EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ASSESSMENT OF EU TELECOM SECURITY LEGISLATION

JULY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please email resilience@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu

AUTHORS

Marnix Dekker, Sławomir Bryska, ENISA

ACKNOWLEDGEMENTS

To complete this guideline, ENISA worked closely with a working group of experts from national authorities, the European Competent Authorities for Secure Electronic Communications (ECASEC) Expert Group (formerly known as the Article 13a Expert Group), as well as all other stakeholders mentioned in Section 2 of this report. We are grateful for their valuable input, comments and support in the process of developing this document.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-505-0 **doi**:10.2824/30649 **Catalogue number**: TP-02-21-565-EN-N

EXECUTIVE SUMMARY

European Union telecom security legislation has been changing over the last few years.

- At the end of 2020, Article 40 of the European Electronic Communications Code[1] (EECC) replaced Article 13a of the Directive on the common regulatory framework for electronic communications networks and services[2] (Telecom Framework Directive).

- With its Recommendation on Cybersecurity of 5G networks[3], in 2019, the European Commission commenced an EU-wide collaboration on cybersecurity of 5G networks. This culminated in the NIS Cooperation Group issuing the EU 5G Cybersecurity Risk Mitigation Toolbox in January 2020[4] (EU 5G Toolbox).

- The European Commission has been reviewing the Network and Information Systems Directive[5] (NIS Directive) and, on 16 December 2020, made a proposal for its amendment[6] (NIS2 proposal), which would bring EU telecom security rules under the NIS Directive.

In light of these policy changes, ENISA carried out an assessment of the implementation of EU telecom security policy, to inform policy makers in the Commission and in the Member States, as well as experts from the sector, about challenges, gaps and possible improvements. This paper contains the highlights of this assessment. We summarize our findings here and we refer the reader to the body of the paper for more details.

This assessment of the implementation of EU telecom security legislation focuses on:

1. Implementation at national level, including the relevant national telecom security legislation, the powers and capabilities of the national authorities, and collaboration and information sharing at national level.

2. Implementation at EU level, including the harmonisation across the EU, the collaboration between the different Member States, and ENISA's role.

The assessment was carried out by interviewing and surveying a balanced group of experts from the public and private sectors, including the national authorities responsible for telecom security, the national authorities responsible for the NIS Directive, and experts from the EU telecom sector (see Figures ES1 and ES2).

[1] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, p. 36.

[2] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services, OJ L 108, 24.4.2002, p. 33.

[3] Commission Recommendation (EU) 2019/534 of 26 March 2019 – Cybersecurity of 5G networks, OJ L 88, 29.3.2019, p. 42.

[4] Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, available at https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

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

[6] Proposal for a directive of the European Parliament and of the Council of 16 December 2020 on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, 16.12.2020.

Figure ES1: Participation in the online survey

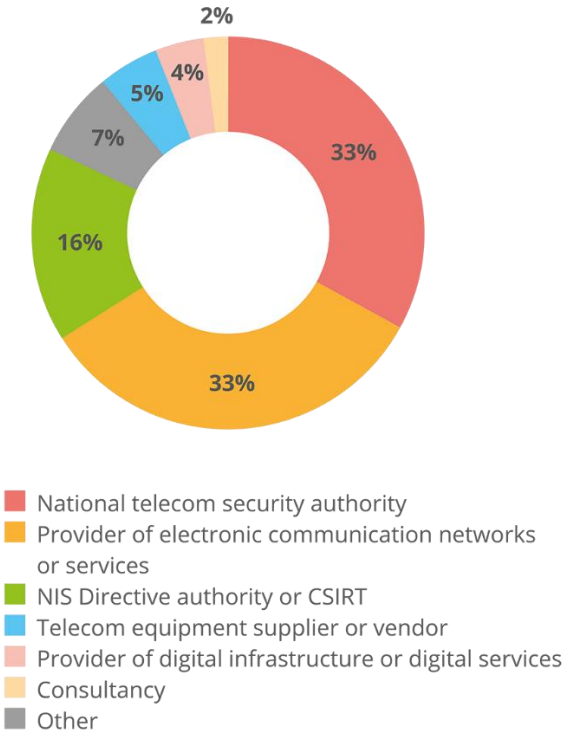
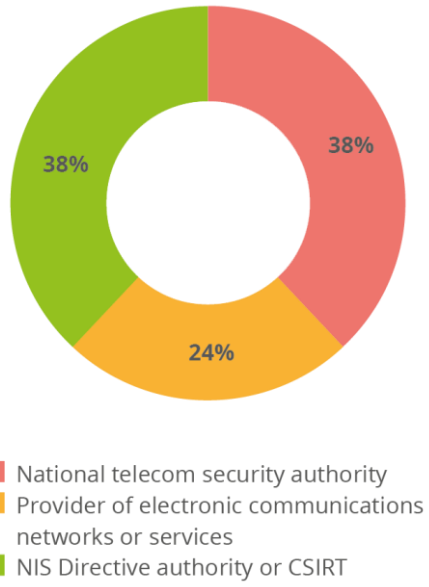


Figure ES2: Participation in the telephone interviews



We highlight the findings from the assessment[7]:

1. **EU telecom security legislation has a positive impact.** The security provisions in the EU regulatory framework have contributed to a high level of cybersecurity in the telecommunications sector.
2. **The legislative framework is complex.** Several experts found national telecom security legislation rather complex.
3. **Authorities have powers but few resources.** The powers of the national telecom security authorities are considered sufficient, but there are concerns about scarcity of resources and expertise.
4. **Incident reporting can be improved.** In general, national-level incident reporting is working well, but there is room for improvement, for example to address the problem of reporting the same incident to multiple authorities, or the lack of feedback after submission of an incident report.
5. **Collaboration at national and EU levels is good.** In general, both national- and EU-level collaboration works well. On the latter, experts recognised the positive contribution of ENISA and the European Competent Authorities for Secure Electronic Communications (ECASEC, formerly Article 13a) Expert Group.

[7] See also Section 6 of this report for full details of the conclusions and recommendations.

The experts who were interviewed and surveyed also provided recommendations for ENISA, Commission, and the national authorities in the EU Member States:

1. **Prioritise the implementation of new policies.** In the short term, the priority is to implement the EECC, the EU 5G Toolbox and the related recommendations.
2. **More resource sharing and collaboration.** To address cybersecurity skills shortages, it is important to explore resource and capability sharing not only between authorities in the same country and between authorities across the EU, but also between authorities and providers, depending on the topic.
3. **More technical guidance for service providers.** While ENISA's role and the work of the ENISA ECASEC Expert Group were valued, experts from the sector asked for more technical and operational guidelines.
4. **Better incident reporting.** To improve incident reporting, it is important that authorities provide feedback in response to incident reports. In addition, definitions of what should be reported and the thresholds for reporting should be clarified.
5. **More trust and engagement between public and private sectors.** Trust between authorities and providers, as well as engagement with the private sector, are important, including in the early stages of policymaking.

As mentioned, at the end of 2020 the Commission put forward its NIS2 proposal. The NIS2 proposal constitutes part of a broader EU cybersecurity strategy[8], which addresses, among other things, the next steps in 5G security policy and updates the existing critical infrastructure protection legislation with a proposal for a directive on the resilience of critical entities[9]. Under the NIS2 proposal, the EU telecom security provisions would be brought under the NIS Directive. We look forward to supporting these policy discussions between the European Commission, the EU Member States and the European Parliament.

[8] European Commission, 'New EU cybersecurity strategy and new rules to make physical and digital critical entities more resilient', press release, 16 December 2020 (https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391).

[9] Proposal for a directive of the European Parliament and of the Council of 16 December 2020 on the resilience of critical entities, COM(2020) 829 final, 16.12.2020.

TABLE OF CONTENTS

1. INTRODUCTION

In 2020, ENISA carried out an assessment of the implementation of EU telecom security policy across the EU. The aim was to provide policymakers with input on a number of recent policy changes and reviews, such as the new EECC (whose Article 40 replaced Article 13a of the Telecom Framework Directive), the review of the NIS Directive and the review of the Commission Recommendation on Cybersecurity of 5G networks.

This assessment was carried out by interviewing and surveying a large and balanced group of experts working in the EU telecom sector, experts working at telecommunications national regulatory authorities (NRAs) and experts working at national authorities for the NIS Directive.

The body of this report contains the main results of this assessment.

1.1. SCOPE

The scope of this assessment includes the security provisions of the EU legislative framework for electronic communications (namely, Article 13a of the Telecom Framework Directive), the new security provisions (Article 40) under the EECC, other relevant EU policies related to telecom security, and national policies and legislation incorporating EU legislation adopted in the EU Member States.

1.2. TARGET AUDIENCE

The target audience of this report are policymakers at EU and national levels and telecom security and policy/legislation experts.

1.3. METHODOLOGY

An online survey was used to gather expert input. The survey was completed by a mixed group of 45 experts from across the EU, including experts working in the telecom sector and experts working at the national authorities. In addition, 21 telephone interviews were conducted with the experts to explore the key issues in more detail. Figures 1 and 2 show how each group was represented in the survey and interviews, respectively.

Figure 1: Participation in the online survey

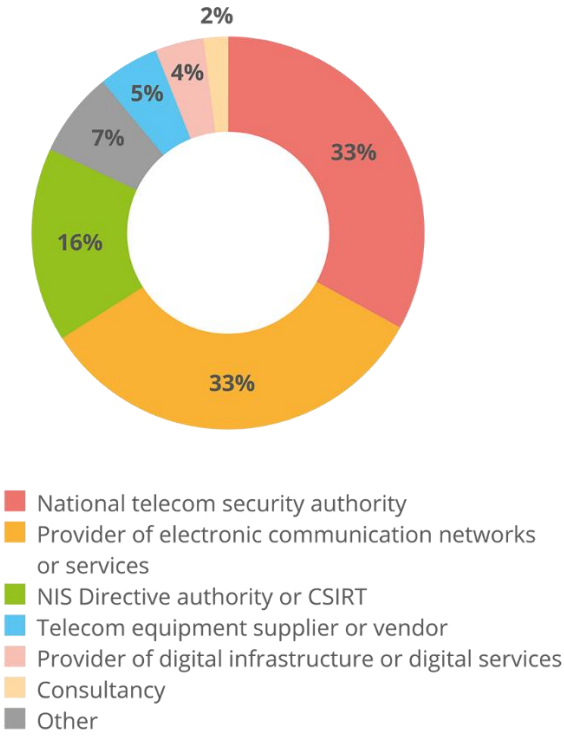
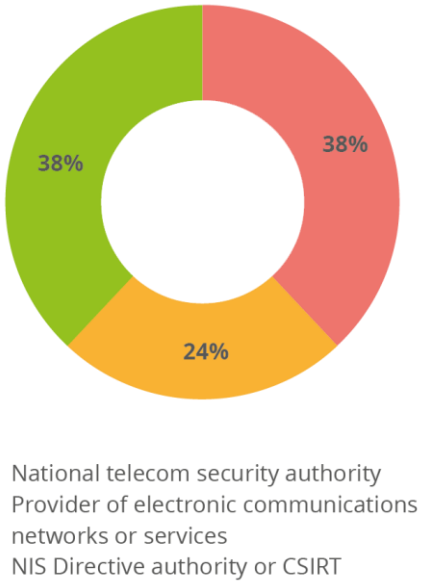


Figure 2: Participation in the telephone interviews



1.4. ACKNOWLEDGEMENTS

We are very grateful to all the experts who took the time to complete the online survey. We would also like to acknowledge the experts who participated in the telephone interviews.

Interviewee	Affiliation
Ahmet Yesilyurt	Federal Network Agency (Bundesnetzagentur), Germany; co-chair of the European Competent Authorities for Secure Electronic Communications (ECASEC) Expert Group (formerly Article 13a Expert Group)
Antoine Berthier	National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information (ANSSI)), France
Costas Efthymiou	Digital Security Authority (Αρχή Ψηφιακής Ασφάλειας), Cyprus
Davide Nardacci **Alessandro Paci**	Ministry of Economic Development, Directorate-General for Communications Technologies and Information Security – Higher Institute of Communications and Information Technologies (Ministero dello Sviluppo Economico, Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica – Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (DGTCSI-ISCTI)), Italy
Costin Masiliev **Előd Hainal-Filla**	National Authority for Administration and Regulation in Communications (Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM)), Romania
George Drivas **N. Chouliaras** **Sotiris Vasilos**	National Cyber Security Authority, Hellenic Ministry of Digital Governance (Εθνική Αρχή Κυβερνοασφάλειας, Υπουργείο Ψηφιακής Διακυβέρνησης) Greece
Heidi Kivekas **Tatu Giordani**	Finnish Transport and Communications Agency (Traficom – Liikenne- ja viestintävirasto)

Interviewee	Affiliation
Ilmar Toom	State Information System Board (Riigi Infosüsteemi Amet (RIA)), Estonia
Jens Marschall **Iain Boyd Richmond** **Rainer Koch**	Deutsche Telekom, Germany
Joseph Stephens	National Cyber Security Centre (NCSC), Department of the Environment, Climate and Communications, Ireland
Lukas Pimper	National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)), Czechia
Manuel Barros	National Communications Authority (Autoridade Nacional de Comunicações (ANACOM)), Portugal
Per Ekare	Swedish Post and Telecom Authority (Post- och telestyrelsen (PTS))
Regis Rousselot **Vincent Maurin** **Franck Laurent** **Francois Zamora** **Luisa Rossi**	Orange
Remi Van de Calseijde **Martin Pickford** **Robert Kolthek**	Liberty Global
Rodrigo Pereira **Jorge Frazao** **Manuela Figueiredo**	NOS, SGPS S.A., Portugal
Stephen Hermanson	Vodafone Group
Tamás Róka	National Media and Communications Authority (Nemzeti Média- és Hírközlési Hatóság (NMHH)), Hungary
Thomas Due Jørgensen	Centre for Cyber Security (Center for Cybersikkerhed (CFCS)), Denmark
Tim Masy	Belgian Institute for Postal Services and Telecommunications (BIPT)
Warna Münzebrock	Radiocommunications Agency Netherlands (Agentschap Telecom (AT)); chair of the ECASEC Expert Group (formerly Article 13a Expert Group)

2. FINDINGS

This section presents the findings of the assessment. They are discussed at two levels:

1. **National level.** Implementation of telecommunications security legislation at national level, including its impact, powers and capabilities of NRAs, incident reporting and national-level collaboration.

2. **EU level.** Operation of telecommunications security legislation at EU level, including harmonisation, EU-level collaboration and work of the Article 13a (now ECASEC) Expert Group and ENISA.

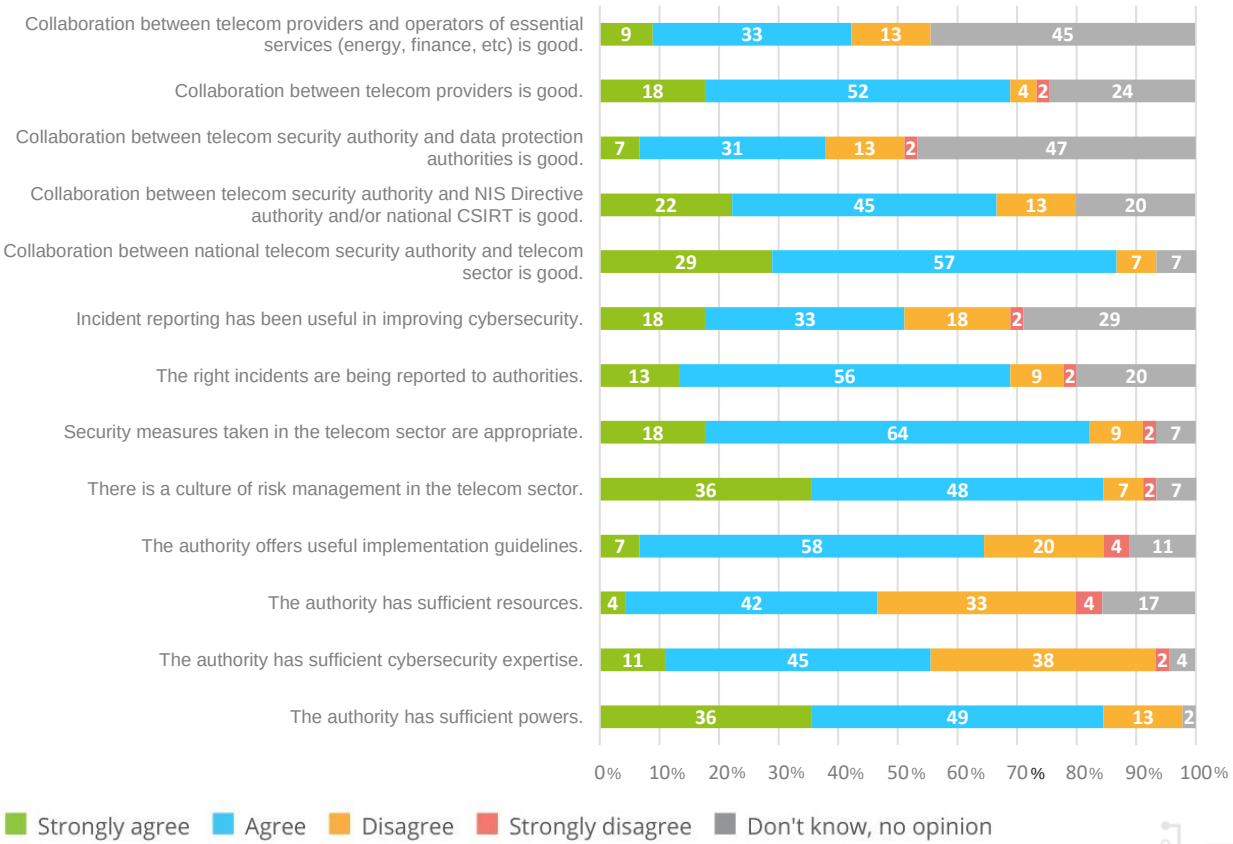
2.1. ASSESSMENT OF TELECOM LEGISLATION AT NATIONAL LEVEL

2.1.1. Summary

Overall, collaboration at national level is considered to be strong, especially between national telecom security authorities and the telecom sector, and between national telecom security authorities and NIS Directive national authorities and/or national cybersecurity incident response teams (CSIRTs). In addition, experts agree that security measures and risk management are good in the telecom sector.

On the other hand, there are mixed opinions on the sufficiency of national authorities' resources. Moreover, there are concerns about collaboration at national level between telecom security authorities and data protection authorities, and between telecom operators and operators of essential services.

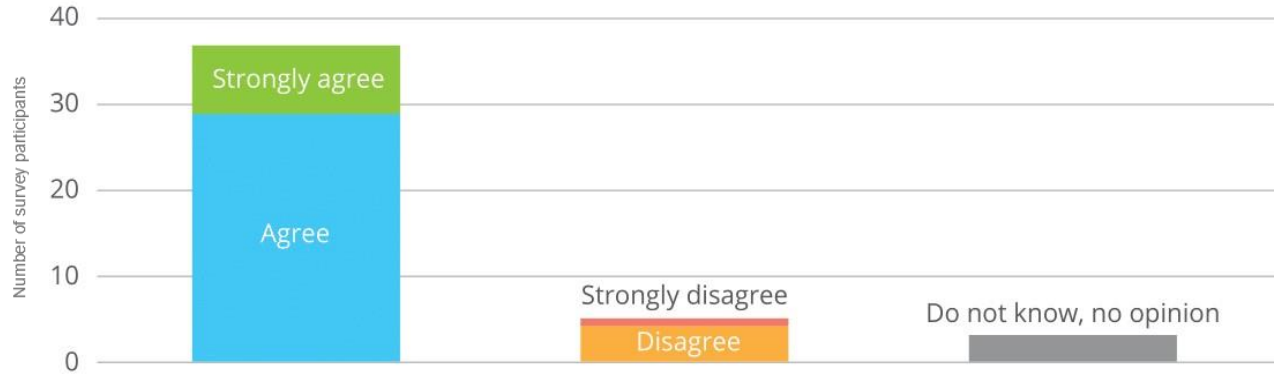
Figure 3: National level – capabilities and collaboration



2.1.2. Positive impact of the legislation

EU telecom security legislation has achieved a culture of risk management	
EU legislation has increased the level of maturity in telecoms security in many countries	There is a culture of risk management across EU Member States and the security measures taken are considered appropriate. The survey results underpin this opinion as 84% of participants agreed that there is a culture of risk management in the telecommunications sector.
Security measures are generally appropriate	Only about 9% of the respondents disagreed with this statement. More than half of the respondents who disagreed with the appropriateness of security measures were CSIRT representatives.

Figure 4: Security measures taken in the telecom sector are appropriate



However, legislation is complex and guidance is missing	
National legislation is complex	Experts found legislation definitions, obligations and terms rather incoherent or unclear. They noted that permissive definitions or a lack thereof under the old EU regulatory framework allowed different interpretations at national level, which could hinder the operation of providers that are present in more than one Member State. The most commonly invoked example was that of an 'incident'[10]. One of the interviewees commented that incidents 'are seen and interpreted differently by many companies'. Closely related to this was the uncertainty around the reporting thresholds and the treatment of digital service providers, domain name systems and Internet exchange points (IXPs). One of the experts noted that the last two services could potentially be within the scope of both the EECC and the NIS Directive.

[10] 'Incidents' were not defined in the Telecom Framework Directive, which may have contributed to the problem. The EECC introduces the definition of a 'security incident' in Article 2(42): "security incident" means an event having an actual adverse effect on the security of electronic communications networks or services'.

In some countries, this is compensated by guidelines	However, in some cases, no additional materials are provided to service providers. In addition, based on the findings of the survey, one quarter of the respondents thought that the guidelines provided by NRAs are not useful enough as they are considered too high level and lack operational and technical details.
Overlapping obligations and requirements have been reported	In some countries, service providers are supervised by and are forced to collaborate with more than one authority regarding network security, for instance the NRA and a cybersecurity agency.
It is not always clear which specific authority a certain service provider falls under	For example, in some cases, telecommunications operators are also IXPs, which raises the question of whether their IXP operations fall within the remit of the NRA (EECC) or the competent authority under the NIS Directive.

2.1.3. Capabilities and powers of national authorities

85% of the survey respondents agreed that the NRA has sufficient power	In addition, some respondents highlighted the continuous adaptation of the NRA's capabilities to technical changes.
However, many stakeholders were concerned about the scarcity of resources and expertise	37% of the survey respondents indicated that authorities' lack of resources is an issue and 40% found that NRAs have insufficient expertise.
Resource sharing and collaboration between authorities helps	For example, NRAs can receive support from national CSIRTs or other security services, such as crisis centres and intelligence services.

2.1.4. Incident reporting and audits

Generally, national-level incident reporting is working well. It has also been useful in improving cybersecurity	69% of the online survey respondents agreed or strongly agreed that the right incidents are reported to authorities. Only a small percentage of respondents disagreed with this statement and 20% of respondents had no opinion on the topic.
However, some incidents are not being reported or are missing essential details	Three main reasons were identified by the respondents: • diverse interpretation of incidents within the scope, • reporting rules focus on the duration of service interruption and, as a result, certain incidents may not be reported (e.g. data leaks), and • lack of trust between the authorities and telecom providers.
Incident-reporting obligations and processes may be fragmented	Some respondents highlighted that there may be reporting obligations to multiple authorities, or the root cause of an incident may not be easy to define, which results in the same incident being reported to more than one authority. A noteworthy example of good practice is the universal reporting tool developed by the Danish Centre for Cyber Security (CFCS), which sends the report to the relevant authority.

It is uncommon to receive feedback on reported incidents	As a result, the interviewees sometimes viewed the incident-reporting obligations as an 'administrative burden'. The interviewees noted that receiving feedback would significantly increase the utility of reporting.

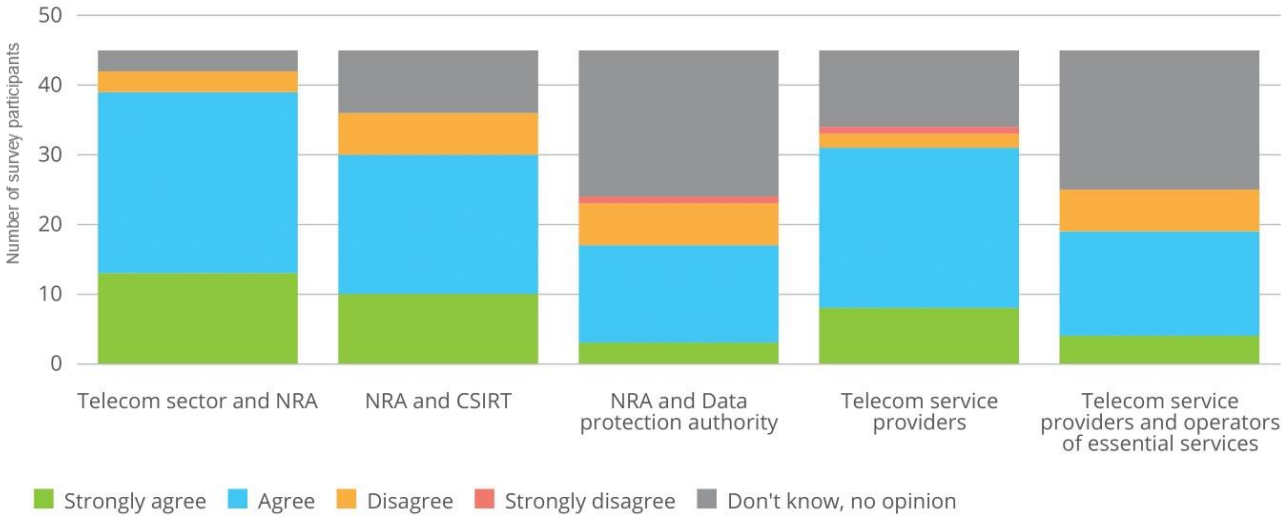
Concern: frequency of audits varies considerably

Some countries carry out 10–15 audits per year, while others conduct more than 250. In general, the view is that authorities have enough power to conduct or order audits, monitor procedures, perform supervision and collect the necessary information.

2.1.5. Collaboration at national level

National-level collaboration is working well. Figure 5 presents the general findings on collaboration between stakeholders. This is followed by presentation of some of the highlights of the online survey and the interviews.

Figure 5: Collaboration between the following stakeholders is good



Collaboration between authorities at national level is improving	
In most Member States, competent authorities recognised the increasing importance of joint work	Collaboration between different telecommunications-related authorities is mostly considered to be good. There is also the intention to combine the capabilities and expertise of the different authorities, and confidence that this can be achieved.
Some challenges have been identified	Challenges exist as a result of the different focuses and approaches of the different authorities involved. For example, while some stakeholders noted that collaborations between NRAs and CSIRTs are fruitful when they do occur, others claimed that such cooperation is still limited. Other stakeholders noted the problem of overlaps in responsibilities, which sometimes occurs between NRAs and other relevant authorities. Nevertheless, the stakeholders surveyed expressed their commitment to resolving any such overlaps.

Collaboration between national authorities and telecom providers is good	
Major telecommunication service providers and the NRAs communicate on a regular basis	The regularity of the cooperation varies: from cooperation 'based on necessity' to 'monthly meetings with the competent authorities' about specific topics (e.g. implementation of the 5G Toolbox).
Some interesting examples of good practice have been reported in select Member States	For example, in Portugal, a collaboration platform coordinated by the National Communications Authority (ANACOM) has been set up for telecom operators' security experts, where they can share and discuss their main issues.
Building and maintaining trust is key	Some stakeholders declared that the relationship between telecom operators and the authorities may not be fully transparent, as the operators are usually careful with the information they share. The majority of the authorities recognised the importance of building trust. They reported making significant efforts to improve collaboration by increasing the level of transparency in their decision-making.

Collaboration between telecom service providers is good	
Telecom service providers have expressed a desire to increase the level of security-related cooperation	Apart from bilateral exchanges, some service providers collaborate in informal groups or communities, where they share information on security topics. In some countries, there are formalised national cooperation groups, which are sometimes even led by the relevant authority.
The quality of such collaboration varies	In some countries, telecom service providers actively cooperate to solve major security incidents. However, in other countries they do not, reportedly because of 'strong competition'.

2.2. ASSESSMENT OF TELECOM LEGISLATION AT EU LEVEL

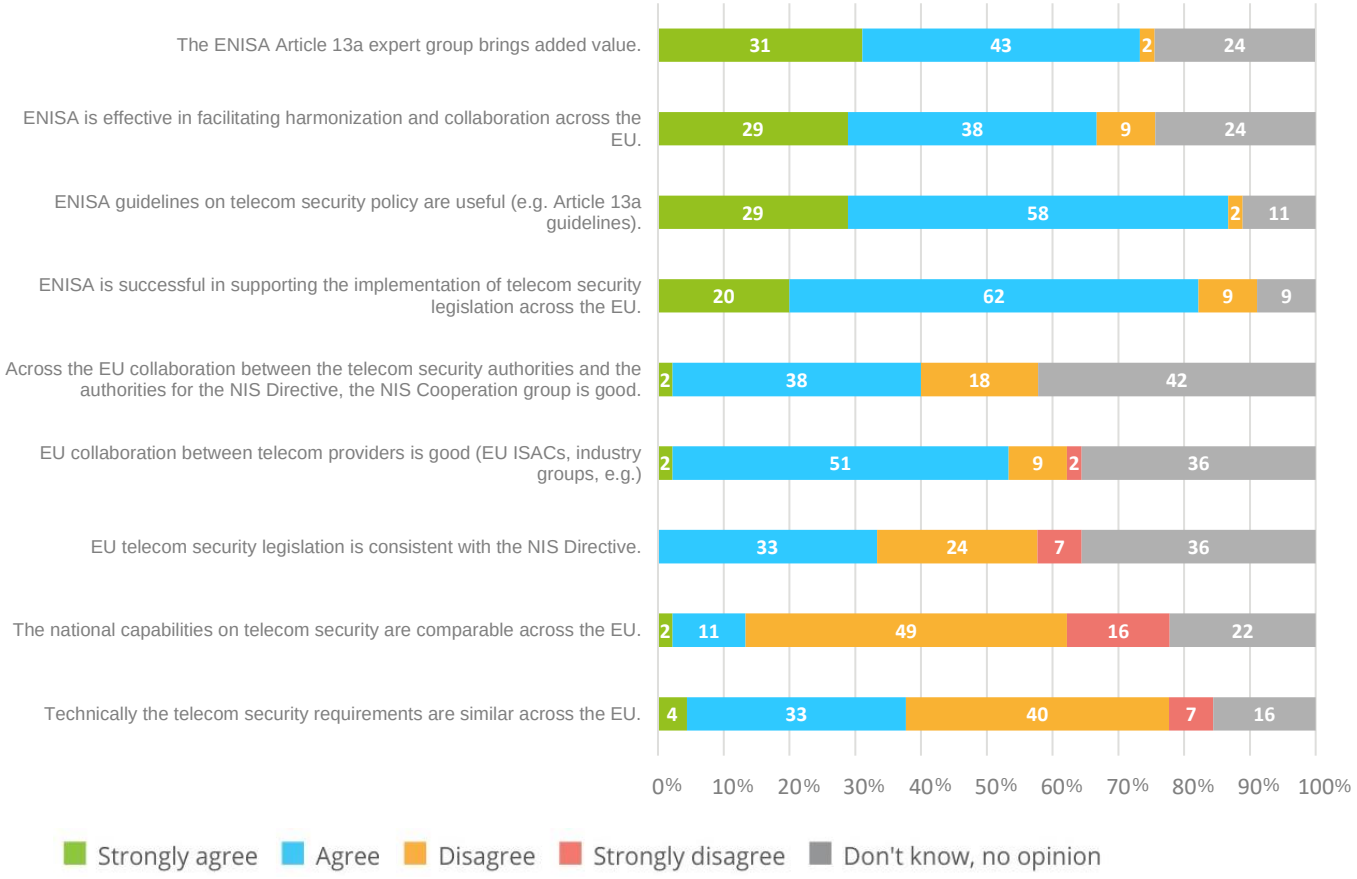
2.2.1. Summary

In summary, experts gave positive feedback on:

- the added value of the Article 13a Expert Group (now called ECASEC); and
- ENISA's role in supporting the implementation of EU telecom security legislation, as well as ENISA's technical guidelines.

On the other hand, experts highlighted issues with harmonisation and consistency. They did not agree that national capabilities in telecom security are comparable across the EU. In addition, experts expressed concerns about the consistency of telecom security requirements across the EU, as well as the consistency between EU telecom security legislation and the NIS Directive.

Figure 6: EU level – harmonisation and collaboration



2.2.2. Harmonisation of implementation across the EU

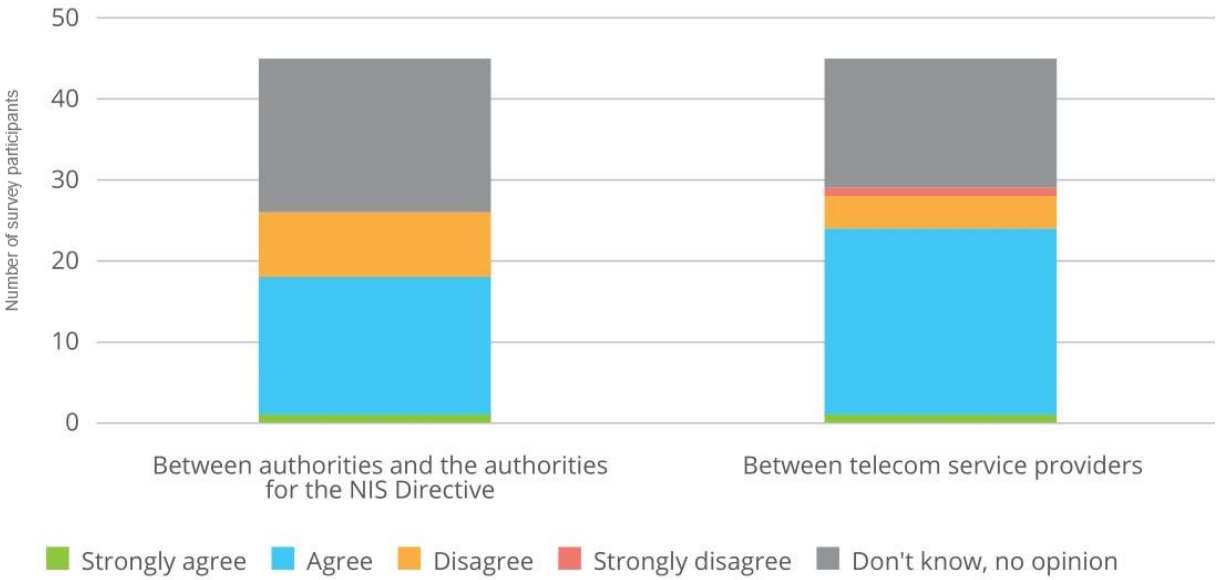
Article 13a was considered rather general in scope	Surveyed experts reported that this freedom of interpretation of Article 13a has led to dissimilar telecommunication security requirements across the Member States.
Article 13a Working Group guidelines have helped to an extent	However, one of the experts interviewed noted that there was 'no official endorsement from the side of the Commission, which leads to unharmonised processes in Member States'. Therefore, beyond legal requirements, some experts argued that it would be beneficial to standardise the implementation too. This would be particularly helpful to cross-border operators.

Figure 7: National capabilities on telecom sector security are comparable across the EU

2.2.3. Collaboration across the EU

EU-level collaboration is generally considered to be good, but it appears to have limited exposure. Many stakeholders could not answer the question on whether EU collaboration is good or had no opinion on the matter.

Figure 8: EU level collaboration is good between the following stakeholders



Most respondents had no opinion on collaboration between the NRAs, the NIS Directive competent authorities and the NIS Directive authorities. This suggests that there is a need to establish better links between these two groups of authorities.

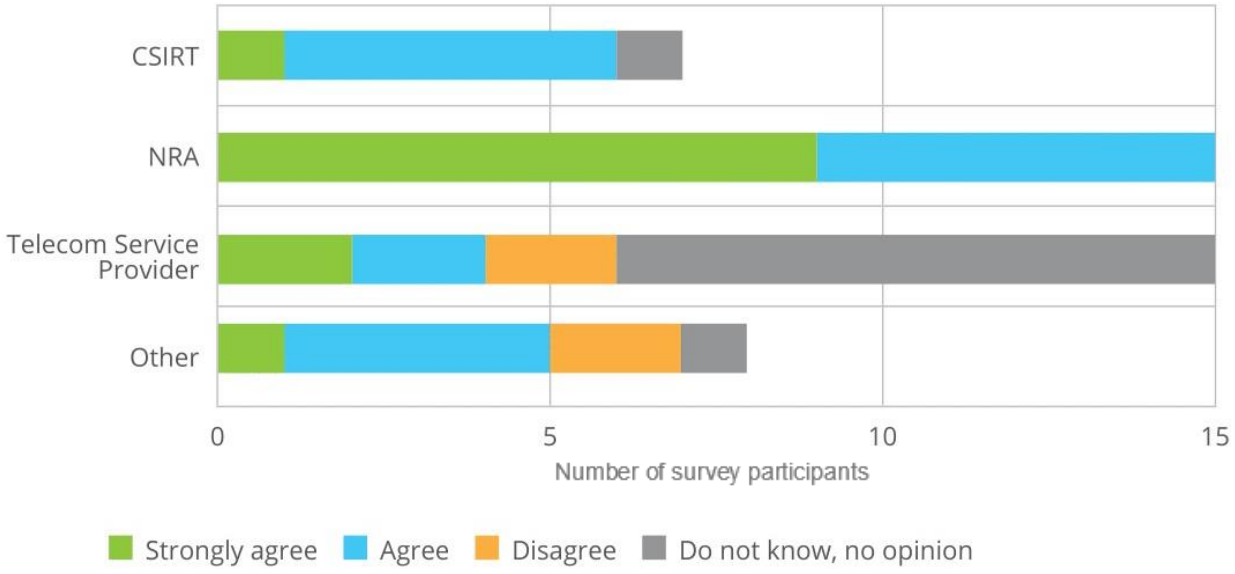
Most respondents considered EU-level collaboration between telecom providers to be good	
This may result from operations in multiple Member States	Strong EU-level collaboration between telecom providers may be connected to the fact that some major providers operate in multiple Member States, which makes it important for them to cooperate and harmonise processes.
34% of respondents could not answer the question, or had no opinion	Those respondents were mainly CSIRT and NRA representatives.

2.2.4. ENISA and Article 13a Expert Group

Role of Article 13a (now ECASEC) Expert Group described as 'extremely beneficial'	
Nevertheless, areas for improvement have been identified	Some telecom service providers did not find the work of the Article 13a Expert Group sufficiently transparent. Some respondents thought that there needs to be stronger collaboration between the Article 13a Expert Group and the NIS Cooperation Group.
Despite its achievements, the Article 13a (now ECASEC) Expert Group does not have a legal status	Some stakeholders also noted that, despite their usefulness, there has been no official approval of the Article 13a technical guidelines (now the revised ECASEC guidelines) by the European Commission. The stakeholders added that this results in unharmonised procedures.

ENISA plays a valuable role, but there is room for improvement	
Positive feedback concerned facilitation of knowledge sharing, incorporation of legislation and establishment of EU-wide guidelines	82% of participants surveyed agreed that ENISA is successful in supporting the implementation of telecommunications security legislation, 87% agreed that the guidelines provided by ENISA are useful and 67% agreed that ENISA is effective in facilitating harmonisation and collaboration across the EU. It was also claimed that ENISA is especially good at bringing together the different Member States. 74% of survey participants thought that the Article 13a (now ECASEC) Expert Group brings added value.
ENISA's guidelines are at too high a level	Some stakeholders expressed the need for more operational and technical guidance.
ENISA's powers and human resources are insufficient	Some stakeholders expressed concerns that ENISA might lack sufficient human resources to manage the more technical and operational tasks requested by many Member States.

Figure 9: ENISA is effective in facilitating harmonisation and collaboration across the EU



3. GOOD PRACTICE EXAMPLES

The experts gave examples of good practice during this assessment, either via the online survey or during the telephone interviews. Some of these suggestions are provided in the following sections.

Guidelines to assist the sector with implementing primary legislation

The Portuguese NRA, ANACOM, had introduced some additional secondary legislation to support telecom providers regarding regulatory interpretation and thus create a basis for more agile responses and approaches. Each telecom operator has to have an employee who is responsible for telecommunication regulation and security. In addition, each telecommunication operator has to have a contact point who is available 24/7; this is an operational position. A collaboration platform is also coordinated by ANACOM, where stakeholders can share and discuss security issues.

Resource and capability sharing

Resource sharing within the public sector. For inspections, the Belgian NRA, BIPT, can obtain help from other departments within the organisation, such as the controls-related department or the legal department. When specific cyber capabilities are needed, the Belgian NRA can obtain support from the national CSIRT or other security services, such as the crisis centre and intelligence services. In cases of both internal and cross-stakeholder types of collaborations and dynamic resource allocation, the effectiveness of task and responsibility fulfilment has been enhanced.

Resource sharing between the public and private sectors. The National Cyber Security Centre in Ireland has an extensive cooperation network with the private sector (e.g. with Amazon and Microsoft) and the partners provide technical assistance.

Combining responsibilities and competences for more streamlined operations. In Finland, Traficom combines the competences of the NRA, CSIRT and cybersecurity agency to maximise the available resources and streamline the execution of tasks.

Single incident-reporting platform

To address the issue of reporting incidents to multiple authorities, the Danish CFCS has developed a universal reporting tool, which is more efficient at sending reports to whichever authorities need to be informed.

Collaborative approach towards the private sector

The Radiocommunications Agency Netherlands uses a collaborative approach to build trust with telecommunication service providers. It tends to avoid the use of fines as a means of control because it considers it more important to create a learning curve, create the right mindset and help service providers improve their cybersecurity and risk-management processes.

The Belgian Institute for Postal Services and Telecommunications tries to carry out inspections and audits in a cooperative way (e.g. providing regular communication and feedback), as, ultimately, it has the same objective as the telecommunication service providers, which is to increase security in Belgium. It noted that those in security teams may find this process annoying initially; however, they realise that the reports help them to obtain resources and organisational support for their projects and improve their security standing.

Collaboration through common projects

Project-based collaboration is a good way to build trust. Belgium provided an example of such a process. In the context of the NIS Directive, there was a need for an incident notification platform. The Belgian Institute for Postal Services and Telecommunications offered the use of its own telecommunication incident notification platform to avoid the need for all authorities to develop their own. It worked closely with the Centre for Cyber Security Belgium to share its incident notification platform and practices. This helped to build trust and improve collaboration between the different authorities involved.

4. CHALLENGES AND RECOMMENDATIONS

This section gives an overview of the perceived future challenges for the sector and lists several recommendations for ENISA and the national authorities.

4.1. CHALLENGES FOR THE SECTOR

The key challenges for the EU telecom sector are:

- next-generation networks, such as network function virtualisation (NFV) and 5G
- cybersecurity skills shortages
- dependencies on vendors and suppliers.

These challenges are described in more detail below.

Complexity of new technologies such as NFV and 5G	The most frequently mentioned challenge was adaptation to and implications of the use of next-generation network technology, such as Network Function Virtualization (NFV) and 5G. 5G not only constitutes a technology change. It also introduces new business models, new vendors and network architecture changes. One expert noted: 'New types of technologies and new types of services are gaining ground, such as machine-to-machine (M2M) and over-the-top (OTT), which brings up different types of security issues.'
Shortages of cybersecurity skills	89% of the online survey respondents identified the availability of cybersecurity skills as one of the biggest challenges in the sector. Some stakeholders reported that this skills shortage is affecting their core operations. Without the required technical expertise, many security challenges become even harder to tackle. For example, even if a public authority has the power to impose specific measures, exercising this power (e.g. effective monitoring) becomes very difficult without the right expertise.
Security gaps in the supply chain	Some of the main challenges highlighted were supplier dependence, lack of security requirements for suppliers, outsourcing and geopolitical issues. According to the online survey and the interviews, many telecom service providers move parts of their operations outside their own countries because of more favourable legislative or business environments. This makes it difficult to oversee or influence critical security factors, and it introduces geopolitics into the security aspect of the supply chain.

4.2. RECOMMENDATIONS FOR ENISA AND THE NATIONAL AUTHORITIES

Experts made several recommendations for ENISA and the national authorities.

Implement new legislation, regulations and related guidelines in a timely and harmonised manner	Timely implementation of the EECC, the EU 5G Toolbox and any related recommendations was identified as the main short-term goal. Experts stressed the need for simplicity and harmonised approaches. The Article 13a Expert Group (now ECASEC) was seen as making a positive contribution to this harmonisation. A priority topic going forward for the Article 13a Expert Group (now ECASEC) and the 5G Toolbox is supply chain security and risks. Developing EU-level standardisation has also been identified as important.
Increase collaboration between private and public sectors – at both EU level and national level	Experts would like to see better and earlier involvement of the private sector, including at the earliest stage of policymaking. This includes providing the private sector with more exposure to ENISA's work. This would contribute to the private sector's understanding of its own obligations and the steps it needs to take to fulfil them. The majority of authorities also recognised the need for deeper collaboration between private and public sectors and reported that considerable efforts are being made to build trust.
Provide more technical guidelines and share them with stakeholders as soon as possible	Technical guidelines provided by ENISA and national authorities are considered useful. However, stakeholders noted that they would find it beneficial to have more detailed guidelines that break the legislation down into specific operational requirements. Telecom providers expressed the need for such guidelines to be made available as soon as possible to facilitate the smooth implementation of legislative requirements.
Review incident-reporting focus areas, carefully define thresholds and avoid obligation overlaps	Avoiding unclear and overlapping obligations on telecom providers from different authorities was one of the key recommendations. For example, as in the Danish (CFCS) good practice example, this could be achieved by creating a single reporting platform where telecom providers could upload their reports, which could then be accessed by relevant authorities. When defining reporting thresholds, stakeholders recommended considering the inclusion of other aspects of network integrity besides focusing on the duration of service interruption. Experts also stated that they would like to see harmonised reporting thresholds across the EU, based on services' characteristics.
Provide regular and detailed feedback on reported incidents	Telecom providers expressed the need for regular and detailed feedback on the incidents they report. They reasoned that such feedback could contribute to creating a learning environment.

5. CONCLUSIONS

In this report, we have provided an overview of an assessment of the EU telecom security legislation that was carried out in 2020. In this section, we list the main conclusions and recommendations.

5.1. CONCLUSIONS FROM THE SURVEY AND INTERVIEWS

1. **EU telecom security legislation has a positive impact.** Based on the responses from our stakeholders, security provisions in the EU regulatory framework, specifically in the Telecom Framework Directive, have successfully contributed to a high level of cybersecurity in the telecommunications sector. Indeed, most respondents were of the view that, in general, there is a culture of risk management across EU Member States and the security measures taken are appropriate.

2. **The legislative framework is complex.** Notwithstanding the above, some stakeholders find national legislation rather complex. Moreover, some of the experts surveyed reported that the generality of Article 13a of the Telecom Framework Directive has led to dissimilar security requirements across the Member States.

3. **Authorities have powers, but few resources.** The powers of the national telecom security authorities are considered sufficient, but there are concerns about scarcity of resources and expertise.

4. **Incident reporting could be improved.** In general, national-level incident reporting is working well, but there is room for improvement. Apart from the scarcity of feedback on reported incidents, doubts sometimes arise over which authority a specific incident should be reported to, which results in telecom operators occasionally reporting the same incident to more than one authority.

5. **Collaboration at national and EU levels is good.** In the latter context, stakeholders recognised the positive contribution of ENISA and the Article 13a (ECASEC) Expert Group. Nevertheless, some challenges were identified, such as the issue of involvement of the private sector in policymaking at both national and EU levels and the relatively low exposure of the private sector to existing EU-level collaboration.

5.2. RECOMMENDATIONS MADE BY THE EXPERTS

The experts we engaged with also made recommendations for ENISA and the national authorities.

1. **Prioritise the implementation of new policies and legislation.** To keep fostering the culture of risk management, timely implementation of the EECC, the EU 5G Toolbox and any related recommendations was identified as the main short-term goal.

2. **Address skills shortages with resource sharing and collaboration.** To address cybersecurity skills shortages, it is important to explore resource and capability sharing. Several resource- and capability-sharing models have been identified to address this, for example resource sharing among public sector stakeholders and compensating resource shortages with private sector collaborations.

3. **More technical guidance for service providers.** While the stakeholders described the outputs of ENISA and the Article 13a (ECASEC) Expert Group as ‘extremely beneficial’, they also expressed the need for more detailed guidelines that break down

the legislation into specific operational requirements. At national level, this report also provides examples of good practice to assist with the interpretation of primary legislation, such as the use of supplementary regulatory instruments and guidelines, and the provision of more direct assistance – such as collaboration groups or contact points.

4. **Improving and streamlining incident reporting.** In addition to clarifying incident-reporting obligations at national level, this report highlights some examples of good practice to address the problem of telecom operators reporting the same incident to more than one authority. Moreover, to improve incident reporting, it is important that the authorities provide feedback in response to the submitted reports.

5. **Better engagement with the private sector.** Regarding both national- and EU-level collaboration, stakeholders would like to see better and earlier involvement of the private sector, including at the earliest stage of policymaking. There may also be a need to increase the level of dissemination of information to the private sector to increase exposure to EU-level collaboration. Finally, the majority of the authorities recognised the importance of building trust between them and the private sector entities they supervise.

We would like to repeat our expressions of gratitude for the valuable feedback provided by the experts who were surveyed and interviewed. We look forward to continuing to work with the sector and the national authorities to address the issues identified in the assessment, and we will follow up on the recommendations made.

TP-02-21-565-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-505-0
DOI: 10.2824/30649