

* Please, elaborate your answer:

IST recommends two areas for standardization within all European cybersecurity certification schemes. First, our view is that labeling should be standardized to allow consumers to quickly understand what is being covered by a certification. Second, IST recommends standardizing maintenance of certification, including how long a certification is good for and best practices for end of life management.

* **Q6. Do you think European cybersecurity certification should be made mandatory for certain products / services / processes / managed security services?**

- (●) Yes
- ( ) No
- ( ) Do not know / no opinion

* Please, elaborate your answer (with maximum 100 words):

No, we do not think it should be mandatory. See detailed comments to discuss our views on how to manage compliance. IST's view is that obtaining certification under the ECCF should allow entities to meet mandatory requirements, such as those laid out in the NIS-2 and CRA. At the same time, we recommend maintaining flexibility in how compliance with the requirements mandated in CRA can be achieved. While there may be a role for mandatory certification for certain categories, we encourage a framework that supports multiple compliance pathways in order to enhance interoperability.

* **Q7. Do you see a benefit in European cybersecurity certification that would be tailormade to specific use-cases (products / services for specific industries)?**

- (●) Yes
- ( ) No
- ( ) Do not know / no opinion

* Please, elaborate your answer (with maximum 100 words):

Based on threat actor activity, ENISA should look at certifications related to edge devices (routers, firewalls, etc.). While many of the secure-by-design principles are the same as for other use-cases, having specific guidance for edge devices would materially reduce risk for a broad swath of industries. In particular, more specificity on appropriate patching capabilities and default configurations could reduce the ability for malicious actors to leverage European consumers and businesses as jumping off points for their attacks. While industry and sector-specific regulations and certifications have led to the fragmentation inefficiencies that governments are currently facing, product-specific certification can provide substantial benefits.

* **Q8: Do you see a benefit in incorporating personal data protection requirements in European cybersecurity certification to ensure synergy with data protection certifications under the General Data Protection Regulation (GDPR)?**

- [ ] Yes
- [ ] No
- [x] Do not know / no opinion

Q9. To what extent do other recent EU legislations aimed at increasing the level of security of ICT products, ICT services and ICT processes, such as the Cyber Resilience Act or the NIS2 Directive, impact the ECCF?

On a scale from 1 to 5 with 5 indicating to the very highest extent

5

Please, elaborate your answer (with maximum 100 words):

IST recommends that the implementation of these laws and regulations leverage the best practices articulated in the ECCF. The ECCF should be used as a benchmark to demonstrate effective compliance with the requirements of recent legislations.

Q10. Do you consider it useful to develop voluntary certification of entities that would support compliance with multiple cybersecurity and data security requirements of EU legislation (e.g. NIS2 Directive, DORA)?

On a scale from 1 to 5, with 5 indicating very useful

5

Section 2.b. Process of development and adoption of certification schemes

The following subsection aims to analyse the effectiveness, efficiency and transparency of the preparation and development of European cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services in the Union for improving the functioning of the internal market.

Q1. Do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* The time needed to develop and adopt a European cybersecurity certification scheme is satisfactory.	○	○	○	○	◉

* European cybersecurity certification schemes need to be regularly updated and amended.	○	○	○	○	◉
* The process for the request, development and adoption of European cybersecurity certification schemes would benefit from increased transparency.	○	○	○	○	◉
* The Union Rolling Work Programme is an effective way of ensuring that industry, national authorities and standardisation bodies prepare in advance for the future European cybersecurity certification scheme (s).	○	○	○	○	◉

Section 2.c. Governance of the certification framework

The questions in this subsection seek to gather views on potential changes to ENISA's mandate and prioritisation of its tasks within the ECCF including, but not limited to, preparation, development and maintenance of European cybersecurity certification schemes, thereby contributing to clarification of the roles and responsibilities.

Q1. What role do you consider ENISA should play in the following areas of the ECCF?

Statement	No role	Supporting role	Leading role	Do not know / No opinion
* Preparation / development of candidate schemes	○	○	○	◉
* Maintenance of schemes: drafting of technical specifications	○	○	○	◉
* Maintenance of schemes: organisation of ECCG subgroup meetings	○	○	○	◉
* Guidance for application of schemes	○	○	○	◉
* Promotion of the uptake of schemes	○	○	○	◉
* Peer review mechanism	○	○	○	◉
* Issuance of certificates for European cybersecurity certification schemes	○	○	○	◉
* Testing and evaluation	○	○	○	◉
* Presumption of conformity with EU legislation	○	○	○	◉

You may elaborate your answer(s) in the table (with maximum 100 words):

Section 2.d. Stakeholder involvement

The questions in this subsection aim to collect additional insights to inform potential amendments to the framework to ensure greater and more streamlined stakeholder involvement, particularly in the preparatory, development and maintenance phases of European cybersecurity certification schemes.

*** Q1. Do you represent or have you in the past represented an organisation in the European Cybersecurity Certification Group (ECCG)?**

- ○ Yes
- ◉ No
- ○ Don't know / no opinion

*** Q2. How do you assess the level of effectiveness of the European Cybersecurity Certification Group?**

- ○ Very low effectiveness
- ○ Low effectiveness
- ○ Medium effectiveness
- ○ High effectiveness
- ○ Very high effectiveness
- ◉ Do not know / no opinion

Q3. To what extent do you agree with the following statements regarding the ECCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
* The ECCG and the ECCF would benefit from more organised stakeholder interactions during preparatory stages of cybersecurity certification schemes.	○	○	○	◉	○
* The role and tasks of the ECCG in the Cybersecurity Act are sufficiently clear.	○	○	○	○	◉
* The ECCG has provided sufficient support to the Member States in the implementation of the ECCF.	○	○	○	○	◉
* Member States should play a more active role in the governance of ECCG subgroups.	○	○	○	○	◉

* **Q4: Do you consider that the mandate of the ECCG should encompass additional tasks to those currently foreseen in the Cybersecurity Act?**

The Cybersecurity Act outlines the tasks of the ECCG in Article 62(4), most prominently to advise and assist the Commission in its work to ensure the consistent implementation and application of the Title III of the Act.

- ○ Yes
- ○ No
- ◉ Don't know / no opinion

* **Q5. In your view, to what extent are relevant stakeholders sufficiently involved in the development of European cybersecurity certification schemes?**

- ○ Not at all
- ○ To a little extent
- ○ To some extent
- ○ To a high extent
- ◉ Do not know / no opinion

* **Q6. What other measures could be taken to further facilitate relevant stakeholders' participation?**

Please, elaborate (with maximum 100 words):

No comment.

* **Q7. Is your organisation directly or indirectly (through association) part of the Stakeholder Cybersecurity Certification Group (SCCG)?**

- ○ Yes
- ◉ No
- ○ Don't know / no opinion

Q8. To what extent do you agree with the following statements regarding the SCCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion

* The SCCG has sufficient opportunities to participate in ECCF.	○	○	○	○	◉
* The SCCG actively contributes to the development of European cybersecurity certification schemes.	○	○	○	○	◉
* A single forum and governance mechanism with regular interactions with the ECCG, ENISA and the Commission could provide better opportunity for the group to fulfil its advisory role.	○	○	○	○	◉

Section 2.e. Supply chain security

Supply chain attacks have been identified as one of the seven prime cybersecurity threats by the ENISA Threat Landscape 2024 report and cybersecurity risks associated with ICT supply chains have been justifiably given a lot of attention in recent years. The EU has taken multiple legislative initiatives to address supply chain security. In particular, Title III of the Cybersecurity Act sets out a framework for the development and adoption of the European cybersecurity certification schemes which provide assurance of the cybersecurity level of ICT products, services or processes that are used in the ICT supply chains. The Directive (EU) 2022/2555 provides for an obligation on Member States to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks. Such measures should cover supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. The recently adopted Cyber Resilience Act introduces mandatory cybersecurity requirements for manufacturers and retailers to be met during the entire lifecycle of their products and at every stage of the supply chain.

*** Q1. In your view, during the last five years, how has the level of risk of cybersecurity incidents originating from ICT supply chains of entities operating in critical and highly critical sectors evolved?**

- ○ Risk level has decreased significantly
- ○ Risk level has decreased
- ○ Risk level is the same
- ○ Risk level has increased
- ○ Risk level has increased significantly
- ◉ Don't know / no opinion

*** Q2: In your opinion what were the most common types of threats that led to ICT supply chain related cybersecurity incidents?**

Please, elaborate with maximum 100 words:

The way that ENISA defines supply chain attacks in public documents seems to align with a fairly narrow view of what constitutes a supply chain attack. IST encourages ENISA to think about supply chain attacks with a broader scope, considering a range of different types of malicious activities as qualifying as supply chain attacks.

IST also notes that edge devices often are particularly vulnerable to targeting. This can include exploits based on known exploited vulnerabilities as well as zero day exploits. Efforts to address edge device security could significantly reduce the risk of supply chain related cybersecurity incidents.

*** Q3. In your opinion, which sectors were the most affected by ICT supply chain incidents (please chose maximum 3)?**

between 1 and 3 choices

- [ ] Energy
- [ ] Transport
- [ ] Banking
- [ ] Financial markets infrastructures
- [ ] Health
- [ ] Drinking water
- [ ] Waste water
- [ ] Digital infrastructure
- [ ] ICT service management (managed security services)
- [ ] Public administration
- [ ] Space
- [ ] Postal and courier service
- [ ] Waste management
- [ ] Manufacture, production and distribution of chemicals
- [ ] Production, processing and distribution of food
- [ ] Manufacturing
- [x] Digital providers
- [ ] Research

The Cybersecurity Act aims at achieving a high level of cybersecurity, cyber-resilience and trust within the Union, for which it addresses threats and risks related to network and information systems. Beyond technical factors, cybersecurity risks for ICT supply chains may also relate to non-technical factors such as undue influence by a third country on supplier (through for instance a strong link between the supplier and a government of a given third country, the third country's legislation, the supplier's corporate ownership or the ability for the third country to exercise any form of pressure on supplier). Such non-technical factors could pose unprecedented security challenges related to ICT supply chains that are currently not covered by the scope of the Cybersecurity Act.

* **Q4. Do you consider that there is a need to develop tools to address non-technical risks related to ICT supply chain security?**

- ○ Strongly agree
- ◉ Agree
- ○ Disagree
- ○ Strongly disagree
- ○ Do not know / no opinion

You may elaborate your answer (with maximum 100 words):

There is substantial room for wider EU adoption of best practices piloted by specific EU member states, such as Estonia and Czechia on 5G, particularly in the context of 5G communications technology deployment. These efforts demonstrate that non-technical factors can present cybersecurity-relevant risks, and offer paths whereby clear non-technical cybersecurity risks can be addressed.

Q5. To what extent do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
* The application of organisational policies, processes and practices, including i.e. information sharing and vulnerability disclosure, in the area of cybersecurity risk management sufficiently mitigates all relevant risks related to the ICT supply chain security of entities.	◉	○	○	○	○
* Purely technical measures, such as the use of on-device processing, appropriate cryptography and other, can sufficiently mitigate all relevant risks related to the ICT supply chain security of hardware and software products.	◉	○	○	○	○
* The current European cybersecurity certification framework is an effective tool to facilitate cybersecurity safeguards for the public procurement of ICT products, ICT services and ICT processes.	○	◉	○	○	○

Section 3: Simplification

This section aims to gather stakeholders' views as regards simplification of the cybersecurity legislation in line with the Commission's simplification agenda. It gathers the stakeholders' views as to whether incident reporting requirements and cybersecurity risk-management could potentially benefit from further simplification and streamlining, with the intended benefit of reducing unnecessary administrative burden.

* **Q1. Which of the following EU pieces of legislation are/will be applicable to your entity/authority:**

- [ ] Directive (EU) 2022/2555 (Network and Information Security Directive – **NIS2**)
- [ ] Regulation (EU) 2022/2554 (Digital Operational Resilience Act – **DORA**)
- [ ] Regulation (EU) 2024/2847 (Cyber Resilience Act – **CRA**)
- [ ] Directive (EU) 2022/2557 (Critical Entities Resilience Directive – **CER**)
- [x] Regulation (EU) 2016/679 (General Data Protection Regulation – **GDPR**)
- [ ] Directive 2002/58/EC, as amended by Directive 2009/136/EC (**e-privacy Directive**)
- [ ] Commission Delegated Regulation (EU) 2024/1366 (Network Code on cybersecurity of cross-border electricity flows – **NCCS**)
- [ ] Aviation rules (Regulations (EC) No 300/2008 and (EU) 2018/1139 and the relevant delegated and implementing acts adopted pursuant to those Regulations)
- [ ] Regulation (EU) 2024/1689 (**AI Act**)
- [ ] Other

Q2. Which of the following cybersecurity-related requirements laid down in the EU legislation referred to in Q1 ("relevant EU legislation") create or are likely to create in the near future the biggest regulatory burden?

Please rate from 1 as the lowest burden to 6 as the highest burden

Different NIS2 incident reporting templates' formats, contents and procedures across the different EU Member States:

4

Different incident reporting tools/processes for relevant EU legislation at a national level:

4

Different incident reporting thresholds defining a reportable/significant /severe incident under the NIS2 Directive and across the different relevant EU legislations:

6

Implementation of cybersecurity risk-management measures stemming from relevant EU legislation:

1

Overlap of cybersecurity risk-management measures stemming from relevant EU legislation:

5

Requirements on how to prove implementation of cybersecurity risk-management measures ('compliance') stemming from relevant EU legislation:

6

Please explain and if possible, provide a quantification to the burden (with maximum 100 words):

Research from the Office of the National Cyber Director in the United States makes it clear that "duplicative or contradictory cybersecurity regulations not only pose unnecessary costs on regulated entities, they also drain investment away from improvements in actual cybersecurity." With the substantial increase in relevant regulation, articulating a common and streamlined set of requirements to meet the standards articulated is crucial.

(For more, albeit in a United States context, we offer this articulation by IST's Nick Leiserson https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Leiserson-2024-06-05.pdf)

* **Q3. Do you consider that there are any other cybersecurity-related requirements laid down in relevant EU legislation not mentioned above that could be further streamlined?**

- (●) Yes
- ( ) No
- ( ) I don't know / no opinion

* Please, elaborate (with maximum 100 words):

In addition to the Cyber Solidarity Act, other relevant EU legislation includes the Cybersecurity Act (2019/881), Cybercrime Directive (2013/40/EU), Radio Equipment Directive (2014/53/EU), Data Act (2023/2854), Data Governance Act (2022/868), Digital Services Act (2022/2065), and Digital Markets Act (2022/1925). These acts collectively address certification, criminal law, device security, data governance, and platform obligations, all of which are crucial for the security and resilience of data, technology, and ICT supply chains.

Q4. How effective do you consider the following solutions would be in removing administrative burden?

Please rate from 1 as the least effective to 6 as the most effective

Align reporting templates for NIS2 incident reporting of entities across all Member States:

4

Align reporting timelines for incident reporting across relevant EU legislation:

4

Align reporting requirements as regards content of reporting obligations across relevant EU legislation:

5

Introduce machine-readable standardised data formats for reporting across the EU:

3

Introduce one comprehensive set of rules for incident reporting in EU legislation:

6

Introduce a single reporting platform at national level for the compliance with reporting obligations stemming from relevant EU legislation:

4

Introduce a single reporting platform at EU level for the compliance with reporting obligations from NIS2:

3

Introduce a single reporting platform at EU level for the compliance with reporting obligations from all relevant EU legislation:

3

Introduce technical protocols and tools (such as APIs and machine-readable standards) for the purpose of automated reporting by entities to facilitate the integration of reporting obligations into business processes:

2

Align cybersecurity risk-management requirements stemming from relevant EU legislation:

4

Introduce one comprehensive set of rules for cybersecurity risk-management in EU legislation:

4

Introduce a higher level of harmonisation across specific sectors:

1

Please specify which sector (with maximum 20 words):

Critical infrastructure sectors, especially those dependent on OT and cross-border operations—energy, communications, transportation, water, and manufacturing—are most in need of harmonized cybersecurity regulations.

* **Q5. Would you suggest any other solutions to remove unnecessary administrative burden further to those mentioned above?**

- (•) Yes
- ( ) No
- ( ) Don't know / no opinion

* Please, elaborate (with maximum 100 words):

Most important for reducing administrative burden is ensuring some level of reciprocity or mutual recognition for compliance. Having even identical requirements for risk management steps will not significantly reduce the compliance burden if an entity needs to demonstrate that compliance to many different auditors who require separate artifacts as proof of the efficacy of the cybersecurity program. The U.S. Office of the National Cyber Director has done significant research on this topic, albeit in a United States domestic context: https://www.hsgac.senate.gov/wp-content/uploads/Testimony-Leiserson-2024-06-05.pdf

* **Q6. Would you agree for the Commission to potentially contact you for further discussion on simplification measures regarding cybersecurity legislation?**

- (•) Yes
- ( ) No

* Please, fill in an email address and the name of your representative:

elizabeth@securityandtechnology.org

If you wish, please upload here a file with a more detailed contribution

Only files of the type pdf,doc,docx,odt,txt,rtf are allowed

11dc4aba-d750-4fba-9dfe-929eee2ce07a

/Institute_for_Security_and_Technology_submission_to_the_EU_Cybersecurity_Act_Review_Consultatio

Contact

EC-CNECT-CSA-REVIEW@ec.europa.eu