An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation

Network Incident Reporting Thresholds: Response to Consultation

On the revision and replacement of ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum-Security Standards)

Response to Consultation

Reference:	ComReg 24/23
Decision No:	D08/24
Version:	Final
Date:	02/04/2024

Content

Annex

Table of Figures

Section Page

1 Executive Summary

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

2 Significantly, Articles 40 and 41 of the EECC, relating to the security of networks and services, replace Article 13a and 13b of the then European Telecommunications Regulatory 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").

3 The EECC and subsequently the Act bring more electronic communications services within scope, and the terms **"Security"**[2] and **"Security Incidents"**[3] are now explicitly defined. Part 2 of the Act details security obligations for providers of: electronic communications networks and services, and of Number Independent Interpersonal Communication Service ("NI-ICS")[4].

4 In particular, Part 2 of the Act has the following requirements:

[1] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

[2] '*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*', see Article 2(21) of the EECC, as transposed in section 5 of the Act.

[3] '*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', see section 5 of the Act.*

[4] NI-ICS are as defined in Article 2(7) of the EECC and Regulation 2 of the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (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.

- Under section 6(1) of the Act, providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services;

- Under section 11(1) of the Act, 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 undue delay; and

- Under 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 taken by ComReg in accordance with this section.

5 Furthermore, under section 13 of the Act, ComReg shall take reasonable steps to ensure that providers comply with the obligations placed on them by or under Part 2 of the Act.

6 In light of these changes, on 25 April 2023, ComReg published a consultation[5] on Network Incident Reporting Thresholds to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards) ("Consultation").

7 This Response to Consultation considers the views of respondents in relation to the Consultation and sets out ComReg's conclusions on:

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

- 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, and enforce the obligations imposed on them under section 11 of the Act.

[5] Network Incident Reporting Thresholds, A consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards) – ComReg Document 23/36 – https://www.comreg.ie/media/2023/04/ComReg-2336-2.pdf

8 This Response to Consultation and the associated Decision Instrument, contained in Annex 2 of this document ((D08/24) the "Decision Instrument"), set out how ComReg will require providers to report significant incidents under the relevant provisions of the EECC, the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022"), and the Act. The Response to Consultation and the Decision Instrument also describe the actions ComReg expects providers to take, to ensure compliance with the Act.

1.1 Management of the security of Networks

9 ComReg notes that under the Act obligations are placed on providers in respect of the management of the security of their networks and these are set out in Part 2 of the Act. Furthermore, section 6(1) requires that providers take appropriate technical and organisational measures to manage the risks posed to the security of networks and services and pursuant to section 6(2), those measures taken, shall ensure a level of security appropriate to the risk presented, having regard to the state of the art.

10 This Response to Consultation in the main, refers to the incident reporting thresholds for providers under the ENISA Revised Guidelines[6]. It is noted, that contrary to the previous practice, there are not only updated thresholds, consequential to the aforementioned changes brought in by Part 2 of the Act[7], but greater information requirement obligations on providers, including:

- 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[8]; or

[6] 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

[7] As transposed from Article 40 of the EECC.

[8] "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.[9]

11 In short, the ENISA Revised Guidelines provide a guide to a Competent Authority ("CA") on the significance of the security incident and the measures that have been taken by a provider.

12 This notwithstanding, under section 7 of the Act, ComReg may also issue a security measures direction to require a provider to, inter alia:

a) provide information that would be used to assess the security[10] 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[11].

1.2 Summary of Proposed Approach

13 The Regulatory Impact Assessment ("RIA") in Chapter 4 considers and evaluates the options available to ComReg for it to fulfil its statutory obligations and functions pursuant to Part 2 of the Act. After the evaluation of the options in the RIA, the proposed approach has the following differences and benefits:

- When reporting a security incident, providers **must now categorise the incident**. That is, whether the security incident can be categorised as affecting: Confidentiality, Integrity, Authenticity or Availability[12], as defined below:
    - **Confidentiality**[13]**;** 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

[9] See the Economic and Societal Impacts of Network Incidents Study | Commission for Communications Regulation (comreg.ie), ComReg Document No. 23/59a.
[10] Section 14 (3)(c) of the Act.
[11] Section 14 (3)(d) of the Act.
[12] Please note that these categories are not mutually exclusive.
[13] 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)

place with the communications being forwarded to unauthorised parties;

- **Integrity**[14]; 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**[15]; 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**[16]; when the security 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'.

- While several thresholds remain from the previous approach[17], and as detailed above, now providers will be required to report security 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, security incidents affecting a network or service should be reported[18] to ComReg:

  - where a security incident affects more than 1% of the National User Base of that service, or
  - where the number of hours lost for the affected service exceeds the **absolute threshold**[19].

[14] 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)
[15] 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)
[16] 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)
[17] ComReg Document 14/02
[18] The calculations for which are set out in Part III Section 2 in the Decision Instrument
[19] See: Part III, Section 2, of the Decision Instrument in Annex 2 to this document.

- 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**[20] and that any such security incident be included in the annual summary report, to ENISA, if the **absolute threshold is greater than or equal to one million (1,000,000) user hours lost**.

- The information required for reporting a security incident is detailed in section 11 of the Act[21]. ComReg notes that typically, providers would in any event already report such security incidents voluntarily under the current reporting obligations. The approach detailed in this Response to Consultation and Decision Instrument therefore provides for a pragmatic reporting methodology, minimising ambiguities and simplifying the reporting requirements for the provider.

- The reporting of security incidents – within the required timescales, as detailed in the Decision Instrument, allows for valuable lessons to be learned quickly. The sharing of learnings from incidents with ENISA, particularly where an incident occurs involving more than one MS, ensures that other MS benefit from this, and vice versa. This approach promotes improved resilience of networks throughout MS and may mitigate any further propagation of security incidents.

14 Furthermore, the RIA below notwithstanding, there are other benefits to the revised approach:

- The use of the incident reporting portal by the increased number of providers required to report under the Act simplifies the reporting requirements, while enhancing the consistency necessary for summary reporting to ENISA, pursuant to section 11(9) of the Act;

- ComReg continues – where appropriate to have regard to and align to the reporting thresholds and timings for the reporting security incidents, as contained in the current ENISA Guidelines on incident reporting;

[20] Defined in Article 2 of the EECC.
[21] S. 11 of the Act.

- For ease of reference, the thresholds and timings for the reporting security incidents are detailed in the Decision Instrument; and

- This document replaces ComReg's procedural guidance document regarding Incident Reporting and Minimum-Security Standards for Network Operators[22] , Document 14/02. Industry should note that a Decision Instrument is legally enforceable by ComReg.

[22] Response to Consultation – Reporting and Guidance on Incident Reporting and Minimum Security Standards – https://www.comreg.ie/media/dlm_uploads/2015/12/ComReg1402.pdf

2 Introduction

15 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.

16 ComReg Document 14/02[23] set out the appropriate thresholds for reporting incidents[24], 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").

17 On 20 December 2018, a revision of the European Telecoms Regulatory Framework, relating to the electronic communications sector, called the European Electronic Communications Code[25] (the "EECC") entered into force. The EECC updates the preceding European Telecoms Regulatory Framework of 2009 by repealing and replacing the underlying EU Directives ("Telecoms Framework"), namely the: Framework Directive[26]; Authorisation Directive[27]; Access Directive[28]; and Universal Services Directive[29].

---

[23] 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

[24] 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."

[25] 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

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

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

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

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

18 The security provisions of the EECC, namely Articles 40 and 41, are transposed into Irish law by 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").

19 Other elements of the EECC, not of direct relevance to this Response to Consultation, are transposed in the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022").

20 Furthermore, on 22 March 2021, ENISA published revised guidelines on incident reporting, under the EECC (the "ENISA Revised Guidelines"). [30] These 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.

21 Under 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[31].

22 Article 40, as transposed in Part 2 of the Act, in a similar manner to the existing EU Framework, continues to require ECN and ECS providers to report significant security incidents to ComReg. A **'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'*, (emphasis added)[32].

[30] 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

[31] "provider" means a provider of public electronic communications networks or of publicly available electronic communications services, as defined in the Act.

[32] Section 5 of the Act.

23 Furthermore, Part 2 of the Act details security obligations for providers of ECN, ECS, and Number Independent Interpersonal Communication Service ("NI-ICS")[33].

24 In the event of a security incident that has a significant impact on the operation of ECN, ECS or NI-ICS, reporting obligations for providers are outlined in Annex 2 of this document.

25 Sections 13 to 16 of the Act[34] detail how ComReg can implement and enforce the security incident requirements and reporting obligations[35], as detailed in Chapter 5 of the Consultation.

26 Under section 11(5) of the Act, where ComReg is notified of a security incident under section 11(1), it shall- (a) inform the Minister[36] 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[37]. Where ComReg determines that it is in the public interest, and after having consulted with the Minister, ComReg may inform the public of the incident or require the provider concerned to do so[38].

27 This Response to Consultation:

a) considers the nine responses received to the Consultation, ComReg Document No. 23/36, through the lens of the additional requirements introduced by the Act as compared to those in Document 14/02;

b) takes account of the guidance provided by the ENISA Revised Guidelines;

[33] 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.
[34] As transposed from Article 41 of the EECC.
[35] 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.
[36] The Minister for the Department of the Environment, Climate and Communications ("DECC").
[37] The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe.
[38] Section 11(6) of the Act.

c) further clarifies the appropriate thresholds for reporting incidents and the requisite timing for submission of these reports; and

d) contains in Annex 2 of this document, the Decision Instrument (D08/24), which will, in final form, replace Document 14/02.

28 The updated thresholds and processes for reporting security incidents, as detailed below, set out clearly ComReg's decision[39] on what is required by providers to comply with the new and updated reporting requirements.

29 This Response to Consultation, and the accompanying Decision Instrument (contained in Annex 2 of this document), contains ComReg's approach to both assessing and enforcing providers' compliance with their reporting obligations in respect of Part 2 of the Act.

2.1 The Act and the EECC

30 As has been noted above, the EECC updates and merges the existing European framework governing the European telecommunications sector. The EECC is transposed into Irish law by the Act and by the European Communications Code Regulations 2022 ("Regulations of 2022"). The Act gives effect to the provisions of the EECC not included in the Regulations of 2022, including provisions related to security and security incidents (contained in Part 2 of the Act), 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 in particular the notification requirement for security incidents contained in Article 40(2) of the EECC transposed by section 11 of the Act.

Part 2 of the Act: security of networks and services

31 Section 5 of the Act defines a "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." (emphasis added).

[39] Implemented and enforceable under the Decision Instrument D08/24.

32 The security of networks and services is provided for in the Act by virtue of:

- section 6 of the Act: providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services. Furthermore, section 6(2) provides that: measures taken in accordance with subsection (1) shall ensure a level of security appropriate to the risk presented having regard to the state of the art;

- section 11(1) of the Act: 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 subsection (3) without undue delay. Section 11(2) provides: 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; and
    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;

- section 11(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; and

g) such other information as ComReg may specify.

- section 11(4:) Where a provider notifies ComReg of an incident in accordance with this section 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. Section 11(5) provides that: Where ComReg is notified of a security incident under subsection (1) 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. Section 11(6) Where ComReg 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.

Implementation and enforcement

33 This is provided for by the following sections of the Act:

- section 11(7) of the Act provides that subsections (1), (2), (3) and (4) are regulatory provisions, and are thus subject to civil enforcement by ComReg under Part 7 of the Act;

- section 11(8) provides that: 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 ComReg 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; and

- section 14 of the Act, ComReg has the power to serve security measures directions. Section 14(1) provides that: a provider shall, on the request of the Commission, provide the Commission with the information needed to assess the security of the provider's networks and services, including documented security policies. Section 14(2) provides that ComReg may serve a direction on a provider—

  a) to remedy a security incident,

  b) to prevent a security incident from occurring when a significant threat has been identified, or

c) to ensure that the provider is in compliance with Part 2. By virtue of section 11(7), a provider that fails to comply with a security measures direction commits an offence and is liable on summary conviction to a class A fine.

2.2 The ENISA Revised Guidelines

34 The ENISA Revised Guidelines on Incident Reporting under the EECC[40] 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 security incident reports:

1) National incident reporting from providers to CAs;

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

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

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

- To give feedback to CAs regarding:
  - Security incidents that have had significant impact;
  - Root causes of security incidents;
  - Lessons learned from security incidents; and
  - Security incident trends.
- To provide aggregate analysis of security incidents for policy makers, the public and the industry, describing the overall frequency and impact of security incidents across the EU;

[40] 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

- To facilitate the exchange of experiences and lessons learned among CAs;
- Issue recommendations and guidance for CAs, the private sector, policy makers; and
- Evaluate the effectiveness of security measures in place.

2.3 Responses Received to the Consultation

36 There were nine responses received to the Consultation, as follows:

- eir;
- ENEA;
- Imagine;
- Microsoft Corporation;
- National Broadband Ireland ("NBI");
- Sky Ireland;
- Three;
- Virgin Media Ireland Limited ("Virgin Media"); and
- Vodafone.

37 ComReg would like to thank the interested parties for their responses. ComReg has published the non-confidential versions of the responses as ComReg Document xxx.

38 Having carefully considered the responses, the points made therein and other relevant information, this document, among other things, sets out ComReg's views in relation to the matters raised by the respondents, and ComReg's conclusions.

2.4 Chapters of this Document

39 The Chapters of this Document deal with the following matters:

Chapter 1	Executive Summary;
Chapter 2	Introduction;

Chapter 3	Assessment of Consultation Issues;
Chapter 4	Regulatory Impact Assessment;
Chapter 5	Next Steps;
Annex 1	Legal Basis;
Annex 2:	Decision Instrument: D08/24; Replacement of ComReg Document No. 14/02; and
Annex: 3	National User Base Calculations.

3 Assessment of Consultation Issues

3.1 Introduction

40 The Consultation in summary, addressed the following matters:

- The proposed categorisation, thresholds, timescales and exceptions required for the reporting of security incidents to ComReg;
- The proposed process for communicating details of security incidents to ComReg; and
- The proposed approach that will be followed by ComReg to enable it to monitor providers' compliance with the obligations imposed on them under Part 2 of the Act.

41 The Consultation also contained an associated draft Decision Instrument, which formally set out the proposed obligations on providers to report significant incidents under the relevant provisions of the Act.

42 Furthermore, two questions were posed in the Consultation document, and these were as follows:

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.

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.

43 As outlined in Chapter 2 of this document, there were nine responses received to the Consultation and ComReg notes that eight of these were generally supportive of the proposed changes to incident reporting, as contained in the Consultation.

44 The particular matters raised by respondents to the Consultation are categorised under the following headings:

i) Definition of a Security Incident;

ii) Security Incident Categorisation;

iii) Thresholds and the National User Base;

iv) NI-ICS Thresholds and National User Base;

v) Qualitative Thresholds;

vi) Reporting Information Requirements;

vii) Reporting Portal;

viii) Security Incident Reporting and Timescales; and

ix) Other Matters Raised

45 The following sections set out ComReg's views in relation to each of the matters raised. Readers are reminded to refer to the Consultation document for further details.

3.2 Definition of a Security Incident

46 In the Consultation, ComReg used the security incident definition as set out in Part 2 section 5 of the Act:

- *'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'*[41]*; 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'*[42]*.*

3.2.1 Views of Respondents

47 Vodafone suggested some refinement in ComReg's guidance in relation to the definition of a security incident. Vodafone contends that the inclusion of availability within the definition of a security incident, will cause confusion for its operational teams in determining which incidents must be reported.

48 Vodafone is also of the view that in categorising an incident caused by power outages as a security incident, it will cause operational teams further confusion.

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

49 NBI opined that the Consultation uses various terms when referring to incidents and this creates a degree of confusion and NBI stressed the importance of clarity in terminology. NBI referred to articles 40 and 41 of EECC and Part 2 of the Act, which it contends exclusively use the term "security incidents". NBI is further of the view that including reporting requirements for weather incidents adds confusion. NBI contends that storms are not security incidents and therefore should not be treated as such in its view.

50 Furthermore, NBI notes ComReg's requirements on providers to report security incidents that have a significant impact as soon as possible and NBI requested clarification from ComReg on its definition of a security incident with a significant impact.

3.2.2 ComReg's View

51 As respondents will be aware, the obligation on operators to report all 'security incidents' having a 'significant impact on the operation of the providers electronic communications networks or services' is a requirement of section 11(1) of the Act. Furthermore, the definition of a security incident, set out at section 5 of the Act, includes any action that affects 'the **availability**, authenticity, integrity or confidentiality of networks and services', emphasis added.

52 Given the above, it is apparent that a storm and power outage typically falls within the meaning of a security incident. In this case it is one that specifically affects availability of the providers ECN or ECS in the areas affected. ComReg also recognises that the extent that a provider is affected, will depend on, but may not be limited to, any back up power facilities, redundant transport (backhaul) link technology; and the adaptability of the access technologies in use by the provider.

53 Furthermore, ComReg notes NBI's comments regarding the terms 'incident' and 'security incident'. ComReg confirms that the term "incident", as used in its Consultation, is a reference to a "security incident". For the avoidance of all doubt, in this document, where ComReg refers to 'incident', ComReg means "security incident".

3.3 Incident Categorisation

54 In chapter 4.2 of the Consultation, ComReg detailed that when reporting a security incident, providers are required, under section 11 of the Act, to clearly categorise the security incident, according to whether the incident has compromised the confidentiality, integrity, authenticity or availability of the ECN and/or ECS affected by the incident[43].

3.3.1 Views of Respondents

55 Vodafone is of the view that when developing a reporting regime and other security measures, that micro-management or reporting to multiple agencies on network security incidents or storm related events are avoided. Vodafone submits that ComReg should ensure that any duplication is avoided especially with the increased focus on Security matters through the implementation of ECSMs. Vodafone further contends that, in its view, the objective of reporting of any security incident should be through one channel.

56 Sky Ireland opines that security incidents affecting confidentiality, integrity, and authenticity are likely to be cyber in nature and that the extension of the incident reporting obligation to these security incidents should also consider that service providers will have cyber monitoring obligation under the Electronic Communications Security Measures ("ECSMs"). In light of this, Sky contends that there may be lead-in time needed for service providers to implement new incident reporting obligations.

3.3.2 ComReg's View

57 ComReg reiterates that the focus of this Consultation is on security incidents that are to be reported under section 11 of the Act and not the 'Security Measure Guidelines'[44], made under section 7 of the Act.

[43] See paragraph 106 in document 23/36 for the relevant definitions of these incident categories.
[44] See section 7 of the Act.

58 Finally, ComReg notes Sky's thoughts regarding the probable cause of security incidents affecting confidentiality, integrity, and authenticity *"… are likely to have a root cause of a cyber-nature…"*. While the evidence available to ComReg contests this assertion. In particular, ComReg notes from both its Network Operations Annual reports[45] and the ENISA evidence available on a pan-European basis (as shown in figure 1 below), that most security incidents are in fact of a consequence of system failures. However, ComReg recognises that the classification of the type of security incident experienced by a provider when reporting is important and will take this into account when modifying the incident reporting portal on e-licensing, which should minimise the need for any 'lead in' time.

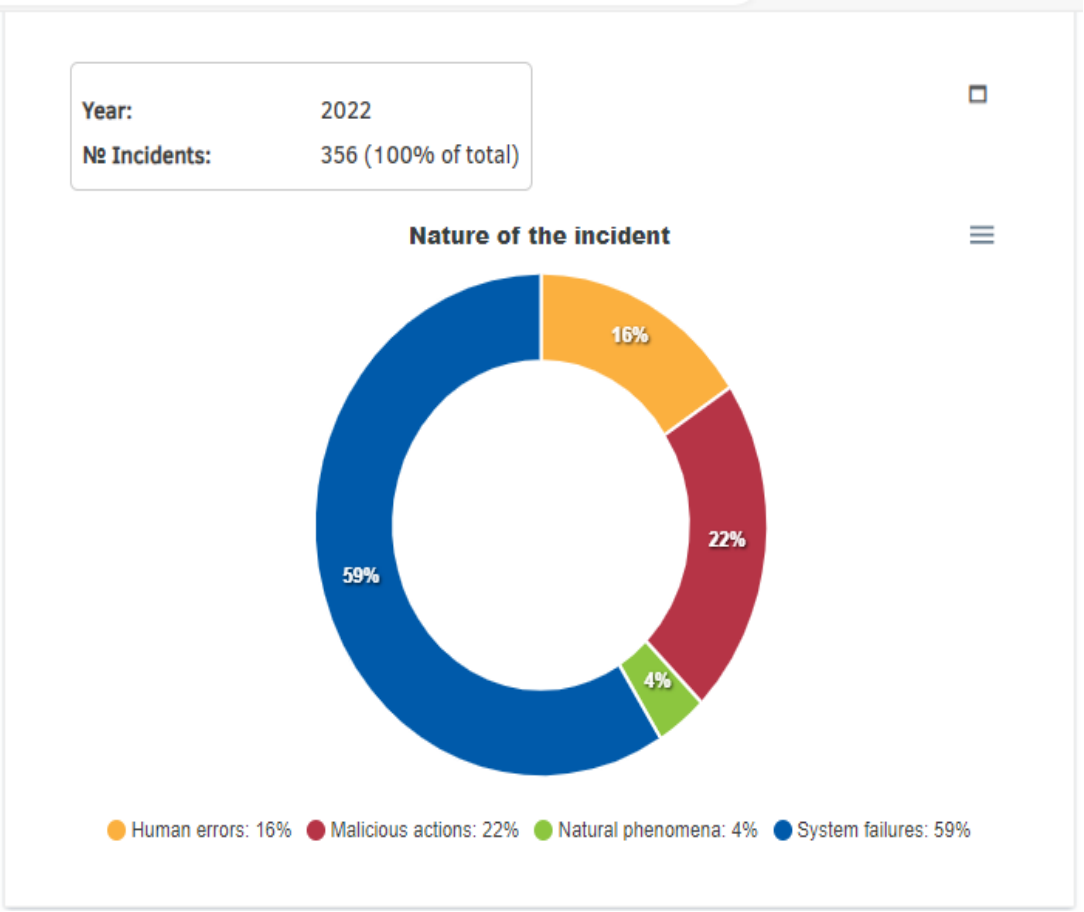

Figure 1: Reported Security Incidents for 2022 in the Communications Sector across MS (ENISA)

[45] See ComReg Document Nos.: 23/60, 22/44, and 21/29 etc.

3.4 Thresholds and the National User Base

59 In the Consultation, ComReg set out its proposed thresholds for reporting significant security incidents and the proposed rules to calculate the National User Base ("NUB") for each service associated with any outage.

60 For the proposed Thresholds, ComReg outlined the following:

- In the main, the proposed reporting thresholds for security incidents are similar to those contained in Document 14/02, comprising of the percentage of the national user base of the service impacted and the duration of the security incident, as detailed in figure 2 below:

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

Figure 2: Thresholds, based on National User Base and Incident Duration[46]

- The exception to those contained in Document 14/02 arises from the introduction of an absolute threshold: that is **any security incident**, affecting availability, greater than or equal to one million (1,000,000) User Hours[47], must now be reported; and

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

[46]Page 21, Technical Guideline on Incident Reporting Under The EECC, ENISA, March 2021.
[47] User Hours is the product of the Number of Users affected and the Duration of the incident.

61 For the proposed national user base calculations, ComReg highlighted that providers should reference the figures set out for the relevant service[48] in ComReg's Quarterly Key Data Report[49] ("QKDR") when determining the relevant percentage for each service associated with any outage:

- For fixed voice communications service and fixed internet[50] access, providers should use the separate values outlined in the report.
- 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.
- For mobile internet[51] 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[52].
- 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[53].

[48] The services as per the ENISA Revised guidelines and contained in the QKDR are as follows: Fixed Telephony (Voice including VOIP); Fixed Internet (Broadband); Mobile Telephony (Voice and Data); and Mobile Internet (Data only, i.e., USB data dongles).
[49] Quarterly Key Data Report | Commission for Communications Regulation (comreg.ie).
[50] Including all data such as broadband access.
[51] Including all data such as broadband access.
[52] i.e., those using a dongle or similar device.
[53] Refer to Pg 20, Technical Guideline on Incident Reporting Under The EECC, ENISA, March 2021.

3.4.1 Views of Respondents

62 Three noted that, while there is the absolute threshold of one million (1,000,000) user hours, in relation to smaller outages, ENISA in its guidelines recommended the exclusion of: *"very small incidents, which affect less than 25.000 user connections, as well as very short incidents, which last less than 1 hour*". Three therefore suggested that ComReg should set out the exclusion of such very small and very short incidents in its Decision, if the alignment with ENISA guidelines is ComReg's intention.

63 Sky contends that there are no apparent differences between the reporting of incidents that impact the availability of fixed lines and mobile services. Sky therefore sought further guidance on identifying thresholds for incidents which have an impact on the availability of mobile services, in particular, mobile RAN sites. Sky observes that, unlike fixed networks, the relationship between RAN sites and subscribers varies over time.

64 Microsoft contends that enterprise services are not addressed in ComReg's proposed guidance. Microsoft suggests that *"ComReg recognize explicitly that enterprises (not their employees) are the customers for purposes of counting thresholds. For example, the terms "User" and "User Hours" should be interpreted as referring to subscribers, at least with respect to enterprise customers...".*

65 Microsoft also contends that the proposed guidance does not set out the appropriate National User Base to be used for telephone calling services accessible via mobile or fixed data networks. Microsoft requests that ComReg clarify how the thresholds apply to nomadic/internet-based VoIP telephone calling services and suggests that VoIP services could be subjected to the same thresholds as fixed voice services.

66 Further, Microsoft opines that, unlike typical fixed or mobile voice services which allow for a user to both make and receive telephone calls, there are some applications that have limited telephone calling features, i.e., they allow for calls to telephone numbers but cannot receive calls from telephone numbers (or vice versa). Microsoft contends that while these applications may qualify as NB-ICS, it is of the view that they are not critical lifeline services such as typical fixed or mobile voice services. Therefore, they should not be subject to the same reporting thresholds for typical fixed or mobile voice services but more aligned with those for reporting security incidents on NI-ICS.

67 eir suggested that, for clarity, ComReg should identify and publish the relevant National User Base each time the Quarterly Key Data report is published.

3.4.2 ComReg's View

68 ComReg notes that, in general, respondents are supportive of the proposed thresholds and seek clarification on the application of reporting thresholds in certain instances.

69 Regarding the absolute threshold for reporting security incidents (equal to or greater than one million user hours lost) and very small incidents, ComReg confirms that for a security incident under this value, these need not be reported (i.e., less than 25,000 customers, and less than one hour in duration). This aligns with the guidance provided by ENISA.

70 In respect to security incidents that impact Fixed and Mobile ECN or ECS, ComReg described in Section 4.2.3 of the Consultation the proposed thresholds applicable for reporting security incidents with a significant impact on the operations of the provider's ECN or ECS.

71 In relation to eir' s suggestion that ComReg should identify and publish the relevant National User Base, ComReg notes that the values required to calculate the national user base figures are easily accessed from the QKDR publication. However, ComReg has provided further clarity in the Decision Instrument to make clear the relevant components of the National User Base. These are Fixed Voice, Fixed Broadband, Mobile Voice Communications Service, Mobile Internet Access and Machine to Machine Communications. Providers should have regard to these figures each quarter to ensure effective reporting of security incidents going forward.

72 ComReg notes the view of Sky that the relationship between mobile RAN sites and subscribers may vary, however ComReg points out that user base thresholds formed part of the reporting guidelines for mobile services in ComReg Document 14/02. As such, providers should be best positioned to use data available to them to calculate this number.

73 By way of example, the estimate used by the provider may be based on a simple average of the number of the provider's mobile subscribers divided by the total number of sites operating the service and then multiplying this by the number of sites affected by the incident. Or an alternative, could be to estimate this on a per county, rather than national basis. ComReg is cognisant that the number of subscribers per provider, per RAN site is always going to be a best effort estimate.

74 Regarding the appropriate NUB for voice telephony services accessible via mobile or fixed data networks, ComReg notes that in the ENISA Revised Guidelines, the VoIP service is included in the scope of Number-based Interpersonal Communication Services. Specifically, as a service that is provided over a fixed network. This implies that the fixed voice calculations are appropriate for VoIP services. In general, if the voice service is provided over a fixed network, the applicable threshold should be based on the fixed voice calculation. If a service (such as VoLTE) is provided over mobile network, then the mobile voice calculations should be used.

75 VoIP services that are provided over fixed networks and connect to number-based services, whether Internet Protocol ("IP") or Circuit Switched ("CS") are subject to the reporting threshold for fixed voice services. In general, voice services that are provided over ECN/ECS including Apps with limited telephone calling features should be subject to ComReg's proposed quantitative thresholds that set out in part III section 1 in ComReg's Decision Instrument. Noting that for any significant security incident to be reportable to ComReg, it should fall within ComReg's thresholds detailed in part III section 1 of the Decision Instrument.

76 Regarding security incidents that impact enterprise customers, ComReg clarifies that providers consider users as the number of subscribers impacted. This approach is consistent with the presentation of subscriber data in the QKDR. ComReg refers readers to Annex 3 of this document for how national user bases for each service are calculated using the most recently published QKDR data. A provider should have regard to the most recently published QKDR data at the time of reporting a security incident.

3.5 NI-ICS, Thresholds and National User Base

77 In the Consultation ComReg proposed identical security incident reporting thresholds for Number-Independent Communication Services (NI-ICS) as it did for other ECN and ECS, and these are outlined in Figure 2 above.

78 In respect of its proposed National User Base (NUB) calculation rule, ComReg outlined that 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[53].

3.5.1 Views of Respondents

79 eir requested clarification in relation to the calculation of the national user base for the NI-ICS services. In doing so, eir highlighted that paragraph 115 of the Consultation suggests that providers of the NI-ICS services will have the responsibility to calculate the NI-ICS national user base. eir contends, that in its view, this appears inappropriate due to impartiality and commercial confidentiality concerns. eir referred in making its case to an ENISA guideline which states *"For NI ICS CAs may sum up the number of active users of the services in the end of a period[54]"*. eir contends that this places the responsibility for the calculation of the NI-ICS NUB on the National Competent Authority, in this case ComReg. eir therefore contends that the national user base for NI-ICS services should be published with the other national user bases in ComReg's QKDR.

[54] Refer to Pg 21, Technical Guideline on Incident Reporting Under The EECC, ENISA, March 2021.

80 Microsoft sought clarification in relation to the NUB metric for NI-ICS as it noted that the QKDR does not currently contain NUB metrics for NI-ICS. Microsoft contends that the approach proposed for the calculation of the NI-ICS user base seems to diverge from the other service categories as it bases the calculation of the user impact on the total user base of the individual provider, rather than the NUB for the NI-ICS market as a whole. Microsoft believes that such an approach would significantly reduce the user base denominator, which in turn would, in its view, lead to overstating the user impact, thereby imposing a much lower threshold for NI-ICS than that for NB-ICS.

81 Additionally, Microsoft expressed concerns in respect to the calculation of a NUB for the NI-ICS market. Firstly, Microsoft opines that the scope of the NI-ICS definition can possibly include different types of services, from email services to app-based voice or messaging services and therefore calculating the user base for NI-ICS, as a whole would, in its view, overstate the market size and result in under-reporting. Further, Microsoft notes that customers can subscribe to multiple services of the same type, for example email services, but again this would further overstate the NI-ICS market size. All of this makes it difficult, in Microsoft's view, to determine a reliable user base metric for the NI-ICS market as the NI-ICS user base is susceptible to larger fluctuations across time and events.

82 For the reasons it outlines, Microsoft proposes the adoption of a modified user base calculation that relies on the best available proxies for the market size of each specific NI-ICS service type. More specifically, Microsoft contends that ComReg would be best served by basing NI-ICS thresholds on a percentage of the total Irish population, instead of attempting to define a market where determining actual users across competing services can be problematic.

83 Microsoft further contends that the availability reporting thresholds should reflect the distinct and unique features of NI-ICS, such as, the high degree of substitutability and the fact that they do not support lifeline services[55]. Therefore, these thresholds should be appropriately tailored. For paid NI-ICS services, Microsoft suggested that applicable availability reporting threshold should be the absolute threshold of one million or more user hours. For free of charge NI-ICS services, the applicable availability reporting threshold should, in its view, be 15% or more of the Irish population affected for a period of at least 8 hours. Such an approach, it argues, accounts for the unique features of NI-ICS and would be appropriately tailored to capture and report only outage incidents with significant impact.

3.5.2 ComReg's view

84 Given the definitions of NI-ICS contained in Regulation 2 of the Regulations of 2022 and taking into account the guidance in Recital 95 of the EECC; in the Consultation, that NI-ICS providers must now register on the incident reporting portal.

85 In relation to a NUB for NI-ICS; the QKDR does not include or provide figures for NI-ICS services. Furthermore, NI-ICS are relatively substitutable, as a user may have more than one similar NI-ICS product from different providers on their device. Therefore, ComReg considers that a NUB based approach to the reporting of security incidents for NI-ICS would lead to considerable ambiguity.

[55] Emergency Call Answering Service, (999 and 112 services).

86 As such, ComReg considers that a clearer and more consistent approach, is to make providers of NI-ICS only subject to the absolute threshold for a significant security incident, which within the jurisdiction of Ireland, is one million (1,000,000) user hours. That is, NI-ICS providers will therefore be required to report a security incident to ComReg if the product of the duration of the incident and the number of users affected is equal or exceeds sixty million (60,000,000) user minutes i.e., one million (1,000,000) user hours. However, in a similar manner to the obligations of the Act on providers of conventional ECN and ECS, failure to report a security incident on a NI-ICS will constitute an offence under section 11 (8) of the Act by the NI-ICS provider concerned. Furthermore, pursuant to Recital 95 of the EECC, ComReg reserves the right to revise this approach following re-assessment 'of the security risks involved' as experience and knowledge of NI-ICS and their operation grows.

3.6 Qualitative Thresholds

87 In its Draft Regulatory Impact Assessment, ComReg was of the view that an approach which uses clearly defined quantitative values to guide the reporting of incidents will continue to be an effective approach and lessens the risk of ambiguities in reporting. ComReg did not propose any qualitative measures at this time but noted that it may revisit the matter in the future.

3.6.1 Views of Respondents

88 ENEA opined that ComReg should reconsider its position in regard to qualitative thresholds for reporting of security incidents. In particular ENEA contends that the inclusion of qualitative thresholds is essential to:

(i) align with ENISA's recommendation that both qualitative and quantitative thresholds should be applied to capture significant security incidents;

(ii) align with ENISA's 2018 high level recommendation for NRA's to consider including signalling security in terms of reporting security incidents and adopting minimum security requirements;

(iii) enable information sharing with ENISA to support improved resilience of networks throughout the EU;

(iv) avoid leaving a gap in reporting of security incidents which involve the threat of significant societal or economic harm but would not be captured by quantitative reporting thresholds, in particular signalling borne threats and interconnect attacks;

(v) avoid adversely affecting operators approaches to resourcing threat detection capabilities; and

(vi) avoid a potential deficiency in ComReg's Network Operations functions.

3.6.2 ComReg's View

89 In relation to (i), ComReg notes that the 'qualitative thresholds' for security incidents, as described in the ENISA Revised guidelines, are guidelines only. Whereas section 11 (2) (c, d and f) of the Act require that providers shall have regard to such information, (as used by ENISA as qualitative thresholds) in determining whether a security incident that impacts their ECS and/or ECN is significant. Furthermore, section 11 (3) of the Act requires that the information relating to the same, be included when reporting the security incident to ComReg. Further, to minimise ambiguities and promote efficient reporting by providers, ComReg's preferred approach is to use quantitative thresholds for reporting security incidents as these are objective and allow for direct comparison across Member states, with less vagaries in interpretation.

90 In relation to (ii), (iii) and (v) ComReg observes that Member States NRAs are likely to adopt different approaches for providers to notify significant security incidents and notes the examples provided in section 4 of ENISA's Guidelines which emphasises this. ComReg's approach has regard to the criteria in section 11(2) of the Act, and the quantitative threshold types and levels recommended by ENISA.

91 Regarding (iv), ComReg confirms that security incidents that are Denial of Service ("DoS") or signalling storms are reportable under section 11(2) (e and g) of the Act, as they impact network integrity.

92 Further, regarding a security incident that impacts interconnection, where a security incident affects an ECN or ECS that uses an interconnection service from another provider, then it is the provider of the interconnection service that is responsible for reporting the security incident.

93 Finally, regarding (vi), it should be noted that ComReg's ability to evaluate network security is not dependent on incident reporting thresholds whether they be quantitative or qualitative. The updated incident reporting thresholds are being put in place for providers of ECN and ECS to notify ComReg that a security incident has occurred and is having or had a significant operational impact on the providers ECN or ECS, as required under Part 2, section 11 of the Act. Providers should note that the reporting mechanism, in itself, is not for network security evaluation but instead is for the notification of a network security breach or failure on a providers ECN or ECS.

3.7 Reporting Information Requirements

94 In the Consultation, ComReg outlined that the following further information that is now required, pursuant to section 11(2) (c), (d) and (f) of the Act (and section 11(3)(d)) and that providers should take account of these when considering a security incident's significance:

- 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[56] affected; or
- The impact of the incident on economic and societal activities.

95 For completeness, ComReg also set out the full set of information, as required by section 11(2) and section 11(3) of the Act, that providers must provide with any incident reports.

3.7.1 Views of Respondents

96 eir disagrees with the inclusion of information on the economic and societal impacts in the incident report. It contends that its Service Management Centres ("SMC") i.e., operational staff do not possess the skillsets required to assess the societal and economic impacts of an incident and that the focus of the SMC should be on resolving incidents.

[56] "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.

97 eir also submits that, in its view, there is some confusion regarding this requirement and makes reference to citations from the ENISA Revised Guidelines, the EECC and the Communications Regulation Act to support its contention. In this regard, eir states that "*As noted in the ENISA Technical Guidelines the consideration of socio-economic impact is relevant to determining the significance of an incident and whether reporting should be triggered. The European Electronic Communications Code also makes reference to this consideration in the context of determining significance thresholds in Article 40 but is silent on this category being a mandatory feature for every incident report. eir notes that section 11(2) of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 lists this as a feature in determining significance but also, in section 11(3) requires this Information to be Included in individual reports".*

98 eir considers that this raises questions of what it terms "proportionality" regarding whether providers have the required skillsets to perform such assessments, and whether the need for such assessments could have a negative impact on a provider's ability to report incidents in a timely manner. eir believes that the operation of incident reporting should be based on objective criteria and that considerations of the societal and economic impact should be inherent in the incident reporting thresholds in section 1 of ComReg's proposed decision instrument.

99 Instead, eir contends that ComReg should develop and publish a consultation on a draft guideline as to how the societal and economic impact should be assessed for inclusion in an incident report if the information of the impact of the incident on economic and societal activities is to be maintained as an obligation on providers.

100 NBI requested guidance regarding the impact of the incident on economic and societal activities as the content, the nature of the content and the detail to be reported to satisfy ComReg's requirements appears unclear to it.

101 NBI is also seeking clarification on the information requirement, "Date and time the incident occurred and its duration", and on the term "incident occurrence". NBI opines that security incidents are detected at a point in time, but the date and time of occurrence often predates detection of the security incident and can be unknown at the point of detection. NBI highlighted that identifying the date and time of a security incident occurrence within the reporting timelines proposed in the Consultation may not be possible or offer the required accuracy. This, in NBI's view, affects the accuracy and completeness of reporting to ComReg, duration of the incident and calculation of the absolute threshold.

102 NBI also raised queries with regard to information concerning any likely cross-border impact with another EU Member state. NBI specifically raised the status of Northern Ireland, and whether it is to be considered a Member State or, in light of the UK's decision to leave the EU, to be considered as outside the EU for the purposes of the Consultation.

3.7.2 ComReg's View

103 In relation to information on the economic and societal impact of an incident, this is required as part of a notification made to ComReg, pursuant to section 11(3) (d) of the Act, which provides that a notification made under section 11(1) shall (emphasis added) contain the information specified in paragraphs (a) to (g) of section 11(2). The initial report of the security incident should contain the items listed in section 11(3) (d) to the best of the providers knowledge at the time of reporting. ComReg understands that a full report at such an initial stage, will in the majority of cases not be possible. However, ComReg notes that further updates can be provided once the details of the incident become apparent. Such a flexible approach should not therefore impact a provider's ability to report incidents in a timely manner. However, a full report must, prior to its closure, contain all the required information as set out in the Act. Because this information is set out in the Act, there is no discretion but to seek it from the provider.

104 With regard to the views expressed in relation to an assessment of the economic and societal impacts, ComReg notes that this information category should capture at a high level, any economic and societal impacts arising from an incident that a provider is aware of or should reasonably be aware of. Given that the Act requires providers to include this information, ComReg at this time does not see any reason to develop or consult on guidelines as to how providers could carry out this assessment. ComReg further notes that section 6.2.3 and Annex A of the ENISA Revised Guidelines provides examples of potential economic and societal impacts arising from an incident. However, ComReg will keep this matter under review and may revisit this issue in light of experience gained.

105 In relation to the date and time of occurrence of a security incident and its duration, ComReg can clarify that, where the date and time of a security incident occurrence is unknown at the point of detection and initial notification, providers can provide a reasonable estimate, to the best of its knowledge at the time of reporting and stating any assumptions made. The provider can subsequently update this information as the details of the security incident become clearer. For the security incident duration, and regardless of the sub-categories affected (confidentiality, authenticity, integrity or availability), ComReg expects that the duration of the security incident can only be finally determined upon resolution of the security incident and the restoration of normal services and /or a return to a Business as Usual ("BAU") state.

106 Finally, and with regard to any cross-border impacts, ComReg notes that the United Kingdom of Great Britain and Northern Ireland (the "U.K.") is not regarded as a 'third country' under section 19 of the Act. In relation to cross-border issues affecting the security of networks and services with the U.K., ComReg will continue to work closely with colleagues at Ofcom[57] , as required.

107 ComReg notes that the European Commission has a potential role in setting out the circumstances, format and procedures applicable to notification requirements under Article 40(2) of the EECC. Article 40(5) of the EECC provides that: *"The Commission, taking utmost account of ENISA's opinion, may adopt implementing acts detailing the technical and organisational measures referred to in paragraph 1, as well as the circumstances, format and procedures applicable to notification requirements pursuant to paragraph 2. They shall be based on European and international standards to the greatest extent possible and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraph 1".* The European Commission has not yet promulgated such implementing acts, but ComReg will of course take account of such implementing acts in relation to Article 40 if and when they are made.

[57] The Office of Communications.

3.8 Reporting Portal

108 In the Consultation, ComReg set out that going forward, all providers[58] will be required to use ComReg's e-licensing incident reporting portal to notify it in the event of a security incident with a significant impact on the operation of networks or services.

3.8.1 Views of Respondents

109 NBI contend that the e-licensing incident reporting portal and the incident reporting process should have the capability to enable service providers to report a security incident that is categorised under more than one category (that is: confidentiality, authenticity, integrity or availability) without having to make any duplication.

110 Microsoft posited that it would be efficient if ComReg could provide a streamlined reporting mechanism, to allow providers to report an incident by identifying it as either an initial or final notification, so as to eliminate the need for unnecessary additional reporting or resubmitting previously reported information, after fully reporting an incident as resolved or completed.

111 Vodafone suggested that, at the next update, ComReg provide a simple template for storms related reporting to enable service providers to maintain a tracker of 10am and 4pm storm reports. Vodafone further opined that mandatory fields, i.e., customer numbers, should only be compulsory for the final report stage, along with information regarding root cause analysis and remedy actions.

112 eir requested confirmation that the incident reporting template will be consistent with ComReg's proposed decision and any redundant requirements will be removed.

[58] For the avoidance of doubt, this includes Providers of, ECN, ECS, and NI-ICS.

3.8.2 ComReg's View

113 ComReg confirms that a security incident may feature more than a single category (confidentiality, authenticity, integrity and availability). Therefore, providers should use any or all of the categories that accurately describe the security incident in progress.

114 All information known at the time of the initial report (i.e., within 24 Hours) should be entered into the incident reporting portal, which was introduced in 2019. Further data can then be entered as it becomes available by updating the portal. Note that the data is editable until the Incident Report is completed, and it will not be overwritten unless the provider chooses to actively do so, such as during a correction.

115 Regarding storms, these are considered to meet with the definition of a security incident, under section 5 of the Act, as they affect networks availability at a given time. Storms will typically affect all providers in the affected area to some extent, depending on, but not limited to, any back up power facilities, redundant transport (backhaul) link technology; and the adaptability of access technologies in use by each provider. In order to streamline reporting, providers should select storms on incident type when reporting an incident on e-licensing Portal.

116 To enable ComReg, the National Emergency Co-ordination Group ("NECG") or DECC to assess the impact of a storm in a given area it is important that providers provide the most reasonable estimate of the number of users, or sites and locations affected by the storm that they can. This can be updated when more information is to hand, but an early estimate with the sites and locations allows ComReg to coordinate with the NECG, so that NECG and other state agencies can prioritise assistance as necessary.

117 ComReg will update the e-licensing Portal and the Guide to its incident reporting portal (ComReg Document No. 19/98) to take account of changes made following this Response to Consultation and Decision. ComReg is updating the e-licensing Portal in order for it to have the additional functionality to permit the selection of multiple categories for each security incident. As detailed above and previously in paragraph 116, information such as the number of sites affected, and customer numbers will necessarily remain a mandatory requirement.

118 Following the update, there will be three (currently there are two) overall types of security incidents from which the provider will select the appropriate type; these will be as follows: Isolated, Storm and Malicious. This latter category is intended to catch security incidents including but not limited to those caused by the malicious actions of a third party, whether of a cyber or other origin (i.e., arson, physical damage etc.). These modifications and the use of the pre-existing incident reporting portal should ameliorate the issue raised earlier by Sky in paragraph 56 regarding the lead in time required.

3.9 Security Incident Reporting and Timescales

119 In the Consultation, ComReg noted that where a security incident has a significant impact on the operation of an ECN or ECS, a provider must report to ComReg as soon as possible and within the first 24 hours of the initial incident.

120 To determine the urgency for reporting the security incident, ComReg highlighted that providers should employ the criteria outlined by ComReg at paragraph 124 of the Consultation which stated that, 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.

121 Also, in the Consultation ComReg noted that initial reports should contain all of the information available at the time the report of the security incident is made. This should include as a minimum[59]:

- 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 in the Consultation;
- Details of the number of the user base impacted;
- The service impacted;
- An indication of the likely cause; and

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

- If possible, the expected duration of the incident.

122 Furthermore, ComReg highlighted the timings of and the required information for the subsequent updates. ComReg noted that existing reports must be updated within 72 hours, and a comprehensive update must be provided within 4 weeks of the first reporting of the incident.

3.9.1 Views of Respondents

123 NBI suggested that, in its view, a 72-hours timeframe is more appropriate for initial reporting of a security incident by service providers to ComReg. NBI stated that it is concerned by the very short 24-hour reporting timeline that is being proposed and contends that the 24 hours is too short a time window to provide a security incident report, that meets with the requirements set out in ComReg's Consultation, that the reporting of security incidents will be incomplete and/or unintentionally inaccurate as a result of "*rushed*" reporting within the 24-hours timeline and, as a consequence, it is possible that submitted reports will require corrections and/or revisions.

124 Microsoft contends that service providers should be allowed up to 72 hours to report a security incident with a significant impact and that the reporting window should begin after the service provider determined that a security incident breaches the threshold for significance. Microsoft also contends that the reporting requirements should reflect the incident response and that service restoration must be the priority. Microsoft further opines that gathering information from engineers for regulatory reporting during an active outage detracts from the incident response, particularly with a 24-hour deadline. In Microsoft's view, imposing an obligation on service providers to provide an initial report in advance of 72 hours following confirmation carries what it terms a significant risk for both the reporting entity and the public authorities who could consume and action such potentially erroneous or heavily qualified information. Microsoft is also of the view that for non-network-based services, it may take time to gather enough information to determine that the reporting threshold has been met.

125 Microsoft suggested that additional reporting should only be required if all the relevant information for a security incident was not initially available. Microsoft contends that the relevant information of a security incident would include the information set out in section 3 of ComReg's proposed decision, along with an explanation of the measures taken by the service provider to prevent recurrence of such a security incident.

126 Microsoft further contends that where a detailed final report is required, it should be provided only after the investigation of the security incident is complete or within six months of confirmation that the security incident is significant, *"whichever is sooner"*. This would, it believes, allow providers to investigate and provide accurate reports. Further, Microsoft suggested that ComReg should allow service providers to unilaterally defer the deadline if internal investigations are still ongoing or to amend final reports if the providers investigations are incomplete or the providers analyses change, noting that investigations for complex security incidents could extend for many months.

127 Virgin Media refers to section 11(1) of the Act, which in its view does not specify an initial incident reporting time frame of 24 hours. In its view, if there is to be a 24-hour reporting obligation on providers, this should only be for an initial report, as the first 24 hours of an incident is a period where the focus would be on evaluating and resolving the incident and information regarding the incident may not be fully known. Virgin Media agrees that an initial report of a significant incident could be reported to ComReg, but it noted that it may not be possible to provide all the information proposed in the Consultation in the initial report. Rather, Virgin Media believes that it would be more practical to have some flexibility around the minimum information requirement, so that the information that is available can be provided in the initial interim report and other information including, likely cause can be provided subsequently as further facts emerge.

128 Sky is of the view that reporting a significant incident should be done as soon as reasonably possible. Sky sought clarification in relation to the reporting of a loss of availability incident, that includes the duration of the incident, can only be made once the incident has been resolved and the outage has been rectified. Sky also opined that; the reporting of a cyber-incident impacting confidentiality, integrity, and authenticity can only be reported once the provider becomes aware of the incident.

129 Sky is also of the view that it may not be possible to determine when a security compromise resulting in a reportable incident occurred. Sky therefore suggested an alternative approach, whereby service providers notify ComReg as soon as they become aware of a cyber-compromise with a significant impact that affects confidentiality, integrity and authenticity. Sky believes that the initial notification would be limited with just initial information related to the breach. Service providers could, in its view, follow up subsequently and provide more details once the security incident has been managed and finally resolved.

130 Three referenced paragraph 123 of the Consultation, which sets out that *"...ComReg operates between 09H00 and 17H30 and does not operate a 24Hour or 'on-call' type service..."*. Three requested that ComReg review the necessity for the incident reporting timelines being expressed in "clock-hour" terms as ComReg is not available to take any action to any reports outside the working hours. Three maintain that in an out of hours situation when non-operational staff may not be at work and ComReg is not available to take any action on foot of the reports, the burden of meeting the "clock-hours" target will fall to the resources primarily tasked with focussing on incident management and resolution.

131 NBI also requested clarification with regard to the status of the criteria set out in paragraph 124 in the Consultation, as to whether this criteria is provided as a guideline for determining security incidents of significant impact or for determining all security incidents.

3.9.2 ComReg's View

132 Under the Act, an initial report from a provider, of a security incident, must contain the items listed in section 11(3) (a to g) of the Act, inclusive, and to the best of the operator's knowledge at the time of reporting. ComReg recognises that a full report at this time is impractical and further updates can be given once the details of the security incident become apparent. The reporting timescales are as follows:

- Initial Report: Within 24 Hours;
- First Update: (Detailed Report[60]) within 72 Hours;
- Other Updates: Every 72 Hours as necessary; and
- Root Cause Analysis ("RCA") and Closure Report: within 30 Calendar Days of the first report of the incident to ComReg, unless otherwise agreed in advance with ComReg.

[60] This should include all details known at the time of the update.

133 First, there are several advantages in ensuring that security incidents are reported promptly and in a clear and coherent manner across MS. The standardisation of reporting, using the ENISA Revised Guidelines, where possible, allows for CAs, such as ComReg, to: examine the types of security incidents that have had significant impact, their frequency, their root causes, and the necessary mitigation methods.

134 Second, in the particular case of a security incident that has a cross-border impact, it allows for a timely coordinated and cohesive response across MS. Allowing for the possibility of limiting the further spread of the security incident by alerting other CAs and providers within other MS to, the details of the security incident, the best mitigation and prevention methods.

135 Third, timely reporting gives ComReg an organisational awareness of significant incidents which can facilitate its other statutory functions such as managing any enquiries accurately and effectively, coordinating or sharing information, where required, with other State Agencies.

136 Furthermore, when these security incidents are reported to ENISA it allows for a degree of peer review and discussion in the ENISA European Competent Authorities for Secure Electronic Communications ("ECASEC") working group. The learnings from such a review can lead to an overall improvement in knowledge of the type of security incident and can subsequently lead to the revision of the relevant security measures where necessary.

137 Finally, ComReg has chosen the appropriate and proportionate timescales for reporting, not only to fit in with the Revised ENISA Guidelines but also to be broadly in accordance with the future requirements of relevant EU legislation[61] once they are transposed. The initial reporting of a significant security incident should be within 24 Hrs of the provider becoming aware of the incident.

[61] NIS 2 Directive and CER Directives: DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive); and Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC respectively

138 For clarification, if the full circumstances of the security incident – the information required under section 11 of the Act, and its Root Cause Analysis are available within 24 Hours of it being discovered then the security incident report may be closed at this stage.

139 Regarding the duration of security incidents, regardless of the sub-categories affected (confidentiality, authenticity, integrity or availability), ComReg would only expect that the duration of the security incident can be determined upon resolution of the security incident and the restoration of normal services, or a Business as Usual ("BAU") state.

140 In clarification of a respondent's query on when security incident reports can be made, other than the case in paragraph 143 below, the initial report must be made within 24 hours of the security incident being detected by the provider. At this time, ComReg would naturally expect the primary focus of the provider concerned to be on resolving the security incident. More details can be given by the 72-hour report, or further updates as necessary.

141 In relation to amending final reports, ComReg would note that as the final report will have been submitted and the security incident will have been marked as closed, it will not be possible for service providers to make any further changes. However, should it be required by a service provider, ComReg may, in exceptional circumstances and at its sole discretion, reopen the security incident to allow the service provider to make any corrections or to submit further information.

142 ComReg confirms that Normal Business Hours apply, in ComReg's case this is 09H00 until 17H30, Monday through Friday inclusive, excluding both Bank and Public Holidays. Regarding this, ComReg would like to clarify that when reporting a security incident regardless of if its during normal business hours or out of working hours, the reporting should be made through ComReg's e-Licensing portal.

143 Regarding the NBI requested clarification on the criteria listed in paragraph 124 of the Consultation, ComReg notes that the initial reporting to ComReg before the 24 hours initial reporting deadline would be justified, for example, but not limited to, where the provider was concerned that the severity of the security incident was rapidly increasing, poses a risk to other providers ECN or ECS, assistance is needed from other State Agencies, is gaining coverage in the media, or poses a risk to ECN and ECS in other Administrations including but not limited to other Member States. A valid and recent example of this, is where a NI-ICS provider's service fails and causes knock on congestion to providers of ECN[62].

[62] i.e., the Facebook group outage[62] of 04 October 2021.

3.10 Other Matters Raised

144 This part addresses some other matters raised by the respondents, which are beyond the scope of the Consultation questions.

3.10.1 Views of Respondents

145 Vodafone commented on ComReg's use of the data provided in incident reporting and noted that in its opinion it was concerned that such data could be used out of context. In this regard Vodafone highlighted an extract from ComReg's Customer Charter consultation which states that "*In 2020, more than 50.7 million user hours were reported lost to incidents such as software bugs, poorly implemented software updates, hardware failures and weather events causing power outages".* Vodafone opined that this may mislead customers and affect their perception of the actual quality of service. However, Vodafone observed that in its opinion most customer hours were lost in network incidents related to power outages, which it contends are beyond its control and that in the majority of cases service providers mitigate through the provision of battery back-up.

146 eir requested clarification on whether ComReg will act as a Single Point of Contact ("SPoC") for the reporting of all incidents or whether providers will be required to continue reporting some incidents to the National Cyber Security Centre (the "NCSC") or the Computer Security Incident Response Team ("CSIRT") in addition. eir noted that a SPoC would seem to be a more pragmatic and efficient approach.

147 Three notes that ComReg's Consultation does not set out an assessment of how the current ComReg proposals interact with reporting obligations under other adjacent and relevant regulations and Three contends that in its view there is a potential for an increase in overlapping reporting to different supervisory authorities on the same security incident resulting from expanding the scope of the incident categories (Confidentiality, Integrity and Authenticity), with the reportable incident categories under the NIS and the e-Privacy Directive[63]. Three states that the e-privacy Directive already requires reporting of a high volume of usually relatively minor incidents. Furthermore, Three opines that ComReg should only impose additional reporting requirements where necessary unless there is a clear requirement for parallel reporting interfaces into multiple Supervisory Authorities for the same incident so that Service Providers can focus on incident resolution rather than reporting administration.

148 Imagine notes the requirements for reporting security incidents in relation to *"Confidentiality, Integrity, Authenticity or Availability"* and *"related services offered by, or accessible via those electronic communications networks or services[64]"*. Imagine contends that the provider should only be required to report incidents that are directly related to the networks and services under the providers' control. Therefore, Imagine asserts that the provider should not be required to report incidents related to any third party services that are accessible over the top ("OTT") of the provider's network, such as NI-ICS.

149 eir noted sections 8 to 10 in ComReg's proposed Decision Instrument, and that these sections relate to how ComReg will address information required by the European Commission, Other NRAs and ENISA and questioned the validity of these sections applying to providers.

150 Virgin Media is of the view that it would be helpful if ComReg was to host a workshop following ComReg's Decision so as to update all service providers of any revised obligations, including reporting timeline and the process for reporting.

[63] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 as amended.
[64] As provided in the definition of security incident in section 5 of the act.

151 Imagine referred to paragraph 111 of the Consultation, stating that it agrees with the reporting requirements of security incidents impacting Confidentiality, Integrity, Authenticity or Availability. However, Imagine contends that ComReg's commentary seemed, in its view, vague and/or open to interpretation. In its view, Imagine considers that further work is required to bring clarity to the piece. This could for example take the form of industry workshop(s) and perhaps with a brief to create more detailed *"guidelines/templates using the examples provided within Annexes A and B of the ENISA Technical Guideline*." Imagine opines that this would facilitate clear, consistent, and practical reporting across all providers, it also opines that this would address issues such as:

- The exact scope of incidents within each category.
- How to consistently detect and quantify such incidents.
- How to relate certain incidents to time (e.g., the start and end of an incident related to misuse of authentication credentials).
- How to ensure consistent reporting by operators and different types of operators or networks.

3.10.2 ComReg's View

152 ComReg notes Vodafone's view on the cause of security incidents and, there is no question that power outages contribute to network incidents, but this is just one contributory factor of many. Only earlier this year, ComReg published Document 23/59, "*The Economic and Societal Impacts of Network Incidents*", a foundational study by DotEcon and Analysys Mason.

153 The study found that users reasonably expect to be able to access services with minimal disruption. However, security incidents that impact the experience of the end user can occur for a variety of reasons and include, in no particular order of frequency of occurrence:

- weather and natural phenomena: storms, wind, high temperatures, fog, snow and ice, and solar storms;
- third party damage: including damage to physical infrastructure, vehicular impact, fibre cuts and cable damage;
- malicious acts: Telephony Denial of Service ("TDoS") attacks, Distributed Denial of Service ("DDoS") attacks, cable theft, vandalism, 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

- system failures including but not limited to hardware and software failure; insufficient redundancy; inadequate procedures and deficient supervision of both own and outsourced staff.

154 While ComReg notes that the context of the comments in the consultation on the Customer Charter[65] may not have been fully given, it can confirm that the three largest outages affecting ECN and ECS of the year in question (2020), were caused by what ENISA categorise as 'system failures'[66] Furthermore, ComReg notes that this is a common factor in outages throughout MS reporting to ENISA and is consistent across years and not unique to Ireland[67].

155 In relation to the points raised by eir and Three, (SPoC, parallel reporting and cooperation with other agencies of State, respectively) notwithstanding, ComReg offers the following response:

- First, ComReg has implemented the incident reporting portal, as part of the e-licensing portal, to make the reporting of security incidents, as per the requirements of the Act, less onerous – it's a familiar environment;

- Second, there may be separate reporting processes for incidents in various pieces of legislation, the Consultation process is only concerned with the reporting of security incidents under section 11 of the Act;

- Third, the ability of ComReg 'for the purposes of exercising its functions' under Part 2 of the Act, to cooperate and consult with certain defined statutory bodies and other MS CAs, is outlined under section 16 of the Act; and

[65] Proposals for Implementing a Customer Charter (Consultation) – ComReg Document 23/14 – https://www.comreg.ie/?dlm_download=proposals-for-implementing-a-customer-charter
[66] which includes: software failure and bugs; hardware failure, and configuration issues, etc.
[67] See p. 26 of this document.

- Finally, ComReg will keep the concept of a SPoC under review in light of any new legislative developments.

156 In relation to providers with very limited or no control/visibility over the impacted services or networks, ComReg confirms that the obligation is on the wholesale providers of ECN and ECS to report the security incident to ComReg. In circumstances where the security incident impacts a retail providers own ECN or ECS equipment then the retail provider must report the security incident to ComReg. Similarly for NI-ICS providers, where the service provided is impacted by a security incident affecting its own equipment (such as but not limited to, routers, gateways, servers, firewalls, data centres etc.) then the NI-ICS provider itself is responsible for making the incident report.

157 Furthermore, where a provider of traditional ECN or ECS, or NI-ICS has its service or network affected by a security incident that affects a third-party provider of a service to it, then the provider of ECN, ECS or NI-ICS shall report the security incident to ComReg.

158 Regarding eir's view on the validity of sections 8 – 10 in ComReg's proposed Decision Instrument (which set out what is required by providers). ComReg concurs that these sections, relate to how ComReg will address information required by the European Commission, Other NRAs and ENISA, is not appropriate for inclusion in the Decision Instrument. Therefore, ComReg will remove these sections of the Decision Instrument.

159 Regarding the request by some respondents for workshops, on incident reporting, ComReg believes that a workshop at this moment in time is premature, as the Consultation process and modifications to the subsequent Decision Instrument have sought to clarify the issues raised by respondents. ComReg would prefer to reserve such an option for future legislative or technological changes.

3.11 Conclusion

160 Having carefully considered the submissions, the points made therein and other relevant information, the above sections of this chapter set out ComReg's views in relation to the matters raised by the respondents, along with several clarifications.

161 ComReg remains cognisant of the guidance provided by Recital 95 and the definition of NI-ICS in Article 2 of the EECC. As such, ComReg confirms that providers of NI-ICS will be required to report all significant security incidents to ComReg but will only be subject to the absolute threshold for a significant security incident within the jurisdiction of Ireland (i.e. is equal to or exceeds one million (1,000,000) user hours).

162 As detailed above, ComReg noted that, NI-ICS providers will not be required to base their calculations, when determining the significance of a security incident, on the NUB, or the provider's total user base. Instead, and as highlighted above, NI-ICS providers should report a security incident to ComReg, if the product of the duration of the incident and the estimated number of users affected is equal or exceeds sixty million (60,000,000) user minutes i.e., one million (1,000,000) user hours in the jurisdiction of Ireland.

163 In relation to the Decision instrument, and having taken account of the useful responses received, ComReg has made some amendments, as follows:

- Removing sections 8 – 10, which relate to how ComReg will address information required by the European Commission, Other NRAs and ENISA, that were set out in the proposed decision instrument, considering that the Decision Instrument is addressed to service providers.

- Removing the NI-ICS National user base calculation rule that was set out in Section 2 Part III in the proposed decision instrument, considering the concerns raised by respondents in relation to the NI-ICS NUB calculation rule and noting the absence of NI-ICS user base figures in ComReg's QKDR.

- Modifying Section 2 in Part III (National User Base Calculations) of the Decision instrument to clarify the components of the National User Base.

4 Regulatory Impact Assessment ("RIA") on Reporting Thresholds for Security Incidents

4.1 Introduction

164 In Chapter 3 of the Consultation, ComReg set out its draft RIA on the reporting thresholds for providers to report security incidents to ComReg. Having considered the impacts on stakeholders, competition and consumers, ComReg was of the preliminary view that it would be appropriate to align the reporting thresholds with the quantitative thresholds set out in the ENISA Revised Guidelines. Having considered the views of respondents to Document 23/36, this chapter sets out ComReg's final RIA on the reporting thresholds for security incidents.

4.2 RIA Framework

165 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.

166 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 followed in the Consultation and this RIA should be read in conjunction with, the Consultation, Response to Consultation and Decision Document. The final RIA considers the responses received to the Consultation.

167 In conducting the RIA, ComReg has regard to the RIA Guidelines [68], while recognising that regulation by way of issuing decisions, for example imposing obligations or specifying requirements in addition to promulgating secondary legislation, may be different to regulation exclusively by way of enacting primary or secondary legislation.

168 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.

4.3 Structure for the RIA

169 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.

170 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.

4.4 Identification of Stakeholders and Approach to Steps 3

[68] 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

and 4

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

172 In this RIA, stakeholders fall into two main groups:

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

173 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.

174 Of themselves, the RIA Guidelines and the Ministerial Policy Direction on Regulatory Impact Assessment[69] 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[70];
- contribute to the development of the internal market[71];
- promote the interests of users within the Community[72];
- 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[73]; and

[69] Ministerial Direction dated 21st February 2003
[70] Section 12 (1)(a)(i) of the 2002 Act.
[71] Section 12 (1)(a)(ii) of the 2002 Act.
[72] Section 12(1)(a)(iii) of the 2002 Act.
[73] Section 12(1)(b) of the 2002 Act.

- promote efficient investment and innovation in new and enhanced infrastructures[74].

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

176 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.

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

4.5 Step 1: Identify the Policy Issues & the Objectives

4.5.1 Policy Issues

178 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.[75]

[74] 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”).
[75] 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.

179 Users reasonably expect to be able to access the services provided over networks with minimal disruption. However, security 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 security 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
- 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.[76]

180 ECN and ECS providers are obliged to notify ComReg when a security 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 security incidents to its attention. The sections below summarise ComReg's current reporting thresholds and the notable developments that have occurred since.

4.5.2 ComReg's Current Thresholds for Reporting Security

[76] Software failures, human error and storms were the causes for most of the user hours lost in 2022. See ComReg Document 23/60.

Incidents

181 Regulation 23(4)b of the Framework Regulations provided 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.

182 ComReg's previous approach to management of reported security incidents and the coordination of its response to these incidents, was set out in Reporting & Guidance on Incident Reporting & Minimum-Security Standards, ComReg Document 14/02. This outlined the appropriate thresholds for reporting security incidents and the requisite timing for submission of these reports. The thresholds and process for reporting were previously provided as guidance to undertakings providing public communications networks or publicly available electronic communications service. ComReg's approach took into consideration the Framework Regulations[77] and the guidance provided by ENISA at that time in its document Technical Guideline on Reporting Incidents.[78]

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

(i) the threshold to trigger an ENISA report by ComReg would 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 had the additional advantage of enabling ComReg to monitor the performance of an operator in respect to the management of appropriate technical and organisational measures, to ensure that it managed the risks posed to the integrity and security of networks and services.

[77] Regulation 23 and Regulation 24 of S.I. No. 333/2011 European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011.
[78] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0

184 The previous 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.

4.5.3 The European Electronic Communications Code and its Transposition into Irish Law

185 On 20 December 2018, the EECC entered into force and is transposed in the State by the Act, and by the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022. Articles 40 and 41 of the EECC replace Article 13(a) and 13(b) of the Framework Directive (amended)[79] and place a greater emphasis on consumer protection and security of electronic communications.

186 Article 2(21) of the EECC explicitly 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"*

187 It should be noted that this new definition of "security of networks and services" is transposed by section 5 of the Act explicitly includes authenticity, integrity, confidentiality and availability. This has important implications for the scope of a security incident, which is now considerably more broadly than was previously the case. Section 5 of the Act defines a security incident 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."*

188 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, is transposed in section 11(1) of the Act which states:

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

(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.

189 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.

190 Article 40, as has been 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.

191 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.

4.5.4 Applicable Thresholds for NRA Reporting Significant Security Incidents to ENISA

192 In March 2021, ENISA published technical guidelines (ENISA Revised Guidelines) on reporting security incidents, in light of the obligations contained in the EECC[80]. 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.

193 Section 6 of the ENISA Revised Guidelines sets out scope and thresholds for when security 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[81] 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

194 ENISA advocates that quantitative thresholds should consist of two parts.

Relative Threshold

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

---

[80] 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

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

- 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%.

196 ENISA further advocates that NRAs should report security incidents which have an impact on the **confidentiality**, **authenticity** and **integrity** using the relative threshold. In such instances, a security 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

197 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**[82] and advises that a security 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.

[82] Defined in Article 2 of the EECC.

Qualitative Thresholds

198 While quantitative thresholds are clearer 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 a security incident. Specifically, ENISA suggests that geographical spread and the economic and societal impacts associated with a security incident should be considered. ComReg notes that this is in keeping with the information requirements contained in section 11 of the Act.

Objectives

199 ComReg aims to design and carry out its review of the thresholds for reporting security incidents in accordance with its broader statutory objectives as above in Section 4.4 of this RIA.

200 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.

4.6 Step 2: Identify and Describe the Regulatory Options

201 The previous thresholds for reporting 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. In this Consultation Process (ComReg Document 23/36 and this Response to Consultation 24/NN) ComReg has evaluated 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 was to maintain the status quo** and extend the use of the existing reporting requirements under Document 14/02. ComReg's previous approach in Document 14/02 was to set quantitative numeric thresholds based on the number of affected users and the duration of the incident.

202 In relation to other options, ComReg notes that the approach advocated by ENISA is to consider both quantitative and qualitative thresholds to determine whether a security incident should be reported to it and the European Commission (i.e., annual summary reporting). The quantitative thresholds are those set out in section 4.5.4 above ("Quantitative Thresholds"). Therefore, **Option 2** is to align the quantitative thresholds with those in the ENISA guidelines.

203 An alternative option would have been 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., security 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 applied in Document 14/02. However, ComReg notes that these thresholds were set over eight years ago, while the ENISA guidelines have been updated to account for technological developments in the intervening period. Furthermore, ComReg observed that circa 75% of the security incidents reported under Document 14/02 would be captured by the revised ENISA Guidelines in any event.

204 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 security incidents. Furthermore, ComReg observes that most of the security incidents reported have also exceeded the thresholds for inclusion in ComReg's reporting to ENISA.

205 ComReg is therefore of the view that an approach which uses defined quantitative values for providers to report security incidents is effective and provides clarity to providers. Consequently, ComReg does not propose to include qualitative approaches at this time, other than as information to be reported to ComReg as part of a security incident report from a provider. ComReg reserves the right to revisit this matter in the future following future technology and legislative revisions. Further, ComReg notes that any approach does not preclude providers from voluntarily reporting security incidents to ComReg should they consider them to be of importance. ComReg notes that providers have in the past freely reported security incidents to ComReg that while falling below the thresholds, were considered by the operator to be of sufficient interest.

206 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.

4.7 Impact on Stakeholders

Identification of Stakeholders

207 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.

208 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

209 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.

210 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**[83] are stricter 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).

[83] 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.

211 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[84] are provided in Section 1.2 and providers should report these security incidents, if the number of users affected is more than 1% of the national user base of that particular service.

212 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 security 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. Having considered the responses to the Consultation, ComReg is of the view that providers would prefer Option 2.

Impact on Competition

213 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 the 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 reporting security incidents is beneficial (in and of itself) and consequently to promoting competition.

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

214 ECN and ECS are fundamental platforms for the delivery of economic and societal welfare. As dependence on these networks increases; the impact of security 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.

215 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 previous EU Telecoms Framework and 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. The reporting of security incidents plays an important role in these efforts, as it contributes to improving both providers' and NRAs' knowledge of the type and prevalence of security incidents.

216 An effective security 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 practice and processes. An reporting process for security incidents provides valuable transparency to society and allows learning from security incidents, systematically improving the security and operation of ECN and ECS in the electronic communications sector.

217 There are some underlying reasons as to why network reliability may be underprovided by competition between network providers. These are outlined in ComReg's report on the "*Economic and societal impacts of Network Incidents*"[85].

[85] ComReg Document 23/59

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

219 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 security 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. The reporting of security incidents is one part, but an important part, of a larger effort to manage security incidents and emergencies, and to protect network infrastructure.

220 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 security incidents improving the resilience of networks, helping mitigate the potential spread of security incidents; and

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

221 Option 1 already provided a level of security incident reporting in relation to the availability of networks. However, such security incident reporting was 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 security incidents that relate to confidentiality, authenticity, and integrity and could lead to under provisioning of such factors.

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

Impact on Consumers

223 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.

224 The changing work pattern, undeniably 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.[86] 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 a ComReg study on the economic and societal impacts of network incidents revealed that, of the respondents who reported experiencing network outages, approximately a quarter indicated that remote working was affected.[87] 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 security incidents will fall within the scope of national reporting than heretofore. 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.

225 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.[88] These reporting requirements are provided for under Option 2 but not under Option 1 and therefore, ComReg is of the view that consumers would prefer Option 2.

[86] 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

[87] The Economic and Societal Impacts of Network Incidents Study | Commission for Communications Regulation (comreg.ie), ComReg Document No. 23/59a

[88] See ComReg Document 21/09

4.8 ComReg's Preferred Option

226 This RIA considered 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).

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

5 Next Steps

228 Following the publication of this Response to Consultation and its associated Decision Instrument D08/24, ComReg will publish the non-confidential responses received from respondents and will implement the changes required by the Decision Instrument to the e-licensing incident reporting portal.

229 Furthermore, and as stated previously ComReg will review the requirements for incident reporting as technology and legislative changes require.

Annex: 1 Legal Basis

A 1.1 Legal Basis

A 1.2 ComReg is 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[89];
- contribute to the development of the internal market[90];
- promote the interests of users within the Community[91];
- 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[92]; and
- promote efficient investment and innovation in new and enhanced infrastructures[93].

A 1.3 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. It entered into force on the third day following its publication in the Official Journal of the EU ("OJEU") (20 December 2018). Relevant provisions of the EECC have been transposed in the State primarily by means of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 ("the Act"), and by means of the European Union (Electronic Communications Code) Regulations 2022 ("Code Regulations").

[89] Section 12 (1)(a)(i) of the 2002 Act.
[90] Section 12 (1)(a)(ii) of the 2002 Act.
[91] Section 12(1)(a)(iii) of the 2002 Act.
[92] Section 12(1)(b) of the 2002 Act.
[93] 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").

A 1.4 Section 11(1) of the Act provides that: “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”. [94]

A 1.5 Article 40(2) of the EECC set 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 is now transposed in section 11(2) of the Act. This detailed list of parameters is new compared to the previous notification requirements set out in Regulation 23 of the Framework Regulations (now repealed), which transposed Article 13a of the Framework Directive[95].

A 1.6 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.

A 1.7 A further new element of the security provisions of the EECC, now transposed in the Act, is that the notification requirement now applies to NI-ICS. It should be noted that the section 11(1) notification requirement applies to publicly available electronic communications services, and Regulation 2(1) of the Code Regulations defines “electronic communications service”, of which interpersonal communications service is one type of ECS.

[94] This transposes Article 40(2) of the EECC.
[95] Directive 2002/21/EC as amended by Directive 2009/140

A 1.8 Article 2(7) of the EECC defines “number-independent interpersonal communications service” as meaning “an interpersonal communications service[96] 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”.

A 1.9 Recital 95 of the EECC states the following in relation to NI-ICS and security: “Given the growing importance of number-independent interpersonal 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 do not exercise actual control over signal transmission.”

A 1.10 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.

[96] For background on how the EECC treats interpersonal communication services generally, Recital 18 is useful.

A 1.11 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.

A 1.12 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.

A 1.13 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.

A 1.14 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 Decision Instrument: D08/24; Replacement of ComReg Document No. 14/02

Decision

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

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

"Availability"[98] 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;

[97] (ISO/IEC 27000:2018), (see page 12 of the ENISA Revised Guidelines, footnote 9)
[98] (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 6)

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

"Confidentiality"[99] 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" [100] 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" has the meaning assigned to it in the 2023 Act;

"security" has the meaning assigned to it in the 2023 Act;

"security incident" has the meaning assigned to it in the 2023 Act; 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 (ComReg 15/136R3) as amended from time to time; and Commission Document 24/23 of which this Decision Instrument forms a part.

[99] (ISO/IEC 27000:2018) (see page 11 of the ENISA Revised Guidelines, footnote 7)
[100] (ISO/IEC 27000:2018) (see page 12 of the ENISA Revised Guidelines, footnote 8).

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.24/23 to which this Decision is attached;

PART III – THE DECISIONS

ComReg hereby makes the following decisions:

Reporting Thresholds for Significant Incidents

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

(a) Where the percentage of the national user base affected and the duration of the security 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 security incident greater than or equal to one million (1,000,000) User Hours[101] [102], has or is taking place; and

(c) where any security 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.

[101] User Hours is the product of the Number of Users affected and the Duration of the incident.
[102] providers of NI-ICS must report all significant security incidents to ComReg when they exceed the absolute threshold for a significant security incident within the jurisdiction of Ireland (i.e. it exceeds one million (1,000,000) user hours).

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 most recent Quarterly Key Data Report ("QKDR") or any equivalent successor document found on ComReg's webpage[103], as follows:

(a) Fixed services:

- For Fixed Voice, providers should use the value titled in the QKDR as " Total Fixed Voice Subscriber Lines" or any term that replaces "Total Fixed Voice Subscriber Lines" in the QKDR or equivalent successor document as may occur from time to time.

- For Fixed broadband, providers should use the value titled in the QKDR as "Total Fixed Broadband Subscriber Lines" or any term that replaces "Total Fixed Broadband Subscriber Lines" in the QKDR or equivalent successor document as may occur from time to time.

(b) Mobile Services:

- For Mobile Voice Communications, providers should use the value titled in the QKDR as "Mobile Subscriptions exc. MBB and M2M Total" or any term that replaces "Mobile Subscriptions exc. MBB and M2M Total " in the QKDR or equivalent successor document as may occur from time to time.

- For mobile internet access, providers should combine the values titled in the QKDR as "Mobile Voice and Data Subscriptions using 3G/4G/5G Networks" **and "**Mobile Broadband Subscriptions Total" or any terms that replace these in the QKDR or equivalent successor document as may occur from time to time.

- For Machine to Machine, providers should use the value titled in the QKDR as "Machine to Machine Subscriptions" or any term that

[103] Quarterly Key Data Report | Commission for Communications Regulation (comreg.ie).

replaces “Machine to Machine Subscriptions” in the QKDR or equivalent successor document as may occur from time to time.

Information Required for A Notification of any Security Incident

(3) Under the 2023 Act[104]; 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 the security incident, that is whether it is: Confidentiality, Integrity, Authenticity or Availability that is affected by the security incident;
(b) the providers’ name;
(c) the public electronic communications network or publicly available electronic communications services provided by it affected by the security incident;
(d) the date and time the security 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 security incident on economic and societal activities;
(j) the cause of the security 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 Security Incidents to ComReg

(4) Providers must use ComReg’s e-licensing incident reporting portal[105] to report significant incidents to ComReg.

Timing for Reporting A Significant Security Incident

[104] At section 11 (2) c, d and f, and section 11(3).
[105] https://www.elicensing.comreg.ie/

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

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

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

(d) For any significant security incident, ComReg must receive a comprehensive update within 30 calendar days of the significant security incident report that confirms the circumstances of the security incident:

- The duration of the security 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; and
- a Root Cause Analysis report for the security incident which at a minimum is to include the:
    - root cause summary statement for reported security incident;
    - event timeline which details the sequence of contributing events leading to the security incident;
    - description of impact to network infrastructure;
    - remedial timeline which details the sequence of actions taken to resolve the security incident;

- categorisation[106] of the security incident's root cause, including a justification for its categorisation;
- mitigation measures identified to prevent future occurrence of any similar security 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 security 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;

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

[106] 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.

PART IV– EFFECTIVE DATE

Decisions (1) to (7) 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

Annex: 3 National User Base Calculations

In the following tables, ComReg has set out the national user base calculations for Fixed and Mobile Services using the latest data from the QKDR. As set out in the Decision Instrument, providers must reference relevant figures in the most recent Quarterly Key Data Report ("QKDR") or any equivalent successor document found on ComReg's webpage at the time of the security incident.

Table 1 1: Fixed Service User Base Calculations Q4 2023

Reporting	Description	QKDR Metric	National User Base
Fixed Voice	The number of fixed voice subscriber lines	Total Fixed Voice (PSTN, ISDN and VOIP) Subscriber lines	**1,176,013**
Fixed Broadband	The number of fixed broadband subscriber lines	Total Fixed Broadband Subscriber Lines	**1,654,603**

Table 2 2: Mobile Service User Base Calculations Q4 2023

Reporting	Description	QKDR Metric	National User Base
Mobile Voice Communications	For mobile communications service, providers should use the number of active telephony Subscriber Identity Module ("SIM") cards based on the number of voice subscriptions	Mobile Subscriptions exc. MBB and M2M Total	**5,757,780**
Mobile Internet 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	providers should combine: • Mobile Voice and Data Subscriptions using 3G/4G/5G Networks **and** • Mobile Broadband (MBB) Subscriptions - Total	**6,113,373**
Machine to Machine Communications	Providers should use the number of subscriptions dedicated for Machine to Machine use.	Machine to Machine (M2M) Subscriptions	**3,593,307**