An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Incident Reporting Thresholds

A consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards)

Consultation

Reference: ComReg 23/36

Version: Final

Date: 25/04/2023

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Legal Disclaimer

This Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Commission for Communications Regulation is not bound by it, nor does it necessarily set out the Commission's final or definitive position on particular matters. To the extent that there might be any inconsistency between the contents of this document and the due exercise by it of its functions and powers, and the carrying out by it of its duties and the achievement of relevant objectives under law, such contents are without prejudice to the legal position of the Commission for Communications Regulation. Inappropriate reliance ought not therefore to be placed on the contents of this document.

Content

Section Page

1 Executive Summary 6

1.1 Management of the integrity of Networks 7

1.2 Proposed Approach Differences and Benefits 8

2 Introduction and Background 11

2.1 The New European legislation 14

2.1.1 Article 40 of the EECC: Security of networks and services 14

2.1.2 Article 41 of the EECC: Implementation and enforcement 15

2.1.3 Section 11 of the Act: Providers to notify Commission of any incident of significant impact on networks or services 16

2.1.4 The ENISA Revised Guidelines 18

2.2 Chapters of this Document 19

3 Draft Regulatory Impact Assessment ("RIA") on Incident Reporting Thresholds 20

3.1 Introduction 20

3.2 RIA Framework 20

3.3 Structure for the RIA 21

3.4 Identification of stakeholders and approach to Steps 3 and 4 21

3.5 Step 1: Identify the policy issues & the objectives 23

3.5.1 Policy Issues 23

3.5.2 ComReg's current thresholds for reporting incidents 24

3.5.3 The European Electronic Communications Code and its transposition into Irish Law 25

3.5.4 Thresholds for the reporting of an incident to ENISA by ComReg 27

3.6 Step 2: Identify and describe the regulatory options 29

3.7 Impact on Stakeholders 30

3.8 ComReg's preferred option 35

4 Incident Thresholds & Reporting 36

4.1 Incident reporting 36

4.2 Changes to Incident Reporting 36

4.2.1 Incident Types and Services Covered Pursuant to the Act 36

4.2.2 Categorisation of Incidents, Reporting Thresholds and Information Required 38
4.2.3 National User Base Calculations 39
4.3 Reporting Process 40
4.3.1 Reporting Incidents to ComReg 41
4.3.2 Information Requirements for an Incident Report 41
4.3.3 Timings for Incident Reporting 42
4.3.4 Exception: Storm Reporting 44
4.3.5 Information Required by the Minister, European Commission, Other NRAs and ENISA. 45
4.3.6 Confidentiality of Submitted Information 45
5 Implementation & Enforcement 47
6 Submitting comments and Next Steps 49

Annex

Section Page

Annex: 1 Legal Basis.....51

Annex 2: Draft Decision Document Replacement of Comreg Document No. 14/02 –draft Decision Instrument 55

1 Executive Summary

1. In December 2018, a revision of the European telecoms regulatory framework, called the European Electronic Communications Code (the "EECC") was published and entered into force on 20 December 2018. The EECC updates the preceding European Telecoms Framework of 2009 and, amongst other things, encourages the roll out of fibre, very high-capacity networks and fifth generation mobile networks ("5G").

2. The EECC brings more communications services within scope and the terms "security" and "security incidents" are expressly defined. Article 40 of the EECC details security obligations for providers of: electronic communications networks and services, and of Number Independent Interpersonal Communication Service ("NI-ICS")[1].

3. Article 40 requires that providers of public electronic communications networks and/or services take appropriate and proportionate technical and organisational measures –to appropriately manage the risks posed to the security of their networks and services. In particular, measures including encryption, where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services. It also requires providers to report significant incidents without undue delay to competent national authorities, who should report about these security incidents to the European Agency for Cybersecurity ("ENISA") and the European Commission ("EC") annually[2].

4. Furthermore, Article 41 empowers the Competent Authority ("CA")[3] to implement and enforce these measures.

5. Articles 40 and 41 of the EECC replace Article 13a and 13b of the current Telecoms Framework Directive, as amended. Articles 40 and 41 of the EECC are transposed in Part 2 ("Security of Networks and Services") of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, (No. 4 of 2023) (the "Act").

6. This consultation presents ComReg's views on:

    - The thresholds and timescales required for the reporting of security incidents to ComReg;

[1] NI-ICS are as defined in Article 2(7) of the EECC and Regulation 2 of the Regulations of 2022 , and are now included in the revised definition of an ECS, as set out in Regulation 2 of the Regulations of 2022 and furthermore NI-ICS are now included in Article 2(4) of the EECC.
[2] Transposed in s.11(9) of the Act.
[3] In this case ComReg under the Act.

- The process for communicating details of security incidents to ComReg; and

- The approach that will be followed by ComReg to enable it to monitor providers' compliance with the obligations imposed on them under Article 40 and as required of it by Article 41 of the EECC.

7. This consultation and associated Draft Decision, contained in Annex 2 to this document (the "Draft Decision"), sets out proposals as to how ComReg plans to implement the relevant provisions of the EECC and the Act and seeks views from respondents. The consultation and Draft Decision also describe the actions ComReg expects providers to take, to ensure compliance with the Act.

1.1 Management of the integrity of Networks

8. ComReg does not intend to be too prescriptive as to what specific measures providers should employ when managing the integrity of networks. Rather, ComReg recognises that such measures will inevitably vary between providers. However, Article 40 requires that providers take appropriate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures taken, must ensure a level of security appropriate to the risk presented.

9. This consultation in the main, refers to the incident reporting thresholds for providers under the ENISA Revised Guidelines[4]. It is noted, that contrary to the previous practice, there are not only updated thresholds, as a consequence of Article 40 of the EECC, but greater information requirement obligations on providers. This includes:

- Reference to the geographic area affected, (Whole Country, Province County or Island);

- When there is Cross Border impact affecting another Member State ("MS") or relevant third country;

- Impact on a particular class of users[5]; or

[4] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu), https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

[5] "user" means a natural or legal person using or requesting a publicly available electronic communications service; see Regulation 2(1) of the European Union (Electronic Communications Code Regulations) 2022, S.I. No. 444 of 2022.

- Has a severe impact on economic and societal activities.[6]

10. The ENISA Revised Guidelines provide a guide to a CA on the significance of the incident and the measures that have been taken by a provider.

11. ComReg may also issue a security measures direction to require a provider to:

(a) provide information that would be used to assess the security[7] of the services and networks of that provider; and

(b) where necessary to submit to a security audit by the Commission or a qualified independent person nominated by ComReg[8].

1.2 Proposed Approach Differences and Benefits

12. The draft Regulatory Impact Assessment (draft "RIA") in Chapter 3 considers and evaluates the options available to ComReg for it to fulfil its statutory obligations under Part 2 of the Act. After evaluation of the options in the RIA, the proposed approach has the following differences and benefits:

a. When reporting an Incident, providers must now categorise the incident. That is, whether the incident can be categorised as affecting: Confidentiality, Integrity, Authenticity or Availability, as defined below:

- **Confidentiality[9];** means, the confidentiality of communications, communications data or metadata has been compromised. For example, but not limited to, the encryption on a service does not work or has been compromised and unauthorised access takes place with the communications being forwarded to unauthorised parties;

- **Integrity** [10]; means, the integrity of the communications data or metadata has been compromised. For example, but not limited to, the IP address and caller id have been tampered with routing the communications to a third party or unauthorised software has been installed on a server;

[6] ComReg expects to publish a report on this in Q2 2023.
[7] Section 14 (3)(c) of the Act.
[8] Section 14 (3)(d) of the Act.
[9] Confidentiality is typically defined as a property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 7)
[10] Integrity is typically defined as a property of accuracy and completeness (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 8)

- **Authenticity** [11]; when there is a compromise of user's identity (identity fraud). For example, man-in-the-middle attacks or eavesdropping on applications lead to theft and misuse of authentication credentials, user accounts become accessible and taken over by attackers; and

- **Availability**[12] ; when the incident affects the continuity of supply of services, degrades the performance of the service, the network or service is "completely" or "partially" down. This is often called 'outage' or 'disruption'.

b. Several thresholds remain from the prior approach outlined in Reporting & Guidance on Incident Reporting & Minimum Security Standards ComReg Document 14/02 ("Document 14/02"), but now, providers will be required to report incidents which have an impact on the **confidentiality**, **authenticity** and **integrity** of the networks and services they provide using the relative threshold. In such instances, an incident should be included if the number of users affected is more than 1% of the National User Base of that service, the calculations for which are set out in Section 4.2.3 below; or it exceeds the **absolute threshold**. The absolute threshold is the product of the duration and the number of users affected for a particular service. ENISA recommends that this threshold is applied for security incidents which have an impact on **availability**[13] and that any such incident be included in the annual summary report if the absolute threshold is greater than or equal to one million (1,000,000) user hours lost.

c. The information now to be supplied is encapsulated in the Act[14], and is as standardised in Article 40(2) of the EECC for all MS. ComReg notes that typically, providers would in any event already report such incidents voluntarily under the current reporting obligations. The approach proposed in this consultation therefore provides for a pragmatic reporting methodology, minimising ambiguities and simplifying the reporting requirements for provider.

d. Timely reporting of incidents allows for valuable lessons to be learned quickly and sharing learnings from incidents with ENISA ensuring that other MS benefit, and vice versa. This approach promotes improved resilience of networks throughout MS and helps mitigate any further propagation of incidents.

[11] Authenticity is typically defined as a property that an entity is what it claims to be (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 9)
[12] Availability is typically defined as a property of being accessible and usable on demand by an authorized entity (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 6)
[13] Defined in Article 2 of the EECC.
[14] S. 11 of the Act.

13. Furthermore and the Draft RIA below notwithstanding, there are other obvious benefits in the revised approach:

- The use of the incident reporting portal by more providers will simplify the reporting requirements, while enhancing the consistency necessary for summary reporting to ENISA, pursuant to section 11(9) of the Act;

- Following the completion of this consultation process, ComReg intends that in the main the reporting thresholds and timings, where practicable, will be aligned more closely with the ENISA Revised Guidelines, facilitating comparison between MS; and It is intended to capture all of the thresholds and timings in a separate reference ComReg Document which is presented along with this consultation, in Annex 2 to this document as the Draft Decision. This document is intended to replace ComReg's current procedural document regarding Incident Reporting and Minimum Security Standards for Network Operators[15] Document 14/02.

[15] https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf

2 Introduction and Background

14. The Commission for Communications Regulation ("ComReg") is the statutory body responsible for the regulation of the electronic communications sector in Ireland. Its activities are governed in part by several Directives enacted by the European Union, which have been transposed into Irish law.

15. ComReg Document 14/02[16] currently sets out the appropriate thresholds for reporting incidents[17], affecting Electronic Communications Networks or Services ("ECN" and "ECS") based on the European Communities (Electronic Communications Networks and Services) (Framework) Regulations, SI 333 of 2011) (the "Framework Regulations") and the European Agency for Cybersecurity ("ENISA") Technical Guideline on Reporting Incidents, December 2011 (the "2011 Guidelines").

16. On 20 December 2018, a revision of the European regulatory framework, relating to the electronic communications sector, called the European Electronic Communications Code[18] (the "EECC") entered into force. The EECC updates the preceding European Telecoms Framework of 2009 by repealing and replacing the underlying EU Directives ("Telecoms Framework"), namely the: Framework Directive[19]; Authorisation Directive[20]; Access Directive[21]; and Universal Services Directive[22].

17. The security provisions of the EECC, namely Articles 40 and 41, will be transposed into Irish law and are reflected in Part 2 ("Security of Networks and Services") of

[16] Response to Consultation – Reporting and Guidance on Incident Reporting and Minimum Security Standards – https://www.comreg.ie/publication/response-to-consultation-reporting-guidance-on-incident-reporting-minimum-security-standards

[17] ENISA uses a working definition of an incident as follows: An incident is "an event which can cause a breach of security or a loss of integrity of electronic telecommunications networks and services." A reportable incident is defined in that document as: "A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services."

[18] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code – https://eur-lex.europa.eu/eli/dir/2018/1972/oj

[19] EUR-Lex - 32002L0021 - EN - EUR-Lex (europa.eu) - https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0021

[20] EUR-Lex - 32002L0020 - EN - EUR-Lex (europa.eu) https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0020

[21] EUR-Lex - 32002L0019 - EN - EUR-Lex (europa.eu) - https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0019

[22] EUR-Lex - 32002L0022 - EN - EUR-Lex (europa.eu) - https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0022

the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, No. 4 of 2023, (the "Act"), once commenced.

18. Other elements of the EECC, not of direct relevance to this consultation, will be transposed in the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022") once commenced.

19. Furthermore, on 22 March 2021, ENISA published revised guidelines on incident reporting, under the EECC (the "ENISA Revised Guidelines"). [23] These helpfully provide guidance to the Member States' ("MS") National Regulatory Authorities ("NRAs") that supervise security and integrity in electronic communications and other Competent Authorities ("CAs") as defined in the EECC.

20. Under the EECC and the Act, the security incident reporting obligation applies to "providers". In the context of this document, the term 'provider' is as defined in section 5 of the Act[24].

21. Article 40, in a similar manner to the existing EU Framework, continues to require ECN and ECS providers to report significant security incidents to ComReg. The definition of 'security incident' is now explicitly defined in section 5 of the Act as, '*any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services'* . [25]

22. Furthermore, Article 40 of the EECC details security obligations for providers of ECN, ECS, and Number Independent Interpersonal Communication Service ("NI-ICS")[26].

23. In the event of a security incident that has a significant impact on the operation of ECN, ECS or NI-ICS, the draft reporting obligations for providers are outlined in Chapter 4 of this document.

[23] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu), https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

[24] "provider" means a provider of public electronic communications networks or of publicly available electronic communications services.

[25] Section 5 of the Act.

[26] NI-ICS are as defined in Article 2(7) of the EECC and Regulation 2 of the Regulations of 2022 , and NI-ICS and are now included in the revised definition of an ECS, as set out in Regulation 2 of the Regulations of 2022 Article 2(4) of the EECC, NI-ICS are now included.

24. Article 41 outlines how ComReg can implement and enforce the security incident requirements and reporting obligations[27], as detailed in Chapter 5 of this document.

25. Currently, when ComReg receives a report of a significant incident affecting ECN and ECS, as defined by the Framework Regulations, it is required to inform the Minister[28]. With the agreement of the Minister and where appropriate, ComReg must also inform the NRAs of other affected Member States ("MS"), the European Commission ("EC") and ENISA[29]. Where it is in the public interest, and again with the agreement of the Minister, ComReg may inform the public of such an incident or require the provider concerned to do so[30].

26. Sections 11(5) (a),(b) and s. 11(6) of the Act reflect the provisions contained in Regulation 23 of the Framework Regulations, as detailed above.

27. This consultation document:

- outlines the additional requirements introduced by the EECC and the Act as compared to those in Document 14/02;
- clarifies the appropriate thresholds for reporting incidents;
- the requisite timing for submission of these reports; and
- is published in draft, alongside Annex 2 to this document, the Draft Decision Document, which will, in final form, replace Document 14/02.

28. The proposed updated thresholds and processes for reporting, as detailed below, reflect ComReg's provisional view of what is required by providers to comply with the reporting requirements. ComReg's approach takes account of the guidance provided by the ENISA Revised Guidelines.

29. This consultation, and the accompanying draft Decision Document (contained in Annex 2 to this document), outlines ComReg's proposed approach to assessing

[27] It should be noted that management of an incident is the sole responsibility of the provider concerned, calling upon the resources they require, as appropriate, to assist in the efficient handling of the issue. In some circumstances this may include a provider requesting the support of ComReg or another relevant body, for example, to assist in its coordination of the incident response with other parties, such as other interconnected providers. This request for support should not be confused with the reporting process to ComReg which will be used by ComReg to undertake its statutory obligations of ensuring compliance by providers with their obligations under the EECC and the Act.
[28] The Minister for the Department of the Environment, Climate and Communications ("DECC"). See Regulation 23(4)(b) of the Framework Regulations 2011.
[29] ENISA -The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.
[30] Regulation 23(4)(c) of the Framework Regulations 2011.

providers' compliance with their reporting obligations in respect of Article 40(1), (2) and (3), which will be transposed by Part 2 of the Act (once commenced).

2.1 The New European legislation

30. The EECC updates and merges the existing European framework governing the European telecommunications sector. Most of the EECC is being transposed into Irish law by secondary legislation, namely the European Communications Code Regulations 2022. The Act gives effect to the EECC provisions not included in the Regulations of 2022, including those provisions related to security, as well as making several further provisions at national level in relation to enforcement and amendments to the Communications Regulation Act 2002 (the "Principal Act"). This consultation relates to the relevant provisions of Articles 40 and 41 of the EECC, as transposed in section 11 of the Act.

2.1.1 Article 40 of the EECC: Security of networks and services

31. Relevant provisions of Article 40 ("Security of networks and services") are as follows:

> 1 *Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.*
>
> *The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council (1), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.*
>
> 2 *Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services*

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical spread of the area affected by the security incident;

(d) the extent to which the functioning of the network or service is affected;

(e) the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph[31].

3 Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself.

32. Article 2(42) of the EECC defines a "security incident" as meaning: "an event having an actual adverse effect on the security of electronic communications networks or services".

2.1.2 Article 41 of the EECC: Implementation and enforcement

33. Article 41 ("Implementation and Enforcement") provides as follows[32]:

1 Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to issue binding instructions,

[31] Annual summary reporting.
[32] To note that Article 41 is transposed in sections 14 to 16 of the Act. 2022.

including those regarding the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time-limits for implementation, to providers of public electronic communications networks or publicly available electronic communications services.

2 Member States shall ensure that competent authorities have the power to require providers of public electronic communications networks or publicly available electronic communications services to:

(a) provide information needed to assess the security of their networks and services, including documented security policies; and

(b) submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit shall be paid by the provider.

3 Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non- compliance and the effects thereof on the security of the networks and services.

4 Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of a Computer Security Incident Response Team ('CSIRT') designated pursuant to Article 9 of Directive (EU) 2016/1148 in relation to issues falling within the tasks of the CSIRTs pursuant to point 2 of Annex I to that Directive.

5 The competent authorities shall, where appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities, the competent authorities within the meaning of Article 8(1) of Directive (EU) 2016/1148 and the national data protection authorities.

2.1.3 Section 11 of the Act: Providers to notify Commission of any incident of significant impact on networks or services

34. Section 11 of the Act, which transposes relevant provisions of Articles 40 and 41 of the EECC is set out below:

(1) A provider shall, where any security incident occurs that has had or is having a significant impact on the operation of the provider's electronic communications

networks or services, notify the Commission in accordance with subsection (3) without undue delay.

(2) In order to determine whether the impact of a security incident is significant for the purposes of subsection (1) a provider shall have regard to the following matters in respect of the incident: (a) the duration of the incident; (b) the number of users affected; (c) any class of users particularly affected; (d) the geographical area affected; (e) the extent to which the functioning of the network or service was affected; (f) the impact of the incident on economic and societal activities; (g) the cause of the incident and any particular circumstances that resulted in the security incident.

(3) A notification made under subsection (1) shall contain the following information in relation to the incident: (a) the provider's name; (b) the public electronic communications network or publicly available electronic communications services provided by it affected by the incident; (c) the date and time the incident occurred and its duration; (d) the information specified in paragraphs (a) to (g) of subsection (2); (e) information concerning the nature and impact of the incident; (f) information concerning any or any likely cross-border impact; (g) such other information as the Commission may specify.

(4) Where a provider notifies the Commission of an incident in accordance with this section it shall, as soon as practicable, notify the Commission when the incident is resolved and of the actions taken by it to remedy the incident and, where applicable, any actions taken to reduce the likelihood of a similar incident occurring in the future.

(5) Where the Commission is notified of a security incident under subsection (1) it shall— (a) inform the Minister of the notification, and (b) where the Commission, having consulted with the Minister, considers it appropriate to do so, notify the competent authorities of other Member States and ENISA.

(6) Where the Commission determines, having consulted with the Minister, that the disclosure of a security incident notified under subsection (1) is in the public interest it may inform the public of the incident or require the provider concerned to do so.

(7) Subsections (1), (2), (3) and (4) are regulatory provisions.

(8) A provider— (a) who fails to notify the commission in accordance with subsection (1), (b) who fails to make all reasonable efforts to provide the information referred to in subsection (3), or (c) that is required by the Commission under subsection (6) to inform the public of a security incident and that fails to do so, commits an offence and is liable on summary conviction to a class A fine.

(9) The Commission shall in each year submit a summary report to the Minister, the European Commission and ENISA on the notifications received and the actions taken by the Commission in accordance with this section.

35. Section 5 of the Act defines "security incident" as meaning: "any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services".

2.1.4 The ENISA Revised Guidelines

36. The ENISA Revised Guidelines on Incident Reporting under the EECC[33] describe the formats and procedures for cross border reporting and annual summary reporting under Article 40 of the EECC. Paragraph 2 of Article 40 describes three types of incident reporting:

1) National incident reporting from providers to CAs and NRAs;

2) Ad-hoc incident reporting between CAs, NRAs and ENISA; and

3) Annual summary reporting from CAs and NRAs to the EC and ENISA. The focus of this guideline is on ad-hoc incident reporting and annual summary reporting.

37. ENISA aims to use annual summary reporting for the following purposes:

- To give feedback to CAs and NRAs regarding:
  - Security incidents that have had significant impact;
  - Root causes of security incidents;
  - Lessons learned from security incidents; and

[33] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu) https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

- Incident trends.

- To provide aggregate analysis of incidents for policy makers, the public and the industry, describing overall frequency and impact of security incidents across the EU;
- To facilitate the exchange of experiences and lessons learned among CAs and NRAs;
- Issue recommendations and guidance for CAs, NRAs, the private sector, policy makers; and
- Evaluate the effectiveness of security measures in place.

2.2 Chapters of this Document

38. The Chapters of this Document deal with the following subjects:

Chapter 1	Executive Summary;
Chapter 2	Introduction and Background;
Chapter 3	Draft Regulatory Impact Assessment (“RIA”);
Chapter 4	Incident Thresholds & Reporting;
Chapter 5	Implementation & Enforcement;
Chapter 6	Submitting comments and Next Steps;
Annex 1	Legal Basis; and
Annex 2	Draft Decision Document.

3 Draft Regulatory Impact Assessment ("RIA") on Incident Reporting Thresholds

3.1 Introduction

39. ComReg is of the preliminary view that it is necessary to review the incident reporting thresholds set out in Document 14/02 and determine whether new thresholds are more appropriate to comply with the EECC as transposed by the Act (once commenced). As described in Chapter 4 that follows, these are primarily based on the ENISA Revised Guidelines and this chapter sets out ComReg's draft RIA on incident reporting thresholds.

3.2 RIA Framework

40. A RIA is an analysis of the likely effect of a proposed new regulation(s) or regulatory change(s) and, of whether regulation is necessary at all. The RIA should help identify regulatory options and establish whether the proposed regulation is likely to have the desired impact, having considered relevant alternatives and the impact on stakeholders. The RIA is a structured approach to the development of policy and analyses the impact of regulatory options. In conducting a RIA, the aim is to ensure that all proposed measures are: appropriate, effective, proportionate and justified.

41. A RIA should be carried out as early as possible in the assessment of regulatory options, where appropriate and feasible. The consideration of the regulatory impact facilitates the discussion of options, and a RIA should therefore be integrated into the overall preliminary analysis. This is the approach which ComReg follows in this consultation and this draft RIA should be read in conjunction with the overall consultation. The RIA will be finalised in the final Decision arising from this consultation, having considered responses to this consultation.

42. In conducting the RIA, ComReg has regard to the RIA Guidelines [34], while recognising that regulation by way of issuing decisions, for example imposing obligations or specifying requirements in addition to promulgating secondary

[34] Guidelines on ComReg's Approach to Regulatory Impact Assessment – ComReg Document 07/56a -https://www.comreg.ie/publication/guidelines-on-comregs-approach-to-regulatory-impact-assessment

legislation, may be different to regulation exclusively by way of enacting primary or secondary legislation.

43. To ensure that a RIA is proportionate and does not become overly burdensome, a common-sense approach is taken towards a RIA. As decisions are likely to vary in terms of their impact, if after initial investigation, a decision appears to have relatively low impact ComReg may carry out a lighter RIA in respect of that decision.

3.3 Structure for the RIA

44. In assessing the available regulatory options, ComReg's approach to the RIA is based on the following five steps:

- **Step 1:** describes the policy issue and identifies the objectives;
- **Step 2:** identifies and describes the regulatory options;
- **Step 3:** determines the likely impacts on stakeholders;
- **Step 4:** determines the likely impacts on competition; and
- **Step 5:** assesses the likely impacts and choose the best option.

45. In the following sections, ComReg identifies the specific policy issues to be addressed and relevant objectives. (i.e., Step 1 of the RIA process). Before moving on to Step 1 of the RIA, ComReg first makes some relevant observations below on the stakeholders involved and on ComReg's approach to Steps 3 and 4.

3.4 Identification of stakeholders and approach to Steps 3 and 4

46. Step 3 assesses the likely impact of the proposed regulatory measures on stakeholders. Hence a necessary precursor, is to identify such stakeholders.

47. In this RIA, stakeholders fall into two main groups:

- Consumers (Impact on consumers is considered separately below); and
- Industry stakeholders

48. Step 4 assesses the impact on competition, of the various regulatory options available to ComReg. In that regard, ComReg notes that it has various

statutory functions, objectives and duties which are relevant to the issue of competition.

49. Of themselves, the RIA Guidelines and the Ministerial Policy Direction on Regulatory Impact Assessment[35] provide little guidance on how much weight should be given to the positions and views of each stakeholder group (Step 3); or the impact on competition (Step 4). Accordingly, ComReg has been guided by its primary statutory objectives which it is obliged to seek to achieve when exercising its functions. ComReg's statutory objectives include, to:

- promote competition[36];
- contribute to the development of the internal market[37];
- promote the interests of users within the Community[38];
- ensure the efficient management and use of the radio frequency spectrum in Ireland in accordance with a direction under Section 13 of the 2002 Act[39]; and
- promote efficient investment and innovation in new and enhanced infrastructures[40].

50. In addition, ComReg is guided by regulatory principles and obligations provided for under the EECC. Such principles and obligations are outlined further at Annex 1.

51. In this document, ComReg has adopted the following structure in relation to Step 3 and Step 4:

- first, the impact on industry stakeholders is considered;
- second, the impact on competition; and
- Finally, the impact on consumers.

52. This order does not reflect any assessment of the relative importance of these issues but rather reflects a logical progression. In particular, a measure which

[35] Ministerial Direction dated 21st February 2003
[36] Section 12 (1)(a)(i) of the 2002 Act.
[37] Section 12 (1)(a)(ii) of the 2002 Act.
[38] Section 12(1)(a)(iii) of the 2002 Act.
[39] Section 12(1)(b) of the 2002 Act.
[40] Regulation 16(2)(d) of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011, S.I. No. 333 of 2011 (the "Framework Regulations").

safeguards and promotes competition should, in general, impact positively on consumers. In that regard, the assessment of the impact on consumers draws substantially upon the assessment carried out in respect of the impact on competition.

3.5 Step 1: Identify the policy issues & the objectives

3.5.1 Policy Issues

53. The electronic communications sector plays a vital role in supporting both consumers and businesses to, live, work and communicate. Access to high quality and resilient ECN and ECS are integral to the social and economic fabric of Ireland and even more so since the Covid-19 pandemic, which saw significant changes in how we use ECN and ECS. The prominence of remote working and studying in addition to the rising demand for communicating and consuming digital content on mobile and computing devices; emphasises the importance of correctly functioning ECN and ECS.[41]

54. Users reasonably expect to be able to access the services provided over networks with minimal disruption. However, incidents can occur that adversely affect ECN and ECS, thereby negatively impacting the experience of the end user. Examples of some of the causes of typical incidents include:

- Weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms;
- Third party damage: including, vehicular impact, cable theft; fibre cuts, deep diving submarines, remotely operated vehicles (“ROV”), anchor, cable plough or trawler related, cable damage;
- Malicious acts: theft, Telephony Denial of Service (“TDoS”) incidents, Distributed Denial of Service (“DDoS”) incidents, vandalism, espionage and sabotage;
- Power outages due to weather, insufficient protection of mains supply, no or insufficient back-up power and poor maintenance of back-up power; and

[41] A consumer survey commissioned by ComReg in 2021 revealed that 81% of respondents believe their household usage of broadband increased since March 2020. See ComReg Document 21/42.

- System failures including but not limited to hardware and software failure; insufficient redundancy; poor procedures, particularly 'roll-back' procedures; poor supervision of both own and outsourced staff.[42]

55. ECN and ECS providers are obliged to notify ComReg when an incident arises that has a significant impact on its network or service. Considering the significance of ECN and ECS, it is important that ComReg has in place thresholds that are fit for purpose and ensure that service providers bring significant incidents to its attention. The sections below summarise ComReg's current reporting thresholds and the notable developments that have occurred since.

3.5.2 ComReg's current thresholds for reporting incidents

56. Regulation 23(4)b of the Framework Regulations provides that when ComReg has been notified of a breach of security or loss of integrity that has a significant impact on the operation of electronic communications networks or services, ComReg must in turn inform the Minister for the Environment, Climate and Communications (the "Minister") of such a notification and, with the agreement of the Minister and where appropriate, ComReg shall also inform the NRAs in other MS in addition to ENISA.

57. ComReg's current approach to management of reported incidents and the coordination of its response to these incidents, is set out in Reporting & Guidance on Incident Reporting & Minimum-Security Standards, ComReg Document 14/02. This outlines the appropriate thresholds for reporting incidents and the requisite timing for submission of incident reports. The thresholds and process for reporting are provided as guidance to undertakings providing public communications networks or publicly available electronic communications service. ComReg's approach took into consideration the Framework Regulations[43] and the guidance provided by ENISA at that time in its document Technical Guideline on Reporting Incidents.[44]

58. In Document 14/02, ComReg notes that the thresholds for national incident reporting should be lower than the ENISA thresholds (i.e., more stringent) because:

[42] Software failures, hardware failures and storms were the causes for most of the user hours lost in 2021. See ComReg Document 22/44.
[43] Regulation 23 and Regulation 24 of S.I. No. 333/2011 European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011.
[44] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0

(i) the threshold to trigger an ENISA report by ComReg will be an accumulation of reports from various providers that reflect a single outage that impacts more than one provider; and

(ii) having a lower (i.e., more stringent) threshold has the additional advantage of enabling ComReg to be able to monitor the performance of an operator in respect to the management of appropriate technical and organisational measures to ensure that it manages the risks posed to the integrity and security of networks and services.

59. The current reporting thresholds have proven effective in ensuring that undertakings providing public ECN and ECS complied with the obligations placed on them by Regulation 23 of the Framework Regulations.

3.5.3 The European Electronic Communications Code and its transposition into Irish Law

60. On 20 December 2018, the EECC entered into force and is transposed in the State by the Act, once commenced, and by the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, once commenced. Articles 40 and 41 of the EECC replace Article 13(a) and 13(b) of the Framework Directive (amended)[45] and place a greater emphasis on consumer protection and security of electronic communications.

61. Article 2(21) of the EECC defines security of networks and services as:

"the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services"

62. It should be noted that the new definition of "security of networks and services" contained within the EECC now explicitly includes authenticity, integrity, confidentiality and availability. This has important implications for the scope of a security incident, which is now considerably broader than previously set out by the Framework Directive.[46] Article 2(42) defines a security incident as:

[45] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009

[46] Article 13a (3) specified that undertakings providing communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services (emphasis added)

"an event having an actual adverse effect on the security of electronic communications networks or services."

63. This wider definition has implications as to how ComReg should view security incidents that have adverse effects on the security of public ECS and ECN. For example, Article 40(2) of the EECC, which will be transposed in section 11(1) of the Act states:

(2) A provider shall, where any security incident occurs that has had or is having a significant impact on the operation of the provider's electronic communications networks or services, notify the Commission in accordance with subsection (3) without undue delay.

64. To determine whether the impact of a security incident is significant for the purposes described, section 11(2) of the Act, which transposes relevant provisions of Article 40(2), sets out that where available the following parameters shall be taken into account:

(a) the duration of the incident;

(b) the number of users affected;

(c) any class of users particularly affected;

(d) the geographical area affected;

(e) the extent to which the functioning of the network or service was affected;

(f) the impact of the incident on economic and societal activities;

(g) the cause of the incident and any particular circumstances that resulted in the security incident.

65. Article 40, as will be transposed by sections 11(5) and 11(6) of the Act, sets out that:

(5) Where the Commission is notified of a security incident under subsection (1) it shall—

(a) inform the Minister of the notification, and

(b) where the Commission, having consulted with the Minister, considers it appropriate to do so, notify the competent authorities of other Member States and ENISA.

(6) Where the Commission determines, having consulted with the Minister, that the disclosure of a security incident notified under subsection (1) is in the public interest it may inform the public of the incident or require the provider concerned to do so.

66. Furthermore, ComReg shall submit an annual report to the Minister, the European Commission and ENISA on the notifications received and the actions taken by ComReg.

3.5.4 Thresholds for the reporting of an incident to ENISA by ComReg

67. In March 2021, ENISA published technical guidelines (ENISA Revised Guidelines) on reporting incidents, in light of the obligations contained in the EECC[47]. Specifically, the document provides guidance to NRAs about implementing paragraph 2 of Article 40 of the European Electronic Communications Code ("EECC") for annual summary reporting and the document focuses on when and how to report security incidents to ENISA, the EC and between NRAs.

68. Section 6 of the ENISA Revised Guidelines sets out scope and thresholds for when incidents should be included in annual summary reporting from NRAs to the EC and ENISA. ENISA defines two types of thresholds for NRA's to consider when preparing the summary report and these are detailed below.

a) Quantitative[48] thresholds: Assessing the impact according to quantitative parameters (for example, the number of the users affected and the duration of the incident); and

b) Qualitative thresholds: Assessing the impact according to qualitative parameters (for example, the geographical spread, impact on economy and society and the extent to which the functioning of the network or service is affected).

Quantitative Thresholds

69. ENISA suggests that the quantitative thresholds consist of two parts.

[47] Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu), https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

48 Quantitative means relating to different sizes or amounts of things, https://www.collinsdictionary.com/dictionary/english/quantitative, accessed 18/11/2022.

Relative threshold

70. This is based on the percentage of the national user base that are affected by a security incident. ENISA recommends that NRAs should report incidents which have an impact on service / network **availability**, if the incident:

- lasts more than an hour, and the percentage of users affected is more than 15%;
- lasts more than 2 hours, and the percentage of users affected is more than 10%;
- lasts more than 4 hours, and the percentage of users affected is more than 5%;
- lasts more than 6 hours, and the percentage of users affected is more than 2%; or if it
- lasts more than 8 hours, and the percentage of users affected is more than 1%.

71. ENISA also recommends that NRAs should report incidents which have an impact on the **confidentiality**, **authenticity** and **integrity** using the relative threshold. In such instances, an incident should be included in the annual report if the number of users affected is more than 1% of the national user base of that service.

Absolute Threshold

72. The absolute threshold is the product of the duration and the number of users affected for a particular service. ENISA recommends that this threshold is applied for security incidents which have an impact on **availability**[49] and advises that an incident should be included in the annual summary report if the absolute threshold is greater than or equal to one million (1,000,000) user hours.

Qualitative Thresholds

73. While quantitative thresholds are clear to understand, ENISA is of the view that they may not fully fit every situation where, for example, the number of users or duration are not always the significant factors. As such, ENISA suggests that qualitative thresholds should be considered in tandem with the quantitative thresholds in determining the significance of an incident. Specifically, ENISA suggests that geographical spread and the economic and societal impacts

[49] Defined in Article 2 of the EECC.

associated with a security incident should be considered. ComReg notes that this is in keeping with the information requirements in section 11 of the Act.

Objectives

74. ComReg aims to design and carry out its review of the thresholds for incident reporting in accordance with its broader statutory objectives as above in Section 3.4

75. In addition, the focus of this RIA is to assess the impact of the proposed measure(s) (see regulatory options below) on stakeholders, competition and consumers.

3.6 Step 2: Identify and describe the regulatory options

76. The current thresholds for reporting network security incidents to ComReg have been in place since 2014 and have been effective in ensuring undertakings providing public ECN and ECS comply with their obligations, as set out in Regulation 23 of the Framework Regulations. ComReg will evaluate the existing reporting framework as an option, given its utility to date, and to fully understand the impact of any change from an alternative option. Therefore, ComReg notes that **Option 1 is to maintain the status quo** and extend the use of the existing reporting requirements under Document 14/02. ComReg's approach in Document 14/02 was to set quantitative numeric thresholds based on the number of affected users and the duration of the incident.

77. In relation to other options, ComReg notes that the approach advocated by ENISA is to consider both quantitative and qualitative thresholds to determine whether an incident should be reported to it and the European Commission (i.e., annual summary reporting). The quantitative thresholds are those set out in Section 3.5.1 above ('Quantitative Thresholds'). Therefore, ComReg is of the view that **Option 2** is to align the quantitative thresholds with those in the ENISA guidelines.

78. An alternative option would be to retain the more stringent availability thresholds from Document 14/02 while also including the broader definition of security and a security incident, (i.e., incidents which also have an adverse effect on the authenticity, confidentiality, or integrity of a publicly available ECS or ECN). In short, this option would be the same as Option 2 except that it would retain the more stringent reporting thresholds on availability as currently applied in Document 14/02. However, ComReg notes that these thresholds were set over eight years ago, and the ENISA guidelines have been updated to account for technological developments in the intervening period.

Furthermore, ComReg observes that circa 75% of the incidents reported under Document 14/02 would be captured by the revised ENISA Guidelines in any event.

79. The Guidelines also include some suggestions on how qualitative thresholds could be applied but ultimately leaves much of this to the discretion of each NRA. Regarding the potential inclusion of a qualitative approach, ComReg notes that in its experience, quantitative thresholds have generally proven effective for capturing significant incidents. Furthermore, ComReg observes that most incidents reported have also exceeded the thresholds for inclusion in ComReg's reporting to ENISA.

80. ComReg is therefore of the preliminary view that an approach which uses defined quantitative values for providers to report incidents is effective and provides clarity to providers. Consequently, ComReg does not propose to include qualitative approaches at this time, although it may revisit this matter in the future. Further, ComReg notes that any approach does not preclude providers from voluntarily reporting incidents to ComReg should they be of importance. ComReg notes that providers have in the past freely reported incidents to ComReg that while falling below the thresholds, were considered by the operator to be of sufficient interest.

81. Considering the above, ComReg is of the view that the policy options available to it are:

Option 1: Set thresholds that match those prescribed in Document 14/02.

Option 2: Set thresholds that match those in Section 6.2.2 of the ENISA Revised Guidelines.

3.7 Impact on Stakeholders

Identification of stakeholders

82. Step 3 assesses the likely impact of the proposed regulatory measures on stakeholders. Hence a necessary precursor is to identify such stakeholders who, in this RIA, fall into two main groups:

(i) industry stakeholders (providers of public ECN and publicly available ECS); and

(ii) competition and consumers.

83. ComReg sets out below a comparative analysis of each of the two options outlined above, in terms of their impact on stakeholders, competition and consumers.

Impact on industry stakeholders

84. The reporting requirements and the associated impacts on industry stakeholders (providers) vary across both Options. Under Option 1 providers would have the same reporting requirements, as have been in place over the previous eight years. Under this Option, no additional reporting requirements are being placed on providers.

85. Under Option 1 providers are already complying with reporting thresholds above these levels (i.e., the reporting requirements outlined in Document 14/02 on the **availability of networks**[50] are more strict than proposed by ENISA's Revised Guidelines) and there are unlikely to be any impacts associated with complying with the Revised Guidelines (as it relates to availability) under this reporting requirement category. Further, there are no reporting requirements in relation to **confidentiality, authenticity and integrity** of networks. Therefore, providers are unlikely to have concerns with the impacts associated with Option 1 as it continues with the existing reporting requirement, (noting that respondents to Section 4.2 of Document 14/02 were broadly in favour of the thresholds at the time).

86. Under Option 2, providers would have a lower reporting requirement in terms of the **availability** of networks.. However, Option 2 includes additional reporting obligations related to the relative threshold for a security incident, which have an **impact on the confidentiality, authenticity, and integrity** of networks. Definitions of Confidentiality, Integrity, Authenticity and Availability[51] are provided in Chapter 4.2 of this document and providers should report these incidents, if the number of users affected is more than 1% of the national user base of that particular service.

87. However, in such cases, it is likely that additional spending for monitoring and reporting could be relatively small because providers are already likely to be monitoring these aspects of their networks (and voluntarily reporting incidents) and Option 2 simply adds a reporting requirement to same. More generally, the reduced reporting requirement under the availability of networks increases scope for increased reporting on **confidentiality, authenticity and integrity** of networks. ComReg is of the preliminary view that providers are likely to be relatively neutral in terms of Option 2.

[50] These threshold requirements are comparable to the quantitative thresholds in ENISA Guidelines and for aid of comparison will be referred to as thresholds relating to **the availability of networks** for the remainder of this document.

[51] And as defined in Article 2 of the EECC.

Impact on competition

88. ComReg's statutory obligations in relation to competition are set out in accordance with section 12 of the 2002 Act. Given the issues discussed in this consultation, of particular relevance is the requirement to safeguard competition to the benefit of consumers and promoting, where appropriate, infrastructure-based competition. However, prior to setting out which option is best likely to best promote competition and particularly infrastructure-based competition, it is useful to first outline the reasons why incident reporting is beneficial (in and of itself) and consequently to promoting competition.

89. ECN and ECS are fundamental platforms for the delivery of economic and societal welfare. As dependence on these networks increases; the impact of network incidents can be felt right across society. The move towards increased remote working, alongside the growing use of upstream digital applications by both consumers and businesses leads to further "locking in" of the dependence on telecommunications networks, thereby magnifying the impact of network failures. The increasing reliance on connectivity (mobile and fixed) and the ever-increasing importance of the internet in delivering all manner of goods and services, prompts concerns about the consequences of network failures.

90. There is a need therefore to establish appropriate policy and regulatory frameworks that can help ensure that networks are provided and operated in a way that meets the needs of the State. With that in mind, the current EU Telecoms Framework, but also the EECC, require providers of networks and services to take appropriate technical and organisational measures to manage the risk posed to security of ECN and ECS. Incident reporting plays an important role in these efforts, as it contributes to improving both providers' and NRAs' knowledge of the *type* of network incidents.

91. An effective incident reporting system also contributes to the collection of reliable and up-to-date data on security incidents. It facilitates the rapid dissemination of information among interested parties, thereby allowing a coordinated response. This permits the NRA to follow up with the providers' infrastructure managers and in a regulatory capacity for the identification of good practices and processes. An incident reporting scheme provides valuable transparency to society and allows learning from incidents, in order to systematically improve the security and operation of ECN and ECS in the electronic communications sector.

92. There are some underlying reasons as to why network reliability may be underprovided by competition between network providers. These will be outlined in detail in ComReg's upcoming assessment of "*Economic and*

societal impacts of Network Incidents", which ComReg expects to publish in in Q2 2023 and ComReg will update this RIA, once this assessment is completed.

93. Notwithstanding, one such reason is that the cause of network incidents is typically unclear and can often be disputed across different entities. Therefore, it may be difficult on occasion to determine whether network incidents are due to some under-provisioning of network infrastructure by providers or due to unforeseen external effects (e.g., weather, technical failures).

94. For example, problems arising from unclear attribution of responsibility for faults (and consequent poor incentives to provide reliability) can arise in many industries with vertical supply chains. Some incidents may occur across all providers and may be difficult to prevent (e.g., extreme weather). However, experience shows that others are often network specific and arise perhaps to some degree because of poor incentives to provide reliability and the inefficient provision of network infrastructure (e.g., software upgrades/overextending asset life). Network incident reporting increases transparency and can thus encourage providers to avoid the inefficient delivery of networks, subsequently improving infrastructure-based competition. Incident reporting is one part, but an important part, of a larger effort to handle incidents and emergencies, and to protect network infrastructure.

95. Of course, the option that best promotes competition is not necessarily that with the highest reporting thresholds but rather one that strikes an appropriate balance between:

- swift reporting that draws valuable lessons from individual incidents improving the resilience of networks, helping mitigate the potential spread of incidents; and

- creating an effective reporting regime that does not place an undue burden on providers.

96. Option 1 already provides a level of incident reporting in relation to the availability of networks. However, such incident reporting is limited to network availability; but there is no requirement in relation to other important aspects of the network, such as confidentiality, authenticity and integrity. While network availability is integral to the provision of connectivity; confidentiality, authenticity, and integrity of networks are also very important, given the provision of 5G services in an ever-connected society. A reporting requirement in relation to confidentiality, authenticity, and integrity would better encourage infrastructure-based competition compared to Option 1, as it provides better incentives for operators to ensure that their networks are dimensioned to

account for factors other than availability. However, under Option 1, operators would not be required to report incidents that relate to confidentiality, authenticity, and integrity and could lead to under provisioning of such factors.

97. Therefore, ComReg is of the preliminary view that Option 2 promotes competition better than Option 1.

Impact on consumers

98. Effectively functioning ECN and ECS are of increasing importance as society continues to become more digitally connected. Users heavily rely on ECN and ECS to carry out a wide range of day to day tasks, be that communicating, internet browsing, studying, streaming, gaming, shopping and for work.

99. The changing work pattern, unquestionably accelerated by the Covid-19 pandemic, has seen many workplaces adopt a hybrid or full remote working approach, which in turn has placed much greater importance on household broadband connection for work.[52] Consequently, a security incident that impacts an ECN or ECS, could have a significant economic and societal impact for users, society and business at large. For example, market research carried out as part of ComReg's forthcoming report on the economic and societal impacts of network incidents reveals that, of the respondents who reported experiencing network outages, approximately a quarter indicated that remote working was affected.[53] However, given the change to how security is now defined, it follows that what will form a security incident is today far broader, and so further incidents will fall within the scope of national reporting. Consumers would likely prefer an option that requires providers to notify ComReg of most incidents, including those that relate to confidentiality, authenticity, integrity and availability, thereby giving ComReg greater visibility of network security.

100. A wide variety of ordinary everyday tasks are conducted remotely (for example, working, banking and online shopping) and consumers require, among other things, that transmitted information is not made available or disclosed to unauthorised individuals, entities, or processes. A survey published by ComReg in 2021 revealed that consumers consider the security and privacy of personal data to be the biggest challenge when online.[54] These reporting requirements are provided for under Option 2 but not under Option 1

[52] For example, a 2022 survey found that 52% of workers were currently working hybrid and 40% fully remotely. See 2022 National Remote Working Survey - Whitaker Institute for Innovation and Societal Change | NUI Galway
[53] ComReg expects to pubish the report in Q2 2023
[54] See ComReg Document 21/09

and therefore, ComReg is of the preliminary view that consumers would prefer Option 2.

3.8 ComReg's preferred option

101. This draft RIA considers two regulatory measures available to ComReg within the context of the analytical framework set out in ComReg's RIA Guidelines (i.e., impact on industry stakeholders, impact on competition and impact on consumers).

102. Considering the above, ComReg is of the preliminary view that Option 2 is preferred in terms of impact on stakeholders, competition and consumers.

4 Incident Thresholds & Reporting

4.1 Incident reporting

103. Building on the Draft RIA in Chapter 3, this chapter addresses the adoption of the thresholds from the ENISA Revised Guidelines and how they might be implemented in Ireland so that ComReg can meet its statutory obligations under the new legislative framework.

104. ComReg also notes that such an approach is largely reflected in Part 2 of the Act, sections 5 to 18 (inclusive), which address security of networks and services.

4.2 Changes to Incident Reporting

4.2.1 Incident Types and Services Covered Pursuant to the Act

Change to the Definition of Security Incident

105. Unlike the Framework Regulations, where security and integrity are not explicitly defined terms, the EECC usefully defines both:

- '*security of networks and services*' means '*the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or service*'[55]; and

- Where a '*security incident*' means '*any action that compromises the availability, authenticity, integrity or confidentiality of networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services*'[56].

106. Currently, when reporting an incident, operators typically indicate whether the availability and/or the integrity of the ECN and/or ECS provided was compromised. Because of the Act, in addition to reporting on whether the availability and integrity of the ECN and/or ECS provided is compromised, operators must also consider

[55] Article 2(21) of the EECC, as transposed in section 5 of the Act.
[56] Section 5 of the Act.

and report on whether a security incident has compromised the ECN and/or ECS provided under the following categories:

- **Confidentiality**[57] means, the confidentiality of communications, communications data or metadata has been compromised. For example, but not limited to, the encryption on a service does not work or has been compromised and unauthorised access takes place with the communications being forwarded to unauthorised parties;

- **Integrity** [58] means, the integrity of the communications data or metadata has been compromised. For example, but not limited to, the IP address and caller id have been tampered with routing the communications to a third party or unauthorised software has been installed on a server;

- **Authenticity** [59]; when there is a compromise of user's identity (identity fraud). For example, man-in-the-middle attacks or eavesdropping on applications lead to theft and misuse of authentication credentials, user accounts become accessible and taken over by attackers;

- **Availability**[60] ; when the incident affects the continuity of supply of services, degrades the performance of the service, the network or service is "completely" or "partially" down. This is often called 'outage' or 'disruption'.

107. Further to section 11(5) of the Act, where ComReg is notified of a security incident under section 11(1), it shall:

a) inform the Minister of the notification; and

b) having consulted with the Minister, and where ComReg considers it appropriate to do so, notify the competent authorities of other Member States and ENISA.

108. ComReg notes that further to section 16(1) of the Act, ComReg may, for the purposes of exercising its functions under Part 2, consult, cooperate, share information with, or obtain the assistance of a number of bodies, including: the

[57] Confidentiality is typically defined as a property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 7).
[58] Integrity is typically defined as a property of accuracy and completeness (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 8).
[59] Authenticity is typically defined as a property that an entity is what it claims to be (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 9).
[60] Availability is typically defined as a property of being accessible and usable on demand by an authorized entity (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 6).

Computer Security Incident Response Team ("CSIRT") of Ireland; a CSIRT in another Member State; or a NRA in another MS.

Number Independent-Interpersonal Communications Services ("NI-ICS")

109. NI-ICS are as defined in Regulation 2 of the Regulations of 2022[61], and are now included in the revised definition of ECS, as set out in Regulation 2 of the Regulations of 2022[62].

110. Consequentially, pursuant to the revised definition of ECS in the Regulations that transpose the EECC, security incidents that affect NI-ICS now fall within scope of notification. Therefore, the reporting process proposed in this consultation would apply to NI-ICS if adopted.

4.2.2 Categorisation of Incidents, Reporting Thresholds and Information Required

Incident Categorisation

111. When reporting an incident, providers should categorise so that it is clear as to whether the incident has compromised the confidentiality, integrity, authenticity or availability of the ECN and/or ECS affected by the incident[63].

Incident Reporting Thresholds:

112. In the main, the proposed incident reporting thresholds are similar to those contained in Document 14/02, comprising of the percentage of the national user base[64] of the service impacted and the duration of the incident. These are shown in figure 1 below.

113. The exception to this arises from the introduction of an absolute threshold: that is any incident, affecting availability, greater than or equal to one million (1,000,000) User Hours[65], must now be reported; and

providers will also need to report any incident impacting 1% or more of the National User Base and which affects the confidentiality, integrity or authenticity of that service[66].

[61] Which transposes (amongst other things) Article 2(7) of the EECC.
[62] Which transposes (amongst other things) Article 2(4) of the EECC.
[63] As per the definitions contained in paragraph 106 above.
[64] See Chapter 4.2.3.
[65] User Hours is the product of the Number of Users affected and the Duration of the incident.
[66] See paragraph 106 for the relevant definitions of these incident categories.

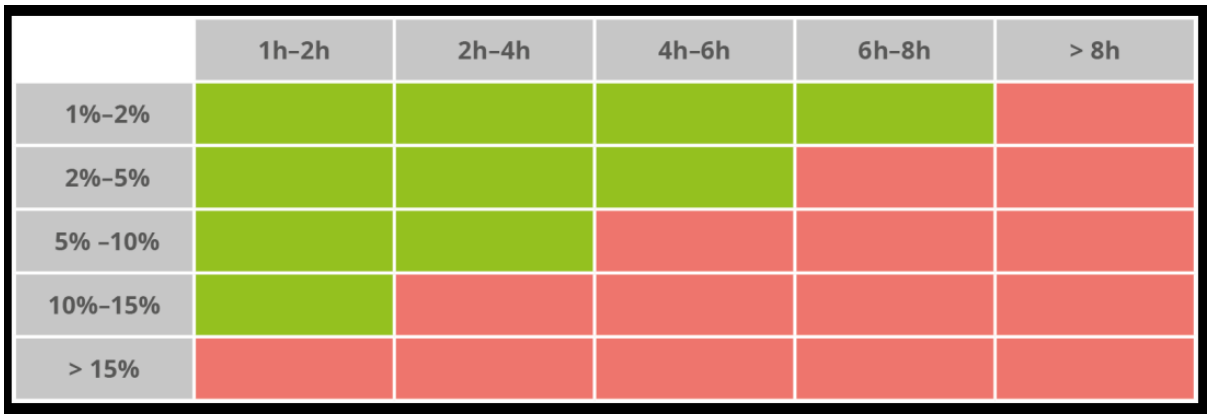

Figure 1: Thresholds, based on National User Base and Incident Duration[67]

Further Information Required

114. The following further information, pursuant to section 11(2) (c), (d) and (f) of the Act, will also now be required:

- The geographical area affected: whole country; province; county or Island;
- Where there is cross border impact affecting another MS or relevant third country;
- Any particular class of users[68] affected; or
- Where there is a severe impact on economic and societal activities.[69]

4.2.3 National User Base Calculations

115. As recommended by the ENISA Revised Guidelines, the thresholds required for a significant incident are derived from national user base for the impacted service. ComReg publishes figures in the Quarterly Key Data Report ("QKDR") found on ComReg's webpage[70], which providers should reference to determine the percentage number of users for each service associated with any outage:

(a) For fixed voice communications service and fixed internet[71] access, providers should use the separate values outlined in the report.

[67] Page 21 TECHNICAL GUIDELINE ON INCIDENT REPORTING UNDER THE EECC.
[68] "User" means a natural or legal person using or requesting a publicly available electronic communications service; see Regulation 2(1) of the European Union (Electronic Communications Code Regulations) 2022, S.I. No. 444 of 2022.
[69] ComReg expects to publish a report on this in Q2 2023.
[70] Quarterly Key Data Report | Commission for Communications Regulation (comreg.ie).
[71] Including all data such as broadband access.

(b) For mobile communications service, providers should use the number of active telephony Subscriber Identity Module ("SIM") cards based on the number of

- Voice Subscriptions; and
- Machine to Machine Subscriptions.

(c) For mobile internet[72] access, providers should combine:

- The number of standard mobile subscriptions, which offer both voice service and internet access; and
- The number of subscriptions dedicated for mobile internet access[73].

- For NI-ICS, providers may sum the number of active users, within the State, of the services in the end of a period. These could be measured as the active users ("MAU"), where an 'active user' can, for example, be defined as the user who has used the service at least once in the respective period[74].

116. Noting that **all security incidents are reportable to ComReg once the absolute threshold of one million (1,000,000) User Hours** has been equalled or exceeded or any incident impacting 1% or more of the National User Base and affects the confidentiality, integrity or authenticity of that service.

Q. 1	Do you support the proposed thresholds, further information requirements and incident typification outlined in this document? If not, please provide a well-supported, justified and evidenced-based explanation for your view.

4.3 Reporting Process

117. As outlined, ComReg has included draft Decision at Annex 2 as part of this consultation. It is intended that following the consultation process this will be published as a standalone document. It will set out the thresholds by ComReg for triggering an incident report, in line with the ENISA Revised Guidelines, and the reporting timelines to be met by providers.

118. The reporting process enables ComReg to monitor the compliance by a provider with its obligations. ComReg requires that information is provided in a

[72] Including all data such as broadband access.
[73] I.e., those using a dongle or similar device.
[74] Refer to Pg 21 Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu)

timely manner to, among other things, enable consumer awareness where incidents have a significant impact. Timelines are informed by the seriousness of the incident and its impact.

119. ComReg is mindful of facilitating consistent incident reporting standards and intends to further align these standards with the ENISA Revised Guidelines principles. Providers will appreciate that there will however be some exceptions, such as incidents that require urgent attention, for example in the case of storms, complete network failure or failure of the networks in a particular geographic area.

4.3.1 Reporting Incidents to ComReg

120. Any provider, considered as providing public communications networks or publicly available electronic communications services, must notify ComReg in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services, once such a breach meets with the prescribed thresholds. In meeting this obligation, providers must use ComReg's e-licensing incident reporting portal, the process for which is detailed in the "*User Guide for ComReg's Network Incident Reporting portal*".[75]

4.3.2 Information Requirements for an Incident Report

121. Taking into account the matters mentioned in section 11(2) of the Act, and the statutory information requirements mentioned in section 11(3) of the Act, ComReg will require providers to provide the following information in an Incident Report:

- The category of incident, that is whether it is: Confidentiality, Integrity, Authenticity or Availability that is affected by the incident, as per the definitions contained in paragraph 106 above;
- the providers' name;
- the public electronic communications network or publicly available electronic communications services provided by it affected by the incident;
- the date and time the incident occurred and its duration;
- the number of users affected;
- any class of users particularly affected;
- the geographical area affected;

[75] https://www.comreg.ie/?dlm_download=user-guide-for-comregs-network-incident-reporting-portal

- the extent to which the functioning of the network or service was affected;
- the impact of the incident on economic and societal activities;
- the cause of the incident and any particular circumstances that resulted in the security incident.
- information concerning any or any likely cross-border impact with another MS; and
- such other information as the Commission may specify.

122. ComReg will facilitate a common reporting format which contains the information required by: ComReg, ENISA and the European Commission. The proposed format and thresholds for reporting incidents are contained in the Draft Decision which will be maintained and updated from time to time as circumstances require.

123. Note, that while ComReg operates between 09H00 and 17H30 and does not operate a 24Hour or 'on-call' type service, all reports in or out of hours should be made through the incident reporting portal without delay.

4.3.3 Timings for Incident Reporting

124. Where a security incident has a significant impact on the operation of an ECN or ECS, as defined in this Chapter, a provider must report to ComReg as soon as possible and within the first 24 hours of the initial incident.

- In relation to the urgency of the incident report, providers should consider the following:
    - Where the incident affects greater than 15% of the national user base for that service, and:
    - has a high probability of deteriorating further;
    - significantly affects another provider's network;
    - affects networks or services in another MS or appropriate third party country; or
    - has a high likelihood of national media coverage.

125. ComReg advocates that providers should report the incident as soon as possible. Providers can follow up subsequently with further updates to the incident

report as further facts emerge. This enables ComReg, in conjunction with the provider, as appropriate, to manage any enquiries accurately and effectively.

126. Initial reports should contain all the information available at the time the incident report is made. This should include as a minimum[76]:

- The category of incident, that is whether either the confidentiality, integrity, authenticity or availability of an ECN and/or ECS has been compromised by the incident, as per the definitions contained in paragraph 106 above;
- details of the number of the user base impacted;
- the service impacted;
- an indication of the likely cause; and
- if possible, the expected duration of the incident.

127. If the incident is not resolved within 72 hours, the provider must supply an update to the existing report, detailing the incident's impact and the action plan to resolve it.

128. Upon the resolution of the incident, ComReg must receive notification via the e-licensing incident reporting portal advising that the incident has been resolved and that services have been restored.

129. For any incident, ComReg must receive a comprehensive update within four weeks of the incident to the initial incident report that confirms the circumstances of the incident:

- The duration of the incident, if different from the previous updates,
- The communication services impacted, along with the number of users impacted for each service, if different from the previous updates,
- a Root Cause Analysis report for the incident which at a minimum is to include the:

  (a) root cause summary statement for reported incident;

  (b) event timeline which details the sequence of contributing events leading to the incident;

  (c) description of impact to network infrastructure;

[76] See section 11(2) of the Act.

(d) remedial timeline which details the sequence of actions taken to resolve the incident;

(e) categorisation[77] of incident root cause, including a justification for its categorisation;

(f) mitigation measures identified to prevent future occurrence of any similar incidents; and

(g) timeline for implementation of identified mitigation measures.

130. Once ComReg is fully satisfied the incident report will be closed.

4.3.4 Exception: Storm Reporting

131. Notwithstanding the reporting timeframes outlined at section 4.3.3 above, the following exceptional incident type requires the following notification timescales.

132. Storm Reporting: when Met Éireann declares a named storm or when Met Éireann issues an orange or a red-level weather warning, ComReg will notify the providers registered on the e-licensing incident reporting portal with further details and the required reporting template or method.

- The timing for reporting the effect on the providers' ECN or ECS to ComReg will be at 10H00 and 16H00;
- Such reports will continue, until providers notify ComReg that Networks and Services are operating on a Business as Usual ("BAU") basis; and
- ComReg will act as a single point of contact between providers, DECC and the National Emergency Coordination Group (the "NECG"), the role of which is to coordinate and manage the national-level response to an emergency, on a "whole of government", cross-sector basis.

Q. 2	Do you agree with the proposed timelines and processes for reporting incidents outlined in this, and the draft Decision, document? If not, please provide a well-supported, justified and evidenced-based explanation for your view.

[77] The root cause of an incident can be categorised into one of five categories; 1. Human errors; 2. System failures; 3. Natural phenomena; 4. Malicious actions; 5. Third party failures. For further information on this categorisation please refer to Part 2 of ENISA Technical Guideline on Incident Reporting under the EECC

4.3.5 Information Required by the Minister, European Commission, Other NRAs and ENISA.

133. Further to section 11(5) of the Act, and where ComReg is notified of a security incident under section 11(1), it shall (a) inform the Minister of the notification, and (b) having consulted with the Minister, and where ComReg considers it appropriate to do so, notify the competent authorities of other Member States and ENISA. ComReg considers that the circumstances under which it would be appropriate to inform other NRAs or ENISA under this provision are likely to involve incidents with cross border significance.

134. ComReg notes that further to section 16(1) of the Act, it may, for the purposes of exercising its functions under Part 2, consult, cooperate, share information with, or obtain the assistance of several bodies, including the Computer Security Incident Response Team ("CSIRT"), a CSIRT in another Member State, or a national regulatory authority in another Member State. Further to, section 11(6) of the Act, where ComReg determines, having consulted with the Minister, that the disclosure of a security incident notified under section 11(1) is in the public interest, it may inform the public of the incident, or require the provider concerned to do so.

135. ComReg anticipates that reporting to ENISA and to the European Commission will, in the main, be via the annual reporting under section 11(9) of the Act. Further to section 11(9) of the Act, ComReg shall in each year submit a summary report to the Minister, the European Commission and ENISA on the notifications received and the actions it has taken in accordance with section 11. Furthermore, when ComReg is notified of a significant incident, as per the thresholds set out in the thresholds document, it will notify the Minister as required under section 11(5)(a) of the Act.

4.3.6 Confidentiality of Submitted Information

136. ComReg shall, subject to the Freedom of Information Acts 1997 and 2003, accept as confidential any information provided to it which is expressed to be confidential, except where the Regulator has good reason to consider otherwise.

137. Such Information will be treated subject to the provisions of ComReg's guidelines on the treatment of confidential information, currently set out in ComReg Document No. 05/24[78]

[78] https://www.comreg.ie/publication/response-to-consultation-guidelines-on-the-treatment-of-confidential-information

138. Confidential information that is furnished by a provider will be dealt with in a confidential manner and ComReg will request that ENISA also treats any such information confidentially.

139. ENISA has outlined how it will handle information that has been classified as confidential by ComReg, or other NRAs, and the provider. Article 5(3) of Directive 2002/2110 states "*Where information is considered confidential by a national regulatory authority in accordance with Community and national rules on business confidentiality, the Commission and the national regulatory authorities concerned shall ensure such confidentiality.*"[79]

140. For Information that will be exchanged with Government departments, agencies and the European Commission, ComReg is currently guided by Article 3(5) of the Framework Directive. In respect of the information exchanged, the receiving authority is to ensure the same level of confidentiality as the originating authority. It is expected that this will continue under section 16(5) of the Act.

[79] Where an incident affects many end users or an important institution, the incident itself is unlikely to be classified as confidential, whereas information relating to aspects of the incident and associated report may be considered as confidential.

5 Implementation & Enforcement

Implementation

141. Article 41 of the EECC and Part 2 of the Act once commenced, offers ComReg several options by which to monitor providers compliance. These include:

- requiring incident reports from providers, as detailed both in Chapter 4 of this document and in the Draft Decision;
- monitoring of incidents by further investigating these reports, for clarification or further details when necessary; and
- audits.

142. ComReg intends to use reporting from providers as one of the main tools for monitoring compliance by providers with their obligations. As detailed in Chapter 4 of this document, it is ComReg's view that in most cases the incident reporting thresholds detailed in the ENISA Revised Guidelines are appropriate for this monitoring, subject to the alterations outlined in Chapter 4.

Enforcement

143. ComReg is cognisant of its statutory obligations under section 13 of the Act and will adopt a proportionate approach to enforcement.

144. ComReg's view is that monitoring compliance with section 15 of the Act, will be a lower burden on providers than regular inspections or audits. However, such inspections or audits may be undertaken by ComReg where appropriate and this may lead to enforcement actions pursuant to any breaches of compliance with section 11 of the Act.

145. While ComReg considers the risk of under reporting is low, as significant incidents will be in the public domain, failure by a provider to report under the Thresholds and Timescales set out in Chapter 4 of this document may require further investigation.

146. ComReg may on occasion commence investigations resulting from complaints received or disputes brought by providers or as described above, by its own initiative, for example:

- information arises that would lead ComReg to believe that network integrity had been compromised; and/or
- a series of consumer complaints are made involving a high number of users complaining over a short of period.

147. Under section 14(3)(c) of the Act, ComReg may serve security measures directions on providers to provide information necessary to assess the security of the services and networks of that provider, including documented security policies. Additionally, and in accordance with section 14(3)(d) a provider may be required to submit to a security audit that would be carried out by a qualified independent person nominated by ComReg, the results of which would be available to ComReg and the Minister. The cost of such an audit would be borne by the provider.

148. Section 14 of the Act permits ComReg to issue security measures directions on providers to ensure compliance with Part 2 (“Security of Networks and Services”) of the Act.

149. Without prejudice to the circumstances under which ComReg may consider requiring an audit be undertaken under section 14 of the Act, ComReg is likely to issue a security measures direction to a provider where it believes there is a lack of compliance with section 15 of the Act. This direction may state how in ComReg’s view, the provider concerned can remedy the situation.

150. A provider that fails to comply with a security measures direction under section 14 of the Act commits an offence as per section 14(7) of the Act.

6 Submitting comments and Next Steps

151. ComReg is publishing this Consultation and Guidance to inform providers about ComReg's expectations as to how providers will fulfil the requirements of the relevant provisions of Article 40 & 41 of the EECC, specifically those relating to the reporting of incidents and the integrity of networks and services.

Submitting Comments

152. All input and comments are welcome. Please reference comments to the relevant chapter / paragraph number in each chapter and annex in this document, as this will assist the task of analysing responses and ensuring that all relevant views are considered.

153. Please also provide reasoning and supporting information for any views expressed.

154. ComReg invites views from interested parties on all aspects of the Consultation over the next four (4) weeks.

155. The four-week **period for comment will run until 12:00 on 25 May 2023**, during which time ComReg welcomes **submissions in written form (e-mail) to marketframeworkconsult@comreg.ie**, clearly marked – **Submissions to ComReg Document 23/36**.

156. Electronic submissions should be submitted in an unprotected format so that they may be readily included in the ComReg submissions document for electronic publication.

157. ComReg appreciates that respondents may wish to provide confidential information if their comments are to be meaningful. In order to promote openness and transparency, ComReg will publish all respondents' submissions to this notice, as well as all substantive correspondence on matters relating to this document, subject to the provisions of ComReg's guidelines on the treatment of confidential information (Document 05/24)[80].

158. In this regard, respondents should submit views in accordance with the instructions set out below. When submitting a response to this notification that

[80] See https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg_1134.pdf Response to consultation and further consultation ComReg 22/56

contains confidential information, respondents must choose one of the following options:

a) Submit both a non-confidential version and a confidential version of the response. The confidential version must have all confidential information clearly marked and highlighted in accordance with the instruction set out below. The separate non-confidential version must have actually redacted all items that were marked and highlighted in the confidential version. OR

b) Submit only a confidential version and ComReg will perform the required redaction to create a non-confidential version for publication. With this option, respondents must ensure that confidential information has been marked and highlighted in accordance with the instructions set out below. Where confidential information has not been marked as per our instructions below, then ComReg will not create the non-confidential redacted version and the respondent will have to provide the redacted non-confidential version in with option A above.

159. For ComReg to perform the redactions under Option B above, respondents must mark and highlight all confidential information in their submission as follows:

a) Confidential information contained within a paragraph must be highlighted with a chosen colour;

b) Square brackets must be included around the confidential text (one at the start and one at the end of the relevant highlighted confidential information); and

c) A Scissors symbol (Symbol code: Wingdings 2:38) must be included after the first square bracket.

For example, “Redtelecom has a market share of [∀25%].”

Next Steps

160. Following the enactment of the Act, ComReg will conclude its review of all submissions received and other relevant material. ComReg’s intention would be to publish a response to consultation with the Final Decision Document.

161. While ComReg cannot provide further clarity on the overall timelines at this juncture, as this will depend, among other things, on the nature of responses received to this consultation and the enactment of the Act, ComReg hopes to issue the above by Q4 2023.

Annex: 1 Legal Basis

162. ComReg has been guided by its primary statutory objectives which it is obliged to seek to achieve when exercising its functions. ComReg's statutory objectives include to:

- promote competition[81];
- contribute to the development of the internal market[82];
- promote the interests of users within the Community[83];
- ensure the efficient management and use of the radio frequency spectrum in Ireland in accordance with a direction under Section 13 of the 2002 Act[84]; and
- promote efficient investment and innovation in new and enhanced infrastructures[85].

163. Directive 2018/1972, also known as the European Electronic Communications Code (the "EECC"), was adopted (by the European Parliament and the Council) through the European Union's ("EU") Ordinary Legislative Procedure on 11 December 2018.10 It entered into force on the third day following its publication in the Official Journal of the EU ("OJEU") (20 December 2018).

164. Article 40(2) of the EECC provides inter alia that: "Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services."

165. Article 40(2) of the EECC also sets out in detail the relevant parameters to judge the significance of the impact of a notifiable security incident, such as the numbers of users affected, the duration of the breach, the geographical area of the breach, and the extent to which the functioning of the service is disrupted. This detailed list of parameters is new compared to the existing notification requirements set out in

[81] Section 12 (1)(a)(i) of the 2002 Act.

[82] Section 12 (1)(a)(ii) of the 2002 Act.

[83] Section 12(1)(a)(iii) of the 2002 Act.

[84] Section 12(1)(b) of the 2002 Act.

[85] Regulation 16(2)(d) of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011, S.I. No. 333 of 2011 (the "Framework Regulations").

Regulation 23 of the Framework Regulations, which transposed Article 13a of the Framework Directive[86].

166. A further new element of the security provisions of the EECC is that the notification requirement now applies to NI-ICS. It should be noted that the Article 40(2) notification requirement applies to publicly available electronic communications services, and Article 2 of the EECC defines electronic communications service, of which interpersonal communications service is one type of ECS.

167. Article 41 of the EECC requires Member States to ensure that their competent authorities are empowered to do the following:

- Issue binding instructions to providers, including instructions on measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time limits for implementation (Article 41(1),
- Require providers to provide information needed to assess the security of their networks and services (including documented security policies) and, at their cost, submit to a security audit carried out by either a qualified independent body or the competent authority and submit same to the competent authority (Article 41(2)).
- Have all powers necessary to investigate cases of non-compliance and the effects of such on the security of the networks and services (Article 41(3)).
- Obtain the assistance of the CSIRT designated under Article 9 of Directive (EU) 2016/1148 on issues falling within the tasks of CSIRTs under that Directive (Article 41(4)).

168. Article 2(7) of the EECC defines "number-independent interpersonal communications service" as meaning "an interpersonal communications service[87] which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans".

169. Recital 95 of the EECC states the following in relation to NI-ICS and security: "Given the growing importance of number-independent interpersonal

[86] Directive 2002/21/EC as amended by Directive 2009/140
[87] For background on how the EECC treats interpersonal communication services generally, Recital 18 is useful.

communications services, it is necessary to ensure that they are also subject to appropriate security requirements in accordance with their specific nature and economic importance. Providers of such services should thus also ensure a level of security appropriate to the risk posed. Given that providers of number-independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. Therefore, where justified on the basis of the actual assessment of the security risks involved, the measures taken by providers of number-independent interpersonal communications services should be lighter. The same approach should apply mutatis mutandis to interpersonal communications services which make use of numbers and which do not exercise actual control over signal transmission."

170. Articles 40 and 41 of the EECC are transposed in Part 2 ("Security of Networks and Services") of the Act, when commenced. Further to section 11(1), a provider shall, where any security incident occurs that has had or is having a significant impact on the operation of the provider's electronic communications networks or services, notify ComReg in accordance with section 11(3) without delay.

171. Section 11(2) provides that in order to determine whether the impact of a security incident is significant for the purposes of subsection (1) a provider shall have regard to the following matters in respect of the incident: (a) the duration of the incident; (b) the number of users affected; (c) any class of users particularly affected; (d) the geographical area affected; (e) the extent to which the functioning of the network or service was affected; (f) the impact of the incident on economic and societal activities; (g) the cause of the incident and any particular circumstances that resulted in the security incident

172. Section 11(3) of the Act sets out the information that a provider has to give to ComReg in a security incident notification. A notification made under subsection 11(1) shall contain the following information in relation to the incident: (a) the provider's name; (b) the public electronic communications network or publicly available electronic communications services provided by it affected by the incident; (c) the date and time the incident occurred and its duration; (d) the information specified in paragraphs (a) to (g) of subsection (2); (e) information concerning the nature and impact of the incident; (f) information concerning any or any likely cross-border impact; (g) such other information as the Commission may specify.

173. Under section 11(4), where a provider notifies ComReg of a security incident, it shall, as soon as practicable, notify ComReg when the incident is resolved and

of the actions taken by it to remedy the incident and, where applicable, any actions taken to reduce the likelihood of a similar incident occurring in the future.

174. Further to section 11(5), of the Act, where ComReg is notified of a security incident, it shall (a) inform the Minister of the notification, and (b) where ComReg, having consulted with the Minister, considers it appropriate to do so, notify the competent authorities of other Member States and ENISA. Further to section 11(6), where ComReg determines, having consulted with the Minister, that the disclosure of a security incident is in the public interest, it may inform the public of the incident or require the provider concerned to do so.

175. Further to section 11(9), ComReg shall in each year submit a summary report to the Minister, the European Commission and ENISA on the security notifications received and the actions taken by ComReg in accordance with section 11.

176. It should be noted that further to section 11(8) of the Act, a provider who (a) fails to notify ComReg of a security incident further to section 11(1), or (b) fails to make all reasonable efforts to provide the information referred to in section 11(3), or (c) fails to inform the public of a security incident where required to do so under section 11(6), commits an offence and is liable on summary conviction to a class A fine.

Annex 2: Draft Decision Document Replacement of Comreg Document No. 14/02 –draft Decision Instrument

Decision

This chapter sets out ComReg's draft Decision Instrument based on the views expressed by ComReg in the preceding chapters and their supporting Annexes.

Please note: The 2023 Act and the 2022 Regulations made by the Minister for Communications for the purpose of transposing the European Electronic Communications Code, namely the Communications Regulation and Digital Hub Agency (Amendment) Act 2023, and *the European Union (Electronic Communications Code) Regulations 2022, SI No. 444 of 2022, have yet, at the time of publication of this Consultation, to be commenced and the legal basis for this replacement of Document 14/02 is accordingly the suite of regulations made in 2011 including in particular the Framework Regulations and the Access Regulations. Were the Electronic Communications Code Regulations to be commenced prior to the adoption of ComReg's final decision, ComReg will adopt its final decision including this Decision Instrument referring to the relevant Regulations as appropriate. For the purpose of this Consultation, references to both the 2011 set of Regulations and to the Electronic Communications Code Regulations have been included where relevant.*

DRAFT DECISION

PART I – DEFINITIONS AND INTERPRETATION

In this Decision Instrument, save where the context otherwise admits or requires:

"2002 Act" means the Communications Regulation Act 2002 (No. 20 of 2002), as amended;

"2022 Regulations" means the European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444 of 2022);

"2023 Act" means the Communications Regulation and Digital Hub Agency (Amendment) Act 2023 (No.4 of 2023);

"Authenticity" [88] means a property that an entity is what it claims to be;

"Availability"[89] means a property of being accessible and usable on demand by an authorised entity;

"ComReg" means the Commission for Communications Regulation, established under section 6 of the Communications Regulation Act 2002, as amended;

"ComReg Document No. 14/02" means Response to Consultation on the Reporting & Guidance on Incident Reporting & Minimum Security Standards;

"Confidentiality"[90] means a property that information is not made available or disclosed to unauthorised individuals, entities, or processes;

"DECC" means the Department for the Environment, Climate and Communications;

"Electronic Communications Network" ("ECN") has the meaning assigned to it in the 2022 Regulations;

"Electronic Communications Service" ("ECS") has the meaning assigned to it in the 2022 Regulations;

"ENISA" means the European Agency for Cyber Security;

"Integrity" [91] means a property of accuracy and completeness;

"MS" means Member States;

"National Regulatory Authority" ("NRA") has the meaning assigned to it in the 2022 Regulations;

"Number Independent- Interpersonal Communications Service" ("NI-ICS") has the meaning assigned to it in the 2022 Regulations;

"provider" means a provider of public electronic communications networks or of publicly available electronic communications services; and

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the 2002 Act; the 2022 Regulations; the 2023 Act; the Numbering Conditions of Use and Application Process document

[88] (ISO/IEC 27000:2018), (see page 12 of the ENISA Revised Guidelines, footnote 9)
[89] (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 6)
[90] (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 7)
[91] (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 8).

(ComReg 15/136R3) as amended from time to time; and Commission Document XX/XX of which this Decision Instrument forms a part.

PART II – STATUTORY POWERS AND DECISION-MAKING CONSIDERATIONS

ComReg,

(a) Having had regard to the powers, functions, objectives and duties of ComReg, including, without limitation, those specifically listed below;

(b) pursuant to its objective under section 12(1)(a) of the 2002 Act in relation to the provision of electronic communications networks, electronic communications services and associated facilities— (iii) to promote the interests of users within the Community;

(c) pursuant to ComReg's statutory duty under section 12(2)(c) of the 2002 Act of, in relation to the objectives referred to in subsection (1)(a), taking all reasonable measures which are aimed at achieving those objectives, including— (vii) ensuring that the integrity and security of public communications networks are maintained;

(d) pursuant to ComReg's statutory duty under section 12 of the 2002 Act of, in carrying out its functions, having regard to international developments with regard to inter alia, electronic communications networks and electronic communications services, and associated facilities;

(e) pursuant to ComReg's specific duty under section 13 of the 2023 Act to take reasonable steps to ensure that providers comply with the obligations placed on them by or under Part 2;

(f) pursuant to ComReg's power under section 11(3)(g) to specify such other information that shall be contained in a notification to ComReg under section 11(1);

(g) pursuant to ComReg's general objective under Regulation 4(3) of the 2022 Regulations to promote the interests of consumers and businesses in the State by maintaining the security of networks and services and by ensuring a high and common level of protection for end-users through the necessary sector-specific rules;

(h) having regard, inter alia, to ComReg's duty under Regulation 4(5) of the 2022 Regulations to apply impartial, objective, transparent,

non-discriminatory and proportionate regulatory principles in pursuit of the policy objectives referred to in regulation 4(3) of those Regulations;

(i) having regard to the requirement in section 6(1) of the 2023 Act for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and service;

(j) having, pursuant to section 13 of the 2002 Act, complied with relevant Policy Directions contained in the February 2003 Ministerial Policy Direction: Policy Direction 5 – Policy Direction only where necessary; PD 6 – Policy Direction on Regulatory Impact Assessment; Policy Direction 7 – Policy Direction on consistency with other Member States;

(k) having considered all relevant evidence before it;

(l) having given all interested parties the opportunity to express their views and make their submissions in relation to Consultation [-], and considered such representations, as set out in the Response to Consultation and this Decision Instrument; and

(m) for the reasons set out in its written response to ComReg Document No.[-] to which this Decision is attached;

PART III – THE DECISIONS

hereby makes the following decisions:

Significant Incident Reporting Thresholds

(1) A "significant incident" for the purposes of reporting to ComReg under section 11 of the 2023 Act, is an incident that falls within the following thresholds:

(a) Where the percentage of the national user base affected and the duration of the incident, is as set out in the table below, where the x-axis represents hours, and the y-axis represents the percentage of the national user base affected:

	1h–2h	2h–4h	4h–6h	6h–8h	> 8h
1%–2%					
2%–5%					
5% –10%					
10%–15%					
> 15%					

(b) where any incident greater than or equal to one million (1,000,000) User Hours[92], has or is taking place; and

(c) where any incident impacting 1% or more of the National User Base which affects the Confidentiality, Integrity or Authenticity of that service, has or is taking place.

[92] User Hours is the product of the Number of Users affected and the Duration of the incident.

National User Base Calculations

(2) To determine its national user base and the percentage number of users for each service associated with any outage, a provider must reference relevant figures in the Quarterly Key Data Report ("QKDR") found on ComReg's webpage[93], as follows:

(a) For fixed voice communications service and fixed internet[94] access, providers should use the separate values outlined in the report.

(b) For mobile communications service, providers should use the number of active telephony Subscriber Identity Module ("SIM") cards based on the number of:

- Voice Subscriptions; and
- Machine to Machine Subscriptions.

(c) For mobile internet[95] access, providers should combine:

- The number of standard mobile subscriptions, which offer both voice service and internet access; and
- The number of subscriptions dedicated for mobile internet access[96].

(d) For NI-ICS, providers may sum the number of active users, within the State, of the services in the end of a period. These could be measured as the active users ("MAU"), where an 'active user' can, for example, be defined as the user who has used the service at least once in the respective period[97].

Information required for a notification

(3) Under the 2023 Act[98]; the following information is required to be contained in a notification made by a provider to ComReg under section 11(1):

(a) The category of incident, that is whether it is: Confidentiality, Integrity, Authenticity or Availability that is affected by the incident;
(b) the providers' name;

[93] Quarterly Key Data Report | Commission for Communications Regulation (comreg.ie).
[94] Including all data such as broadband access.
[95] Including all data such as broadband access.
[96] I.e., those using a dongle or similar device.
[97] Refer to Pg 20 Technical Guideline on Incident Reporting under the EECC — ENISA (europa.eu)
[98] At section 11 (2) c, d and f, and section 11(3).

(c) the public electronic communications network or publicly available electronic communications services provided by it affected by the incident;
(d) the date and time the incident occurred and its duration;
(e) the number of users affected;
(f) any class of users particularly affected;
(g) the geographical area affected;
(h) the extent to which the functioning of the network or service was affected;
(i) the impact of the incident on economic and societal activities;
(j) the cause of the incident and any particular circumstances that resulted in the security incident; and
(k) information concerning any or any likely cross-border impact with another MS.

Reporting significant incidents to ComReg

(4) Providers must use ComReg's e-licensing incident reporting portal[99] to report significant incidents to ComReg.

Timing for significant incident reporting

(5) (a) A provider must report a significant incident to ComReg as soon as possible and within the first 24 hours of the initial incident.

(b) If the incident is not resolved within 72 hours, the provider must supply an update to the existing report, advising the incident's impact and the action plan to resolve it.

(c) Upon the resolution of the significant incident, a provider must notify ComReg via the e-licensing incident reporting portal advising that the incident has been resolved and that services have been restored.

(d) For any significant incident, ComReg must receive a comprehensive update within four weeks of the significant incident that confirms the circumstances of the incident:

- The duration of the incident, if different from the previous updates;

[99] https://www.elicensing.comreg.ie/

- The communication services impacted, along with the number of users impacted for each service, if different from the previous updates; and
- a Root Cause Analysis report for the incident which at a minimum is to include the:
  - root cause summary statement for reported incident;
  - event timeline which details the sequence of contributing events leading to the incident;
  - description of impact to network infrastructure;
  - remedial timeline which details the sequence of actions taken to resolve the incident;
  - categorisation[100] of incident root cause, including a justification for its categorisation;
  - mitigation measures identified to prevent future occurrence of any similar incidents; and
  - timeline for implementation of identified mitigation measures.

Exception: Storm Reporting

(6) Notwithstanding the timings given at section 5 of this Draft Decision Document above, the following exceptional incident type requires the following notification timescales.

(7) Storm Reporting: when Met Éireann declares a named storm or when Met Éireann issues an orange or a red-level weather warning, ComReg will notify the providers registered on the e-licensing incident reporting portal with further details and the required reporting template or method.

(a) The timing for reporting the effect on the providers' ECN or ECS to ComReg will be at 10H00 and 16H00;

[100] The root cause of an incident can be categorised into one of five categories; 1. Human errors; 2. System failures; 3. Natural phenomena; 4. Malicious actions; 5. Third party failures. For further information on this categorisation please refer to Part 2 of ENISA Technical Guideline on Incident Reporting under the EECC.

(b) Such reports will continue, until providers notify ComReg that Networks and Services are operating on a Business as Usual ("BAU") basis; and

(c) ComReg will act as a single point of contact between providers, the DECC and the National Emergency Coordination Group (the "NECG"), the role of which is to coordinate and manage the national-level response to an emergency, on a "whole of government", cross-sector basis.

Information Required by the Minister, European Commission, Other NRAs and ENISA.

(8) Further to section 11(5) of the 2023 Act, and where ComReg is notified of a security incident under section 11(1), it shall (a) inform the Minister of the notification, and (b) having consulted with the Minister, and where ComReg considers it appropriate to do so, notify the competent authorities of other MS and ENISA. ComReg considers that the circumstances under which it would be appropriate to inform other NRAs or ENISA under this provision are likely to involve incidents with cross border significance.

(9) ComReg notes that further to section 16(1) of the 2023 Act, it may, for the purposes of exercising its functions under Part 2, consult, cooperate, share information with, or obtain the assistance of several bodies, including the Computer Security Incident Response Team ("CSIRT"), a CSIRT in another MS, or a NRA in another MS. Further to, section 11(6) of the 2023 Act, where ComReg determines, having consulted with the Minister, that the disclosure of a security incident notified under section 11(1) is in the public interest, it may inform the public of the incident, or require the provider concerned to do so.

(10) ComReg anticipates that reporting to ENISA and to the European Commission will, in the main, be via the annual reporting under section 11(9) of the 2023 Act. Further to section 11(9) of the 2023 Act, ComReg shall in each year submit a summary report to the Minister, the European Commission and ENISA on the notifications received and the actions it has taken in accordance with section 11. Furthermore, when ComReg is notified of a significant incident, as per the thresholds set out in the thresholds document, it will notify the Minister as required under section 11(5)(a) of the 2023 Act.

PART IV– EFFECTIVE DATE

Decisions (1) to (10) above shall apply to providers as from the date of the making of this Decision Instrument.

PART V – MAINTENANCE OF OBLIGATIONS

If any section or clause contained in this Decision Instrument is found to be invalid or prohibited by the Constitution, by any other law or judged by a court to be unlawful, void or unenforceable, that section or clause shall, to the extent required, be severed from this Decision Instrument and rendered ineffective as far as possible without modifying the remaining section(s) or clause(s) of this Decision Instrument and shall not in any way affect the validity or enforcement of this Decision Instrument.

PART VI - STATUTORY POWERS NOT AFFECTED

Nothing in this Decision Instrument shall operate to limit ComReg in the exercise of its discretions or powers, or the performance of its functions or duties, or the attainment of objectives under any laws applicable to ComReg from time to time.

Signed

Robert Mourik

Commissioner, Commission for Communications Regulation