An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Network Incident Reporting Processes

Review and Subsequent Revision of ComReg Decision Instrument D08/24

Consultation

Reference:	ComReg 25/84
Version:	FINAL
Date:	05/12/2025

Legal Disclaimer

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

Content

Section Page

Annex

Table of Figures

Section Page

1 Executive Summary

1. The Commission for Communications Regulation ("ComReg") is the statutory body responsible for the regulation of the electronic communications sector in Ireland.

2. Section 11(1) of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, (No. 4 of 2023) ("the Act of 2023"), requires providers[1] to notify ComReg of any security incident that has had or is having a significant impact on the operation of the provider's Electronic Communications Networks or Services ("ECN" or "ECS").

3. Section 5 of the Act of 2023 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" [emphasis added].

4. Weather events such as storms can result in security incidents, where network infrastructure is damaged and/or the infrastructure which supplies electricity to the network elements is damaged, resulting in network and service availability and integrity being impaired.

5. In January of 2025, the country experienced a record-breaking storm – Storm Éowyn. The extent and scale of the storm caused significant impact across all sectors – not just the electronic communications sector, pushing current processes to their limits.

6. ComReg had a robust reporting system in place, following the making, in 2024, of its Decision Instrument D08/24 "Network Incident Reporting Thresholds" (The "Decision")[2]. ComReg's Decision sets out how providers of ECN/ECS report significant security incidents – including severe weather events such as storms.

7. Notwithstanding, and In light of its experience and assessment of reporting on the serious effects of Storm Éowyn, ComReg, informed by discussion with key stakeholders, has considered the potential improvements to its reporting

[1] Including Number-Independent Communication Services (NI-ICS).

[2] published together with ComReg's Response to Consultation on Network Incident Reporting Thresholds – ComReg document 24/23, https://www.comreg.ie/media/2024/04/ComReg-2423-D0824.pdf

processes that could now be introduced. ComReg's proposed actions provide a twofold basis for this consultation:

i. enhancement of the data requested from providers during significant security incidents – including severe weather events, for the purposes of ComReg's statutory obligations and as a consequence, improving ComReg's reporting of such events to the Department of Culture, Communications and Sport ("DCCS") – as required by legislation; and

ii. improvements to ComReg's reporting platform and processes, as a consequence of stakeholder feedback, including a review of the Decision, where appropriate.

8. In summary, this consultation proposes the following changes to the relevant reporting processes in order to address the learnings and experiences gained from Storm Éowyn:

    - Updates to the reporting templates for storm/weather related security incidents;
    - Adjusting incident reporting frequency and submission times;
    - Making explicit that the geographic area affected is integral to the significance of the security incident;
    - Improving the calculation methodology for estimating the number of mobile users affected by a security incident;
    - Making clear that further information may be required by ComReg under section 11 (3)g of the Act of 2023; and
    - Altering the mechanism for the cessation of regular reporting under the Decision for this type of security incident.

9. This consultation is without prejudice to any future developments in the legislative framework, including any regulatory changes brought about by the transposition of the NIS2 Directive[3]. This consultation is also without prejudice to the implementation of the Critical Entity Resilience Regulations[4].

[3] Directive 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.

[4] S.I. No. 559/2024 – the European Union (Resilience of Critical Entities) Regulations 2024.

2 Background Information

10. In April 2024, ComReg published a Response to Consultation on Network Incident Reporting Thresholds (“ComReg 24/23”) along with its Decision Instrument D08/24 (the “Decision”). The Decision replaced ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum-Security Standards).

11. The Decision sets out how, when and under what circumstances providers must report significant security incidents to ComReg, including storm and weather related security incidents as these can affect the availability and integrity of ECN/ECS.

12. The processes for the reporting of a significant security incident by providers of ECN/ECS – as outlined in the Decision, were rigorously tested during Storm Éowyn. Those aspects of the security incident reporting process that proved most challenging included the frequency of reporting, the information required by key decision makers and the threshold points at which reporting obligations were activated.

13. The purpose of this consultation is to review, enhance and augment the processes set out in the Decision (and as required by section 11 of the Act of 2023) in light of the valuable experiences and learnings gained through Storm Éowyn. This is intended to benefit all relevant stakeholders and ultimately consumers; improving both the alignment of understanding of reported information across stakeholders and the enhancement of the data gathered from service providers to facilitate response and resilience actions, pursuant to providers statutory obligations contained in section 11 of the Act of 2023.

14. In the aftermath of Storm Éowyn, ComReg was eager to discuss and share with industry its experiences and learnings regarding the security incident reporting process. ComReg engaged with the service providers who reported security incidents to ComReg during Storm Éowyn, participating in meetings facilitated by the Irish Business and Employers’ Confederation (“IBEC”)’s Telecommunications Industry Ireland (“TII”) at a multilateral level, but also bilaterally with each individual provider. These meetings were held with industry to benefit from their experiences in reporting on security incidents as a consequence of Storm Éowyn, which informed this consultation.

15. The premise of all such meetings – both multilateral and bilateral, was to get the first-hand experience of the providers who reported to ComReg during Storm

Éowyn, so as to best inform this review of the Decision. Some preliminary views expressed included:

i. The possibility of ‘double counting’ of faults if the proposed geographic areas was to become too granular;

ii. The need for disambiguation by using common definitions for related terminologies; and

iii. The suitability and practicality of Estimated Time to Repair (“ETR”).

16. ComReg has also engaged with officials at DCCS to best understand the information that it and other State agencies now require in light of their Storm Éowyn experiences, to support any future recovery effort that might be necessary. ComReg also notes the recent publication of the Communications Networks Sectoral Adaptation Plan 2025[5], in particular the Potential adaptative capacity-building actions documented in section 3.4.1.2 suggesting that *Service outage and network damage information data could be captured for analysis with existing historical records*[6].

2.1 The Act of 2023 and the European Electronic Communications Code (“EECC”)

17. The EECC[7] repealed and replaced the previous European framework governing the European telecommunications sector. The EECC is transposed into Irish law by both the Act of 2023 and by the European Communications Code Regulations 2022, S.I. No. 444 of 2022 (the “Regulations of 2022”).

18. Part 2 of the Act of 2023 gives effect to provisions related to both security and security incidents, as well as making several further provisions at national level in relation to enforcement and amendments to the Communications Regulation Act 2002 (the “Act of 2022”).

19. This Consultation process relates to the notification requirement for security incidents contained in section 11 of the Act of 2023.

20. Section 5 of the Act of 2023 defines a “security incident” as meaning: “any action that compromises the availability, authenticity, integrity or confidentiality of

[5] https://www.gov.ie/en/department-of-culture-communications-and-sport/policy-information/communication-networks-sectoral-adaptation-plan/

[6] Service outages affect the availability of EN/ECS, whereas network damage affect the integrity of the ECN/ECS, for example causing network congestion.

[7] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018.

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." This includes weather or storm related security incidents.

2.1.1 The security of networks and services is provided for in the Act of 2023

21. Section 6 of the Act of 2023 requires that providers shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services[8]. Section 6(2) of the Act of 2023, 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. Furthermore, section 6(3) of the Act of 2023 provides that in particular, measures, including the use of encryption where appropriate, shall be taken by providers **to prevent security incidents and minimise the impact of any security incidents on users and on other networks and services**, [emphasis added].

22. Section 11(1) of the Act of 2023 requires 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 ComReg in accordance with subsection (3) without undue delay.

23. Section 11(2)of the Act of 2023 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; and

[8] It should be noted that Regulation 92(1) of the Regulations of 2022 provides that: "A provider of voice communications services or internet access services shall, in the event of catastrophic network breakdown or in cases of force majeure, take all necessary measures to ensure the fullest possible availability of voice communication services or internet access services as the case may be provided over public electronic communications networks."

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

24. Section 11(3) of the Act of 2023 provides that a notification made under subsection (1) shall contain the following information in relation to the security 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**, (emphasis added).

25. Section 11(4) of the Act of 2023 provides that where a provider notifies ComReg of a security incident in accordance with section 11, it shall, as soon as practicable, notify ComReg when the security 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 security incident occurring in the future.

26. Section 11(5) of the Act of 2023 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 the European Agency for Cyber Security ("ENISA").

27. Section 11(6) of the Act of 2023 provides that 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 security incident or require the provider concerned to do so.

2.1.2 Implementation and enforcement

28. Implementation and enforcement is provided for by the following sections of the Act of 2023:

- Section 11(7) of the Act of 2023 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 of 2023;

- Section 11(8) of the Act of 2023 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

- Under section 14 of the Act of 2023, 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) of the Act of 2023, 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.

29. It should be noted that this consultation is without prejudice to any future developments in the legislative framework, including any regulatory changes brought about by the transposition of the NIS2 Directive. This consultation is also without prejudice to the implementation of the Critical Entity Resilience Regulations.

30. It should be noted for completeness that if there is any apparent, or unintended, conflict between a successor Decision Instrument to Decision Instrument D08/24, and any provision of the Act of 2023, the provision of the Act of 2023 prevails.

3 Proposed Revision of the Decision

31. As outlined above, the purpose of this Consultation process is to undertake a review of the Decision, which will subsequently result in a revised draft Decision to be published as part of the Response to Consultation. This review includes proposed changes to D08/24, as follows:

    a. Geographic area;

    b. Additional reporting threshold for significant security incidents;

    c. Security incident category;

    d. Frequency of security incident reports related to weather events, such as storms;

    e. Information Required;

    f. Calculation methodology for estimating the number of mobile users affected;

    g. Ending of reporting of a security incident; and

    h. Interim root cause analysis.

32. This section will outline these changes in more detail.

3.1 Geographic area

33. Section 11(2) (d) of the Act of 2023 requires providers to have regard to the geographical area affected when assessing the significance of a security incident. The geographical reporting requirements set out in Decision D08/24 require elaboration, to better align with the Act of 2023 – which, as per section 11(3)(d) of the Act of 2023, in summary states that the geographical aspects of the impact of the security incident need to be documented.

34. It became very apparent during Storm Éowyn of a need to gather and assimilate information in a clear and accurate format, as input to any decision making process undertaken by State agencies in organising and coordinating an appropriate response. One aspect of this, is to quantify the impact of a security incident on a geographical basis, in order to target resources and actions in a pragmatic, proportionate and prioritised manner. To this end a suitable geographical reference area that could have cross sector applicability needs to

be employed. ComReg is also cognisant of ENISA's Technical Guideline on Incident Reporting Under the EECC[9] which states:

> *The following qualitative thresholds should be considered to assess the impact for the security incidents:*
>
> - *a) Geographical spread: This applies to incidents affecting the availability of the services provided in specific regions/areas as defined in national legislation, such as:*
>   - *when there is a cross-border impact*
>   - *large (areas larger than xx km^2), remote or rural areas, islands, affected*
>   - *capital or critical region affected*
>   - *interconnections are affected (or number of international interconnections affected)*

35. ComReg's Decision D08/24 does not specify a geographic area and so during Storm Éowyn, security incident reporting was organised on a per county basis, the suitability of which itself was disputative. To address this, ComReg now proposes the formal introduction of an appropriate geographic reference for security incident reporting purposes which would facilitate a more granular impact analysis of security incidents. ComReg is minded to adopt the Municipal District ("MD") as the geographic reference area for reporting purposes[10]. In this document and the associated Draft Decision, where MD is used it will mean a sub-division of County Council areas into a total of 106 areas nationally, including:

    - Municipal, Borough and Metropolitan Districts; and

    - City Councils.

36. This proposal is informed by the fact that any emergency response activity would be co-ordinated at the overall county level, as per the Major Emergency Management Framework (the "MEMF")[11], but MDs would provide greater emphasis within the county level structure. Where a MD was more impacted than others, the county-level response may choose to focus their resources on its resolution. ComReg further notes that where larger counties are impacted by

[9] https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

[10] A Municipal District is a local government administrative unit that governs a specific territory, which can include towns, villages, or rural areas. They exist as a tier of local governance below the county level.

[11] A framework for major emergency management

weather events, this approach would usefully facilitate coordination on a more granular level.

37. ComReg is minded to adopt this more granular approach as it facilitates better coordination with other State Agencies, who could then more effectively assist providers within the affected geographic area, helping to remedy network outages more swiftly and most importantly reinstating services to consumers.

3.2 Additional reporting threshold for Significant Security Incidents

38. The definition of a "significant security incident" for the purposes of reporting to ComReg is set out under section 11 of the Act of 2023. The Decision currently sets out a number of thresholds that would trigger the reporting of a significant security incident. However, the current thresholds are with respect to the impact of a security incident relative to the national user base of the service affected. This risks undermining the impact of security incidents on smaller subsets of the population, in particular geographical areas such as MD and/or island populations.

39. As ComReg is adopting the MD as the geographic reference area for reporting purposes, in respect of the trigger to report a security incident, ComReg would also wish to consider security incidents that significantly impact the islands off the coast of Ireland.

40. To that end, ComReg proposes that for any single geographical area – MD or island, where more than 50% of any provider's users in that area are affected by the security incident, would trigger a security incident report.

3.3 Categorisation of Incidents

41. The Decision sets out that service providers must select one of four subcategories of security incidents: Confidentiality, Integrity, Authenticity or Availability. Within the Root Cause Analysis, a more detailed description of the cause of the incident shall also be given in free text. This is then used to further categorise the security incident into one of: Human Errors, System Failures, Natural Phenomena, Malicious Actions and Third Party Failures as required by ENISA Technical Guideline on Incident Reporting under the EECC[12].

[12] Part 2 page 26 of Technical Guideline on Incident Reporting under the EECC, https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc

42. ComReg therefore proposes to align the providers' reported categorisation with that of the Root Cause Analysis (i.e., Human errors, System Failures, Natural Phenomena, Malicious Actions and Third Party Failures) to be included in the text document RCA.

3.4 Frequency of weather related security incident reports

43. Decision makers in major emergency situations may often have to make critical decisions using data that is timely, accurate and clear. In the case of weather related events such decision makers are likely to be NECG, Local Authorities ("LA"), site owners, ESBN among others. In order to coordinate effective, efficient and prioritised response activities, such organisations require, in so far as possible, the most up to date geo referenced impact information. Ideally this information would be prepared in time for the daily NECG or such similar meeting.

44. The Decision sets out the reporting frequency during a weather event related security incident in Part Three section (7) (a), where reports are to be submitted by providers' twice daily at 10H00 and 16H00.

45. ComReg is instead proposing a single daily report due **no later than 09H00**, thereby reducing the burden on providers when in practice there is very little difference, if any, between the current evening report and that of the following morning. Among other things, this would reduce the regulatory burden while better facilitating the compilation of all individual provider reports into a timely and comprehensive update for the NECG, as required.

3.5 Information required

46. ComReg notes, section 5.4.6.1 of the Framework for Major Emergency Management which states that decision makers in major emergency situations may have to make critical decisions based upon incomplete information. Efforts should be made to ensure that information for decision makers, is as timely, accurate and as clear as possible. What decision makers need is an organised and contextual representation of what is happening, qualified by sequential steps relating to the security incident as it happened rather than a surge of unfiltered data.

47. ComReg is also cognisant of the additional detailed information requested by the NECG during Storm Éowyn on foot of the needs of key stakeholders. The understandably reactive nature of these requests, reflecting the damage caused by this exceptional weather event, was however open to misunderstanding and misinterpretation by providers, particularly given the variations in network

architectures and standards when coupled with provider business models, most notably in the case of fixed ECN.

48. To this end, two draft replacement storm/weather related security incident reporting templates[13] (Annex 2) have been designed and are available here for comment.

49. The first template ComReg 25/84a[14] covers the initial and daily update reports needed to inform response action coordination by providers, NECG and other agencies and as required by section 11 of the Act of 2023.

50. The second template ComReg 25/84b[15] addresses the final Root Cause Analysis ("RCA") Report post security incident closure and notably accommodates information required by ComReg under section 6 of the Act of 2023.

51. As set out above, section 11 of the Act of 2023 determines the required information to be supplied by providers. In particular, Section 11 (3) (d) requires providers to include the information in Section 11 (2) (a) to (g) when notifying the Commission of a security incident. The use of the newly proposed tabular formatted reporting templates is based on these obligations and outlined in Table 1 below:

[13] Following the conclusion of this consultation, these will be up loadable on ComReg's incident reporting portal (ComReg Data) by selecting 'storm' as the security incident type.

[14] Initial and Update Template "Weather Event Initial and Update Reports Template Draft for Consultation ComReg 25/84a", see Annex 2.1.

[15] Root Cause Analysis Template "Weather Event RCA Template Draft for Consultation ComReg 25/84b", see Annex 2.2

Act of 2023 Reference	Reporting Template Information Heading
(c) the public electronic communications network or publicly available electronic communications services provided by it affected by the security incident;	Access Network, Number of Connected Physical Access Paths affected
	Radio Access Network, No. of Sites (e.g. Base Stations or TXN Hub sites) affected
	Access Network: No. of CPE's (ONT, NTU etc.) affected
	Total Number of Nodes (e.g. PoP, Exchanges, DSLAMs etc.) Deployed Per Municipal District
	Total Number of Base Stations/Nodes Deployed Per Municipal District
	Number of any Nodes or Equipment Impacted (e.g. Base Stations, Transmission hubs, DLAMS, Exchanges, Poles, Core/Transport/Access Nodes, Radio Units or Antennas, MW links etc.)
	Number of Users at Risk
	Utility Power input cause (affected and at risk)
	Access cause (affected and at risk)
	Number of Nodes where Access Issues limited Repair Capability
	Other main causes of outages
(e) the number of users affected;	Total Number of Service Users Affected
	Total number of user hours lost
	Number of users with mitigations to minimise the impact of the incident
(d) the date and time the security incident occurred and its duration;	Estimated time to repair (average ETR for 95% of issues in county)
	Average Time to Repair for All Faults
	Maximum Time to Repair all faults
	Access/Transport/Core Number of nodes affected
(f) any class of users particularly affected;	Service
(g) the geographical area affected;	Municipal District Name
	Local Authority Name
	County
	County Codes
	Network Entity Identity
	Network Entity Name
	X of the network entity or customer premises expressed in IRENET95 format.
	Y of the network entity or customer premises expressed in IRENET95 format.
	Eircode of the customer premises associated with the service affected.
(g) such other information as the Commission may specify.	Notes

Table 1: Mapping of Act of 2023 Information Requirement & Template Information

52. The details of the information proposed for gathering through the tabular formatted templates are listed in Table 2 and Table 3 below:

Fixed ECN	Mobile ECN	ECS (Fixed, Mobile, MVNO, NI-ICS)
Municipal District Name	Municipal District Name	Municipal District Name
Local Authority Name	Local Authority Name	Local Authority Name
County	County	County
County Codes	County Codes	County Codes
Total Number of Service Users Affected (all faults including those related to node faults and/or those related to physical access path faults)	Total Number of Service Users Affected (all faults) [as per agreed calculation methodology]	Total Number of Service Users Affected (all faults including those related to node faults and/or those related to physical access path faults)
Number of users with mitigations to minimise the impact of the incident	Number of users with mitigations to minimise the impact of the incident	Number of users with mitigations to minimise the impact of the incident
Fixed Access Network, Number of Connected Physical Access Paths affected	Radio Access Network, No. of Sites (e.g. Base Stations or TXN Hub sites) affected	Access Network: No. of CPE's (ONT, NTU, How etc.) affected
Access Network: No. of CPE's (ONT, NTU etc.) affected	Mobile Transport: No of nodes affected	Core Network: No. of Nodes affected
Fixed Access Network, No. of Nodes / Exchanges affected	Mobile Core Network: No of nodes affected	No. of Nodes at Risk
Fixed Transport Network: No. of Nodes affected	Number of Nodes (all types Base Stations, Transport or Core) at Risk	Number of Users at Risk
Fixed Core Network: No. of Nodes affected	Number of Users at Risk	Utility Power input cause (affected and at risk)
Fixed Access Network, No. of Nodes / Exchanges at Risk	Utility Power input cause (affected and at risk)	Other main causes of outages
Number of Users at Risk	Access cause (affected and at risk)	Estimated time to repair (average ETR for 95% of issues)
Utility Power input cause (affected and at risk)	Other main causes of outages	Service
Access cause (affected and at risk)	Estimated time to repair (average ETR for 95% of issues)	Notes
Other main causes of outages	Service	
Estimated time to repair (average ETR for 95% of issues)	Notes	
Service		
Notes		

Table 2: Information Gathered in Initial/Update Template ComReg 25/84a

Incident Summary	Fixed ECN	Fixed ECN Premises	Mobile ECN	ECS (Fixed, Mobile, MVNO, NI-ICS)	Affected Network Elements
Incident ID:	Municipal District Name	No.	Municipal District Name	Municipal District Name	Network Entity Identity
Description of the security incident and ECN/ECS affected:	Local Authority Name	Eircode of Customer Premises where Service Impacted	Local Authority Name	Local Authority Name	Network Entity Name
Security incident response and actions Taken	County	Where Eircode is not available: X (ITM Easting Coordinate of the premises in IRENET95 format)	County	County	X (ITM Network Entity Easting IRENET95 format)
	County Codes	Where Eircode is not available: Y (ITM Northing Coordinate of the premises in IRENET95 format.)	County Codes	County Codes	Y (ITM Network Entity Northing IRENET95 format)
	Service		Service	Service	Time to Repair
Mitigations against future recurrence of the security incident and time lines for same	Total Number of Users Affected Per Municipal District (all faults including those related to node faults and/or those related to physical access path faults)		Total Number of Users Affected Per Municipal District (all faults including those related to Access, Transport and/or Core faults)	Total Number of Users Affected Per Municipal District (all faults including those related to node faults and/or those related to physical access path faults)	
	Total number of user hours lost		Total Number of User Hours lost	Total number of user hours lost	
	Total number of users with mitigations to minimise impact of incident		Total number of users with mitigations to minimise impact of incident	Total number of users with mitigations to minimise impact of incident	
	Total Number of Nodes (e.g. PoP, Exchanges, DSLAMs etc.) Deployed Per Municipal District		Total Number of Base Stations/Nodes Deployed Per Municipal District	Total Number of Nodes Deployed Per Municipal District	
	Total number of Nodes affected		Number of Base Station/Node Impacted	Total number of Nodes affected	

	Number of Nodes impacted by Power Failure		Number of Base Stations/Nodes impacted by Power Failure	Number of Nodes impacted by Power Failure	
	Number of Nodes Physically Impacted		Number of Base Stations/Nodes with Mast/Tower Damage	Number of Nodes Physically Impacted	
	Number of Access Path Faults		Number of Base Stations/Nodes Antenna, Remote Radio Unit, Active Antenna Unit and/or Mounting Damage	CPE Power Outage (Router/Home Gateway, ONT, NTU etc)	
	CPE Outage (Router/Home Gateway, ONT, NTU etc)		Number of Base Stations/Nodes with Mobile Backhaul TXN Damage	Number of Nodes where Access Issues limited Repair Capability	
	Number of Poles Affected		Number of Base Stations/Nodes where Access Issues limited Repair Capability	Average Time to Repair for all faults	
	Number of Nodes with TXN Damage		Average Time to Repair for all faults	Maximum Time to Repair for all faults	
	Number of Nodes where Access Issues limited Repair Capability		Maximum Time to Repair (start time of first fault till recovery time of last fault)	Notes	
	Average Time to Repair for All Faults		Mobile Core: Number of nodes affected		
	Maximum Time to Repair all faults		Mobile Transport: Number of nodes affected		
	Fixed Core: Number of nodes affected		Notes		
	Fixed Transport: Number of nodes affected				
	Notes				

Table 3: Information Gathered in RCA Template ComReg 25/84b

53. This notwithstanding, ComReg reserves the right to ask for further information, as set out at section 11(3)g of the Act of 2023, which among other things would ensure that providers are taking the appropriate measures under section 6(3) of the Act of 2023 to prevent and minimise the impact of security incidents on users and on other networks and services.

54. ComReg's objective is to ensure a common understanding[16] across all parties involved in the security incident, as to the format and type of information to be reported, thereby significantly lessening any possibilities for misinterpretation. **As such, providers should be aware that the information provided to ComReg may be relied upon by the Minister in updating the Dáil and could be included in the Dáil records**.

55. The use of the proposed templates in the case of storms or weather related security incidents would also require a change to the reporting platform, moving away from the current web-page based form, to a file upload facility for reporting via the proposed templates.

56. It is envisaged that the advance distribution and subsequent alignment, as described earlier, would allow providers adopt the templates (within an appropriate lead time in so far as possible) in their operational platforms and/or processes for reporting on future storm or weather related security incidents. In order that the information may be more readily reported during the actual security incident and by automation, ComReg's intent is to lessen the reporting burden on providers – as discussed in paragraph 46 above.

57. It is further envisaged that ComReg's assimilation of individual providers reports may be automated through Business Intelligence tools thereby facilitating speedy NECG reporting (via the DCCS) and preserving data integrity.

3.6 Number of Mobile users affected

58. Currently, there is a possibility to notably over or under estimate, depending on the location of the security incident, the number of mobile users affected by a security incident. This imprecision arises from the methodology used to estimate the number of users of the mobile service affected which in turn feeds the National User Base (NUB) relative quantitative threshold calculation. The current approach to estimating affected customers is to divide the service providers total subscriber base by the total number of its base stations. This approach assumes that every base station serves an equal number of users, ignoring significant variations

[16] See Annex 3 for the definition of terms used in the templates.

driven by geography and population density. Storm Éowyn illustrated that this is not a suitably robust methodology for calculating an accurate estimate of the number of affected users. Storm Éowyn struck our western seaboard hardest and in locations where the typical subscriber numbers per affected base station would often be significantly less than a national average. This methodology likely led to an over estimation of mobile users affected, to some degree or other by Storm Éowyn.

59. The alternative approach proposed is to measure actual daily unique users per base station (averaged over a three month rolling period) and sum these figures for all impacted base stations during an outage, delivering a more realistic and reliable count of consumers affected. Emphasising unique users, alleviates some of the risk of overestimating the number of users served, as it avoids counting a single user making multiple calls in one base station. This leads to a more accurately calculated estimation of the affected users being used as an input into the NUB threshold.

60. It should be readily appreciated that due to the transient nature of users, through and within the coverage area of a mobile base station site, it is not possible to determine with absolute precision the number of users impacted by a security incident. This is dependent on but not limited to factors such as, the time of day, time of year and topology amongst other factors. ComReg's proposal, however, if adopted, would deliver a far more accurate estimation of users served than that produced by the current methodology.

3.7 Ending of reporting of a security incident

61. The Decision currently sets out that a provider can claim to have returned to Business as Usual ("BAU") once the recovery has restored services to less than 1% of the National User Base of a particular service affected. This is currently determined by the provider and used to determine the end of reporting for the security incident. In practice, this proved unsuitable given the prolonged recovery and long tail in the case of Storm Éowyn.

62. Consequently and in respect of security incidents due to weather events such as storms, ComReg is proposing that it would instead instruct a provider/providers when reporting of a security incident will stop. This is to take into account matters such as the concentration of affected users in a geographic area, the need for continued reporting by other stakeholders over the period of recovery and any other important and relevant factors in the matter at hand. ComReg already commences the start of reporting for certain significant security incidents – such as storms or severe weather event related security incidents. The bringing of the

end to such security incident reporting by ComReg would therefore appear to be a prudent and practical step that would ensure a greater consistency of approach.

63. This notwithstanding, ComReg understandably reserves the right to ask for further information under section 11(3)g of the Act of 2023 to ensure that providers are taking the appropriate measures under section 6(3) of the Act of 2023 to prevent and minimise the impact of security incidents on users and on other networks and services; and to help ensure the availability of services required by Regulation 92(1) of the Regulations of 2022.

3.8 Interim root cause analysis

64. Decision D08/24 requires a Root Cause Analysis ("RCA") report within 30 calendar days after the commencement of the incident. However, in extreme weather events such as Storm Éowyn, full recovery, and therefore a full RCA took considerably longer. However, it will also be appreciated that an RCA report during the period of recovery where extended, as in the recent case, would not be appropriate.

65. In light of these experiences and practical difficulties, ComReg proposes that, in the case of storm or weather related security incidents, an initial RCA would be provided to ComReg within the 30 calendar days post the event, but this would serve as an interim RCA in cases where full recovery of the ECN/ECS is not yet achieved due to the severity of the security incident. A final RCA would be submitted to ComReg once all impacts are recovered or as determined by ComReg. In cases where the full recovery is prolonged ComReg would also reserve the right to request updates on progress under section 11(3)g of the Act of 2023.

4 Draft Regulatory Impact Assessment (draft "RIA")

4.1 Introduction

66. Section 11 of the Act of 2023, and the Decision sets out the obligations on service providers to report security incidents under the relevant provisions of the European Union (Electronic Communications Code) Regulations 2022, S.I. No. 444 of 2022, (the "Regulations of 2022"), and the Act of 2023. The Decision sets out the process and information providers are required to provide to ComReg during network security incidents, including storms.

67. Ireland experienced several storms during 2025, of which Storm Éowyn, as we noted earlier, was one of the most destructive on record, prompting nationwide red wind warnings and triggering the activation of the National Emergency Coordination Group ("NECG"). Subsequently, ComReg engaged with ECN/ECS providers[17] affected by Storm Éowyn about lessons learned and opportunities for improving the process of incident reporting.

68. ComReg has recently put in place dedicated IT technical support during such weather events and following the update of the portal, published its revised users' guide for reporting security incidents[18] to provide for greater robustness in reporting. However, and as we have outlined, there are improvements that could potentially be made to the security incident reporting process and the information being made available to ComReg (and the NECG among others) during network incidents and particularly storms.

69. The purpose of this draft RIA is to consider the options available to ComReg and assess the impact those options would have on stakeholders, competition and consumers.

4.2 RIA Framework

70. 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

[17] These were in the form of group meetings accommodated by IBEC's Telecommunications Industry Ireland ("TII") forum, as well as subsequent bi-lateral meetings held with a number of providers.

[18] Users-Guide-for-the-Incident-Reporting-Portal-on-Data.ComReg_-Final_03102025.pdf

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.

71. 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. The final RIA is updated as appropriate following responses received to this Consultation and on this draft RIA.

72. In conducting the RIA, ComReg has regard to its RIA Guidelines[19], 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.

73. 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 a relatively low impact ComReg may carry out a lighter RIA in respect of that decision.

4.3 Structure for the RIA

74. 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.

75. 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

[19] 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

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 and 4

76. Step 3 assesses the likely impact of the proposed regulatory measures on stakeholders. In this draft RIA, stakeholders fall into five main groups:

I. Consumers (Impact on consumers is considered separately below).

II. Service providers who are required to report security incidents to ComReg.

III. The NECG which is the established central government platform for responding to national level emergencies under the Strategic Emergency Management Framework.

IV. The DCCS and the National Directorate of Fire and Emergency Management ("NDFEM")[20].

V. Local Authorities which are designated as the lead agencies for coordinating a response to flooding and severe weather emergencies.

77. 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.

78. Of themselves, the RIA Guidelines and the Ministerial Policy Direction on Regulatory Impact Assessments provide[21] 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[22];

[20] NDFEM are a section in the Department of Housing, Planning, Community and Local Government who co-ordinate emergency response and give support to the Irish Fire Service

[21] Ministerial Direction dated 21st February 2003

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

- contribute to the development of the internal market[23];
- promote the interests of users within the Community[24];
- ensure the efficient management and use of the radio frequency spectrum in Ireland in accordance with a direction under Section 13 of the Act of 2002[25]; and
- promote efficient investment and innovation in new and enhanced infrastructures[26].

79. 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. 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 consumers.

80. 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.

4.5 Policy issues and objectives

81. The electronic communications sector plays a vital role in supporting both consumers and businesses to, live, work and communicate. Reliable connectivity is 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. Over 500,000 people now work more than half their week at home[27] and there is rising demand for communicating and consuming digital content on mobile and computing devices, emphasising the importance of a correctly functioning ECN and ECS. Further, extreme weather events such as Storm Éowyn underscore the need for all stakeholders to strengthen infrastructure

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

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

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

[26] Regulation 4(5)(d) of the Regulations of 2022.

[27] Publication Briefing Labour Force Survey Quarter 4 2024 - Central Statistics Office

resilience and provide timely accurate information so end users can take precautions and make alternative arrangements where outages do occur.

82. Users reasonably expect to be able to access services with minimal disruption. However, security incidents on networks do occur and impact the experience of the end user. Security incidents happen for a variety of reasons and include but are not limited to:

- 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, 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.

83. However, high winds from storms are the primary reason for the most widespread security incidents on networks in Ireland. There were 14 named storms during the 2023/24 storm season[28]. The effect of Storm Éowyn on the national telecoms userbase was the largest in ComReg's security incident recording history[29], with a record number of security incidents on ECN and lost consumer hours.

Network incident reporting

84. ComReg's framework for security incident reporting, outlined in the Decision, mandates providers of ECN and ECS, including providers of Number-Independent Interpersonal Communications Services ("NI-ICS")[30] to notify significant security incidents that compromise availability, authenticity, integrity, or

[28] Runs from Friday 1 September 2023 to Saturday 31 August 2024 (inclusive). https://www.met.ie/climate/storm-centre

[29] https://www.gov.ie/en/department-of-the-taoiseach/press-releases/update-from-the-national-emergency-co-ordination-group-on-storm-recovery-response-12/

[30] As defined in Regulation 2 of the Regulations of 2022

confidentiality. In 2024, 15 security incidents resulting in nearly **33 million lost user hours were reported to ComReg**[31] through this system.

85. The notification of security incidents is important to provide early detection, public safety and to support emergency responses to extreme weather events. The timely reporting of security incidents during storms is crucial for enabling the NECG and local authorities to swiftly activate response mechanisms and allocate resources effectively. This coordination of security incident reports by ComReg facilitates real-time information sharing among relevant stakeholders, including emergency services, local authorities and consumers. Transparency of such information enables better preparedness for consumers that are impacted by outages.

Storm Éowyn

86. Storm Éowyn had the highest wind speeds on record in Ireland and joins the list of storms classified as hurricane force 12 on land[32]. The physical resilience of mobile networks was robust with only six mobile phone masts, out of a national base of around 8,300 experiencing structural damage. However, power loss to sites was extensive and resulted in major degradation of mobile network services at the peak of Storm Éowyn.[33]

87. Resilience measures on mobile infrastructure were insufficient for the duration of power loss (which ran to days and weeks in some cases), and service providers experienced physical access issues in supplying & maintaining generators to many sites. This aligns with evidence previously provided by ComReg[34] that showed that when multiple security incidents run simultaneously (as might happen after a large weather event such as a storm), there are limitations on the speed at which these can be cleared, suggesting that service providers' resources for clearing such security incidents are conservatively provided, rather than dimensioned to deal with extreme cases.

88. Storm Éowyn not only stretched the capabilities of service providers, it also stretched the processes and resources used by ComReg in the delivery of security incident information. As we have outlined, ComReg immediately undertook a review of its own security incident reporting processes, leading to the

[31] https://www.comreg.ie/media/2025/07/ComReg-2542R.pdf

[32] January 1839 (estimated wind speeds of 100 knots), Debbie in September 1961 (gusts up to 181 km/h), and more recently Darwin in February 2014 (gusts up to 159 km/h). https://www.met.ie/cms/assets/uploads/2025/08/Eowyn.pdf

[33] https://www.gov.ie/en/department-of-housing-local-government-and-heritage/press-releases/review-of-storm-%C3%A9owyn-response-published/

[34] https://www.dotecon.com/wp-content/uploads/2023/08/ComReg-2359a.pdf

identification of a number of opportunities for improvement. For example, it was identified that the Incident Reporting Portal ("Portal"), used by providers to report the impacts of weather events and network or service incidents would benefit from greater robustness to best facilitate reporting.

89. ComReg has already put in place dedicated IT technical support during weather events and published its revised users' guide for reporting security incidents, following feedback from service providers, that the Incident Reporting Portal ("Portal"), used by them to report the impacts of weather events would benefit from greater robustness to best facilitate reporting.

90. However, Storm Éowyn also demonstrated that there are improvements that can be made to the reporting system to ensure that the most relevant information is shared with DCCS, NECG and local authorities among others, particularly during more intense storms when coordination of timely and reliable information critical to inform decision making. Indeed, the timely and reliable information about outages was raised throughout the Government's Review of Storm Éowyn which is discussed below.

Government Review of Storm Éowyn

91. The review of the coordinated response to Storm Éowyn was published in October 2025 by the National Directorate of Fire and Emergency Management (NDFEM)[35].The report highlights the necessary response actions taken by the NECG and details recommendations considered necessary to consolidate and build on the strengths of the existing coordination structures, acknowledging the need for continuous improvement with an emphasis on community support measures and strengthening the resilience of critical infrastructure. Of particular relevant to this consultation are recommendations 3.17.1 and 3.17.7

Recommendation 3.17.1: Communications is an essential part of the response in rapidly evolving situations.

> "…More agile and streamlined processes should be considered to allow for rapidly evolving scenarios, taking account of the priority information to be communicated, to whom the information should be communicated and the available channels to reach audiences."

92. The review highlights that Recommendation 3.17.1 should be considered in the context of the Strategic Emergency Management (SEM) National Structures and

[35] Review_of_Storm_Éowyn_161025_2.pdf

Frameworks. In that regard, ComReg is listed as the Principal Support for Communications Services and Network Information Services Incidents in the SEM[36]. It is therefore prudent for ComReg to consider, in line with this recommendation whether the process surrounding security incident reporting for telecommunications is sufficiently comprehensive, agile and streamlined to allow for a rapidly evolving scenario such as extreme weather.

Recommendation 3.17.7: Operational systems are an important support to public communications.

> "…Compared to power and water, information was less readily available in relation to telecommunications and broadband outages as they are provided by numerous commercial service providers. It is recommended that efforts are made to address this and ensure greater transparency of information in future."

93. Recommendation 3.17.7 arises because telecommunications and broadband outages during the storm were harder to track and understand compared to power and water outages, which are managed and reported centrally by the ESBN and Uisce Éireann. This highlights the importance of information from service providers being gathered centrally and reported to the DCCS, NECG and other relevant bodies during an extreme weather event.

94. Finally, the report concludes with the observation that the "*longer-term change to climate conditions in Ireland is increasing the frequency of Atlantic storms and flooding emergencies.* ***Early warning, effective coordination****, improved resilience and increased community engagement are identified in this review as the areas that* ***require focus and continuous improvement****.*" [Emphasis added]

DCCS Communications Networks Sectoral Adaptation Plan

95. As noted in Chapter 2, the Governments Sectoral Adaptation Plan for Communication Networks was published in November 2025 by DCCS and sets out how Ireland will strengthen the resilience of our communication networks in the face of climate challenges.

96. Section 3.4.1.2 "*Service outage and network damage information*: collation, *presentation and analysis*" describes the need for much improved information around both service outages and network damage in the aftermath of a resilience event. This section notes, among other things that there is a need for clearer

[36] Strategic Emergency Management (SEM) National Structures and Framework

information about aggregate service outage levels, their locations around the country, and anticipated restoration times. Of particular, relevance the Plan notes that *"This winter saw the first significant test of **ComReg's recently adopted Decision Instrument D08/24** which sets out how providers must report significant security incidents to the Commission. **ComReg are (sic) reviewing the processes around this instrument** to build improvements into how it is operationalised."* [Emphasis added]

Main policy issue

97. Therefore, the main policy issue for consideration in this draft RIA is to identify the options available to ComReg for improving the security incident reporting process.

98. This includes improving the data and information submitted by service providers, the methods used to deliver it to ComReg, and its subsequent dissemination to DCCS, the NECG and other relevant bodies over an appropriate timeframe.

4.6 Identifying Regulatory Options

99. ComReg's current framework for security incident reporting is outlined in the Decision. This has been in place for 21 storms and was the reporting framework in place for Storms Éowyn, Darragh and more recently Storm Amy. ComReg will evaluate the existing framework as an option, given its utility to date, and also to fully understand the impact of any change from an alternative option. Therefore, ComReg notes that **Option 1 is to maintain the status quo** continue use of the Decision (D08/24).

100. ComReg notes that Option 1 (as the status quo) is the minimum set of requirements that would be mandated. Therefore, other options would introduce additional measures over and above Option 1. ComReg assesses potential additional obligations under the various headings below which are set out in further detail in Chapter 3.

1. Geographic Area for reporting incidents

101. Under the Decision, the affected geographical area of a security incident needs to be provided by service providers to ComReg. However, for incidents across large regional or national areas (such as storms) there could be a mismatch between the geographic areas reported by service providers and the area which the local authority is serving. Therefore, there may be benefit in clearly specifying the geographic area over which security incidents should be reported.

102. During Storm Éowyn, information on outages was provided by service providers on a per county basis, which was helpful but did not entirely align with the boundaries of agencies responding to emergencies. In Ireland, 106 municipal districts were established in 2014 and are a sub-division of the county and act as a decision-making subdivision of the full Council that respond to extreme weather.

103. Therefore, any option(s) should include the use of municipal districts as the relevant geographic areas over which security incidents should be reported.

2. Additional threshold for reporting significant incident

104. The definition of a “significant incident” would include a security incident that affects more than 50% of the provider’s users in a municipal district or island.

105. Currently, a large outage in a localised area might not be captured by the definition of a significant security incident under Decision D08/24 because the number of impacted users would be small on a national basis but could be large in a local area or municipal district. This measure would clarify that security incidents that impact more than half of users in a municipal district or island would be a classified as a significant security incident.

106. Therefore, any option(s) should include the additional threshold based on more than 50% of users being affected in a municipal district or island.

3. Incident categorisation

107. Currently service providers must select one of three overarching categorisations of security incidents when reporting on the portal, these are: malicious (cyber-attack, vandalism, etc.); isolated (software bug, hardware failure, etc.) and storm (excessive cold, high winds etc.). Following this, a more detailed description of the cause of the security incident can be given in free text.

108. However, as noted at the outset of this draft RIA, security incidents happen for a variety of reasons and incident reporting may be classified according to one of the five sub-categorisations once the root cause has been identified, as specified in Part 2 of the ENISA Technical Guideline on Incident Reporting under the EECC:

1. Human errors;
2. System failures;
3. Natural phenomena;

4. Malicious actions; and

5. Third party failures.

109. Currently this sub-categorisation uses provider supplied information (using the free text boxes on the portal). However, under this proposal all service providers would report this sub-categorisation through the web portal.

110. Therefore, any option(s) should ensure that the cause of a security incident should be classified according to one of the five ENISA classifications above.

4. Frequency of Security Incident Reporting

111. The current reporting schedule is twice daily at 10H00 and 16H00[37]. This approach has been used for all storms since the commencement of the Decision. In practice however there is little variance between the outages reported at 16:00 and the outages reported at the next morning at 10:00 reporting time partly because service providers typically cannot take significant actions in the field after dusk especially during a winter storm season.

112. Further, to the extent ComReg did require additional information it could do so under section 11(3)g of the Act of 2023[38].

113. Therefore, any option(s) would have a single daily report due at 09H00.

5. Required information and reporting templates

114. During Storm Éowyn, the NECG requested more detailed information which went beyond that set out in Decision D08/24. Therefore any option should consider what additional information would be required by the NECG and local authorities in managing emergency situations. Annex 2 (and Tables 2 and 3 above) sets out the full information proposed. This is not repeated here but includes the following information reported for each day of the security incident:

- Total number of user hours lost;
- Total number of users with mitigations to minimise impact of the security

[37] See Part Three section (7) (a) of the Decision

[38] To ensure that providers are taking the appropriate measures under section 6(3) of the Act of 2023 in order to prevent and minimise the impact of security incidents on users and on other networks and services; and to help ensure the availability of services required by Regulation 92(1) of the Regulations of 2022.

incident;

- Total number of network elements deployed per area;
- Number of network elements impacted by power failure;
- Number of network elements with backhaul damage; and
- Average and maximum time to repair all faults.

115. Separately, within 30 calendar days, service providers would be required to provide the geographic coordinates for each network element (nodes/base stations/poles etc.) that would have been affected by a storm on a municipal basis. This would be used to inform the Root Cause Analysis.

116. All information would be provided to ComReg through a file upload facility for reporting on the portal, using two new proposed templates.

- The first template ComReg 25/84a covers the initial and daily update reports needed to inform response action coordination by providers, NECG and other agencies.
- The second template ComReg 25/84b forms the root cause analysis report post the security incident and importantly includes information required by ComReg under section 6 of the Act of 2023.

117. Therefore, any option(s) should ensure that the information summarised above (and set out in Annex 2 and Tables 2 and 3 above) should be provided to ComReg using the two new templates.

6. Users affected

118. The current approach to estimating affected mobile customers is to simply divide the mobile service provider's total subscriber base by the total number of its base stations. This approach assumes that every base station serves an equal number of users, ignoring significant variations driven by geography and population density. An alternative approach is to measure actual daily unique users per base station (averaged over a three month rolling period) and sum these figures for all impacted base stations during an outage, delivering a more realistic and reliable count of consumers affected.

119. Therefore, any option(s) should include a more accurate method to estimate the number of mobile users affected.

7. Ending of reporting requirement

120. The current requirement to report security incidents continues until service providers notify ComReg that networks and services are operating on a Business as Usual ("BAU") basis, referred in Decision D08/24 as less than 1% of the National User Base of the service affected. The 1% is determined by the service provider and used to end the security incident reporting.

121. However, this approach did not work effectively during Storm Éowyn because the time to fully restore service to all affected customers was lengthy leading to a long tail on the restoration of outages. This creates several issues compromising the effectiveness of security incident reporting. For example:

- The last 1% and location of these incidents can often reveal systemic network weakness e.g., poor redundancy in rural areas/vulnerable areas. Ceasing reporting at 1% can mask these issues from ComReg.

- The end of reporting while some users remain disconnected (the last 1%) erodes trust that ComReg and/or service providers are still prioritising vulnerable consumers, especially after high-visibility events like storms.

122. Under Option 2, reports would continue, until ComReg advises the service provider concerned that reporting on a security incident is no longer required. This allows ComReg to control when reporting can cease depending on the circumstances of a particular security incident or storm or indeed the impact on a geographic area.

123. Therefore, any option(s) should ensure that the ending of reporting is advised by ComReg.

8. Interim Root Cause Analysis

124. Under Decision D08/24, a Root Cause Analysis ("RCA") report is to be submitted to ComReg within 30 calendar days of the security incident. However, in cases of extreme events where recovery is significantly prolonged (e.g. Storm Éowyn), producing a full RCA within this timeframe is often impractical. Instead, the submission of an interim root cause analysis could be submitted to ComReg within 30 days containing preliminary findings. This would be followed by a more comprehensive final report once ComReg is satisfied that the security incident is concluded.

125. Therefore, any option(s) should include provision of an interim RCA report followed by a final RCA once a security incident has concluded.

Option 2

126. ComReg could assess each of the above as individual options, however this would lead to a large number of options. Instead, ComReg proposes to assess these measures together under a single option that can be compared to Option 1 the status quo. ComReg will consider breaking out additional options following the response to consultation if necessary.

127. Given the above, ComReg is of the preliminary view that **Option 2** would be the same as Option 1 except for the following.

I. The geographic unit for reporting security incidents (including storms) is the Municipal District.

II. The definition of a “significant incident” would include a security incident that affects more than 50% of the provider’s users in a municipal district or island.

III. The root cause of a security incident should be categorised into one of five categories; 1. Human errors; 2. System failures; 3. Natural phenomena; 4. Malicious actions; 5. Third party failures.

IV. The timing of reporting updates would change to a single point each day at 09:00

V. When reporting security incidents additional information (as described above) would be provided through two new reporting templates uploaded onto the portal.

VI. The measurement of users affected would be based on actual daily unique users per base station (averaged over a three month rolling period).

VII. Security incident reporting would continue until ComReg is satisfied that, among other things, there are no specific geographic concentrations of faults, and tells the service provider concerned that reporting on this security incident is no longer required.

VIII. Where recovery from a security incident is sufficiently prolonged, service providers would be required to submit an interim root cause analysis to ComReg within 30 days of a security incident commencing.

128. Therefore, ComReg is of the preliminary view that the following options are available to it.

- **Option 1** is the ‘do nothing’ option and involves ComReg continuing to rely on the incident reporting process set out in Decision D08/24; and

- **Option 2** is the same as Option 1 except for the eight additional measures as described in Paragraph 127 above.

4.7 Impact on stakeholders

129. This section assesses the impacts on stakeholders arising from the regulatory options outlined above. As noted in Section 4.3, the four main stakeholder groups are, (i) consumers, (ii) service providers, (iii) the NECG, (iv) the DCCS and NDFEM, and (v) local authorities. Consumers are assessed separately below with the four remaining stakeholder groups assessed in this section.

Service Providers

130. Under Option 1 service providers would have the same reporting requirements as set out in the Decision. Option 2 is the same as Option 1 except for the various enhancements summarised in Paragraphs 128 above and discussed below.

Geographic area

131. In relation to the potential use of municipal districts as the relevant geographic area for reporting security incidents, ComReg notes that service providers previously provided information on a county basis voluntarily during Storm Éowyn. Option 2 would require service providers to update their systems to provide for reporting on a municipal district basis, which is more granular than a per county basis.

132. ComReg is of the preliminary view that there is unlikely to be any significant costs associated with extending the reporting requirement to Municipal Districts. Municipal District boundaries are maintained by Tailte Éireann (formerly Ordnance Survey Ireland) and are available for download on open data portals like the CSO's Census Data website and Tailte Éireann's Surveying Open Data Portal[39]. Any costs (particularly for larger operators) would be limited to some modest upfront costs associated with updating systems to incorporate reporting based on municipal districts.

[39] Surveying Open Data Portal

Affected users

133. In relation to the measurement of users affected being based on actual daily unique users per base station, ComReg notes that this may require some preparation time to provide the average unique users over a three month rolling period. However, in order to dimension their network correctly, service providers should already have access to information about unique users per site across their entire base station network. Under Option 2, service providers would be required to use this information to provide ComReg with accurate information on the number of affected users during a security incident.

134. ComReg also notes that this approach under Option 2 would provide more accurate information about the number of users affected, noting that during Storm Éowyn there was likely to have been an overestimate of impacted users in rural areas. In reality the performance of networks in rural areas was likely better than that reported and more accurate information would have far better demonstrated the resiliency measures service providers are already taking.

Additional requirement to report an incident

135. ComReg notes that the additional requirement to report a security incident that affects more than 50% of the service provider's users in a municipal district or island is unlikely to create any significant costs once systems have been provisioned for reporting on a municipal basis and updated based on number of unique users. Service providers would then be able to estimate the daily number of unique users affected by outages within each municipal district and report to ComReg once 50% of users have been impacted (using the latest available information from the CSO)[40].

Categorisation of Incidents

136. The requirement that service providers would categorise security incidents in line with the five categories provided by ENISA is a relatively minor clarification. These clarifications are unlikely to create any implementation issues or impose any significant costs on service providers.

Frequency of incident reporting

[40] https://census.geohive.ie/datasets/geohive::permanent-private-households-by-year-built-municipal-districts-census-2016-theme-6-2-ireland-2016-cso-osi/about

137. Service Providers are likely to favour reducing the reporting requirement from twice daily to a single reporting requirement at 09:00 under Option 2. This reduces the burden of reporting the additional information requested as part of this consultation. It is also questionable whether such information would be useful because service providers typically cannot take significant actions in the field during night times especially during a winter storm season.

Additional information and templates

138. In relation to the additional information and new reporting templates, service providers have already been providing most of this information as part of their engagement with ComReg and the NECG throughout Storm Eowyn. The additional information beyond what is provided in Decision D08/24 seems likely to already be monitored by service providers as part of their obligations to ensure secure and resilient networks. With an appropriate lead time for automation, the proposed new templates could cater for the submission of this information but in a more consistent and transparent manner than heretofore.

139. Option 2 formalises the need for this information via the templates and provides clarity and certainty that this information would be required for future storms and weather related security incidents.

140. In relation to the Root Cause Analysis requirement to report the location of network assets that were subject to a security incident, providers are already collecting and monitoring such assets. If the service providers know what base stations (or other assets) were down at any point during a storm, then they would also have the associated geographic location that would be provided to ComReg under this option.

141. Similarly, the Root Cause Analysis template also requests a breakdown of individual Eircode's of affected fixed connections for further post storm analysis. The inclusion of Eircode data will allow detailed analysis of areas and customers impacted regularly by storms and assist with identifying vulnerabilities. It will also allow the data to be compared and enriched by other data already available at Eircode level including to assess whether other services are available at the location.

142. The use of the proposed templates in the case of storms or weather-related security incidents would also facilitate a change to the reporting platform, moving away from the current web-page based form, to a file upload facility for reporting. However, this is unlikely to impose any additional costs on service providers given

the reporting requirement is unchanged, but rather requires a different method, for the reports to be submitted to ComReg, which it has provided.

Ending or reporting requirements

143. In relation to the requirement that service providers would continue reporting until ComReg instructs otherwise, the service provider would already be reporting this information internally with a view to restoring services to consumers., Option 2 merely extends the requirement to report until ComReg advises each provider that the reporting is no longer required. There is unlikely to be any significant costs associated with continuing to report on security incidents, particularly when service providers would already be monitoring the restoration of services to users < 1%.

Interim root cause analysis

144. The requirement to provide an RCA within 30 calendar days is the same under Option 1 and Option 2 except in the case where there is a prolonged security incident (i.e. where services have not been fully restored within 30 days). In this case, Option 2 has an additional requirement that service providers would provide an interim report within 30 calendar days with the final RCA being submitted once all impacts are recovered or as determined by ComReg.

145. This is unlikely to impose a significant cost on service providers because they should already be aware of the root cause of a security incident and the circumstances surrounding it even before services are fully restored. To the extent that any information in the interim RCA changed in the intervening period based on new information this could be reflected in the final RCA.

Conclusion on services providers

146. Given the above, ComReg is of the preliminary view that while Service Providers would likely prefer Option 1 they may be willing to support Option 2 given the benefits to wider society and the NECG and/or local authorities in managing emergencies.

147. ComReg also understands that following the October T-RRG meeting, industry reflected a willingness to provide more detailed information on the impact of severe weather related security incidents on their networks.

Local authorities and NECG

148. The NECG requested more detailed information during Storm Éowyn which was made available by providers. This information is not specified in Decision D08/24 (i.e. under Option 1), however, it would be provided under Option 2[41] and would offer the following advantages.

- First, the appropriate categorisation and a fuller description of the impact of storm or weather related security incidents would provide more certainty that security incidents are being appropriately categorised in terms of urgency for review by ComReg and the NECG[42] when responding to emergencies (i.e. incidents caused by storms or other weather related security incidents).

- Second, the provision of more detailed information in the proposed templates, provides greater transparency about the nature of outages, enabling improved coordination across relevant agencies, facilitating a more agile response, enabling more effective restoration efforts.

- Third, it facilitates more streamlined reporting to the NECG through the use of automated systems by both ComReg and service providers. Under this option, the NECG and/or local authorities would receive more detailed information and more quickly than would be the case under Option 1.

- Fourth, the root cause analysis template covers specific assets (e.g. fibre optic cables, base stations etc) which would help DCCS and the NECG to identify vulnerabilities. This could reveal patterns like repeated damage to certain assets which would support storm reviews and assessments on identifying vulnerabilities on which recommendations could be made.

149. Therefore, ComReg is of the preliminary view that the NECG (and relevant agencies from the list of agencies as referenced in Para 21 of Strategic Emergency Management Guidelines) would prefer Option 2.

DCCS and NDFEM

150. The issues highlighted by both the DCCS and NDFEM in their respective reports (as summarised above) were raised based on their experience of the status quo under Option 1.

[41] This additional information is summarised in Paragraph 102 above and set out in full in Annex 2.

[42] The outage data is typically provided to NECG by ComReg through the DCCS.

151. The NDFEM is likely to prefer Option 2 because this option best reflects the recommendations set out in its review of Storm Éowyn. In particular, it would make information more readily available on telecommunications outages allowing for a more streamlined process to be put in place which would allow for relevant information to be provided to consumers.

152. DCCS is also likely prefer Option 2 because the information provided would serve a number of needs, both immediate and long-term as required under the Communications Networks Sectoral Adaptation Plan 2025. During immediate outages, Option 2 provides for clearer information about aggregate service outage levels, their locations around the country, and anticipated restoration times (as referred to in the Adaption Plan). Similarly, under Option 2, the interim RCA would provide additional context on the root cause analysis at an earlier time which would provide relevant information to better promote long term resilience in networks.

153. Furthermore, this option provides for information regarding specific network damage, i.e. line breaks, power loss, physical damage to structures, etc. to be gathered, analysed and so inform possible improvements in network and service resilience.

4.8 Impact on consumers and competition

Consumers

154. 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 or study. For example:

- Reliance on broadband is very high with almost 4 in 5 citing broadband as a definite essential service.[43]
- Over 60% of households now use Internet Protocol Television (IPTV), and almost seven in ten internet users use streaming services such as Netflix, Amazon Prime, Disney+, GAAGO, and Sky Sports.
- Some 87% of internet users used internet banking or mobile banking (including PayPal, Revolut, Apple Pay, etc.) and the same percentage used

[43] https://www.comreg.ie/media/2023/07/ComReg-2359b.pdf

instant messaging services.[44]

- Around 90% of people make contact with emergency services using their mobile. Very few use landline or social media.[45]
- In 2024 almost 540,000 people worked more than half their week at home.[46]
- 40% of internet users made an online appointment or reservation with public authorities or services such as with the National Driver Licence Service, the Passport Office, or public health appointment[47] with a hospital.[48].

155. Consumers value detailed security incident reporting because it allows them to make informed decisions about how to go about their lives in the event of a network outage. While there are no alternatives for some services provided over the internet (e.g. streaming and/or internet browsing), there are others that are widely used over the internet that could be accessed through alternative means. Such services, as described above, include public services, banking/payments and working/studying from home.

156. Consumers can make alternative arrangements for these services which are provided over the internet if sufficient information about outages is made available. For example, banking, payment and public sector services can be obtained on the high street when online services are down. Similarly, those who work or study from home can make arrangements to work in the office. This is particularly relevant for more vulnerable and/or rural consumers where arrangements to travel to towns and cities for hospital appointment services or other services may need to be arranged with family and friends.

[44] Ibid

[45] https://www.comreg.ie/media/2023/07/ComReg-2359b.pdf

[46] Publication Briefing Labour Force Survey Quarter 4 2024 - Central Statistics Office

[47] For example, ComReg notes that the HSE has recently introduced a health app where various appoints and health services can be viewed online. The HSE also offers video health appointments where a consultation with your healthcare professional is done online and includes important services such as:.

- physiotherapy, dietetics, occupational therapy and speech and language therapy
- follow-up with a consultant, for example, to get results
- mental health care
- chronic disease management.

Latest HSE Health App release: Thousands of health service appointments are now available to view on the HSE Health App
Video health appointments

[48] Key Findings Household Digital Consumer Behaviour 2024 - Central Statistics Office

157. However, these arrangements can only be made if more accurate and detailed information is available about broadband/mobile outages in their area. Therefore, consumers are likely to prefer Option 2 because it requires service provides to provide more detailed and localised information about outages across municipal districts.

158. Consumers are also likely to support the proposal under Option 2 that reports would continue, until ComReg advises otherwise. Under Option 1 consumers are unlikely to support a situation where there would be no reporting requirement for the last 1% of outages.

159. Furthermore, consumers are also likely to prefer options that would provide information to ComReg and the NECG (through the Root Cause Analysis) that would assist in improving the long-run resiliency of networks to reduce the occurrence of network outages in the first instance.

160. Consumers would prefer Option 2 over Option 1 because it requires services providers to report more detailed information resulting in more comprehensive reports being made available to the NECG and to the public about service disruptions. This improved information flow allows consumers to better plan around outages and shift to alternative means of accessing services that were previously accessed online.

161. Therefore, ComReg is of the preliminary view that consumers are likely to prefer Option 2.

Competition

162. The impacts on competition from either Option are likely to be small, noting that Option 1 has not created any competition concerns and has been in place for nearly 18 months. That said, there are aspects of Section 12 of the Act of 2002 that are relevant to determining which option would better promote competition. In particular, promotion of competition includes:

- ensuring that users, including disabled users, derive maximum benefit in terms of choice, price and quality (under Section 12 (2) (a) (i)); and
- encouraging efficient investment in infrastructure and promoting innovation (under Section 12 (2) (a) (iii))

163. ComReg has already outlined above in ‘Impact on Consumers’ why Option 2 would be preferred for consumers and vulnerable users.

164. In relation to efficient investment, Competition would be better served by providers submitting more information about security outages under Option 2, because more detailed reporting to ComReg creates a stronger incentive for providers to prevent security incidents in the first instance and to resolve any disruptions as quickly as possible given the heightened scrutiny on reliability. This transparency is more likely to promote infrastructure based competition as providers invest in networks to maintain reputation, noting that reliability is one of the top three factors considered important by consumers[49]. Further, verifiable regulatory reports on outages (whether during a storm or not) makes it more difficult for individual providers to downplay the impact any security incident is having on its services.

165. Therefore, competition is likely to be better promoted under Option 2.

4.9 Overall Preferred Option

166. In light of the assessment above, ComReg is of the preliminary view that the overall preferred option is Option 2.

167. ComReg is also of the preliminary view, having regard to the applicable legislation and legal principles, its draft RIA and the material to which it has had regard, that the Overall Preferred Option is objectively justified, proportionate, and non-discriminatory. In particular, the preferred option:

- is objectively justified given the detailed assessment provided in this draft RIA, including that the preferred option is that which would best facilitate local authorities and NECGs requirements during storms.

- takes all reasonable measures to promote competition under section 12 of the Act of 2002, by making relevant information and data about security incidents of all service providers publicly available.

- would not give rise to discrimination in the treatment of undertakings because the requirements would apply to all service providers equally.

- is proportionate because, among other things, there does not appear to be a less onerous means by which these objectives and principles could be achieved because there is no other source available from which to collect the information. Furthermore:

[49] https://www.comreg.ie/media/2023/07/ComReg-2359b.pdf

- much of the information required under Option 2 is already being collected and monitored by service providers and was provided to ComReg in relation to Storm Eowyn.
- the additional information required under Option 2 is needed by the local authorities and the NECG to appropriately manage emergency response to storms and this information should already be used by service providers to assess the impact of outages;
- Option 2 would be more in line with the relevant recommendations set out in the Governments Review of Storm Eowyn: and
- Option 2 does not impose a significant impact on service providers.

168. Accordingly, in light of the above and on the basis of the information currently before it, ComReg is of the preliminary view that Option 2 is the preferred option.

5 Draft Decision Instrument: DNN/26

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:

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

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

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

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

"Availability" 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 Act of 2002, as amended;

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

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

"DCCS" means the Department of Culture, Communications and Sport;

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

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

"ENISA" means the European Agency for Cyber Security;

"Incident reporting portal" means the portal for reporting security incidents at ComReg Data (https://data.comreg.ie/);

"Integrity" means a property of accuracy and completeness;

"MD" means Municipal District[50], a sub-division of County Council areas into a total of 106 Municipal Areas nationally, including: Municipal, Borough and Metropolitan Districts; and City Councils;

"MS" means Member States;

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

"National User Base", means the total number of users in the state accessing a particular ECS, such as but not limited to Fixed or Mobile Voice or Broadband, as defined in section 2 below;

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

"provider" has the meaning assigned to it in the Act of 2023;

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

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

"service" means using ENISA Technical Guidelines one of

Fixed Voice - fixed telephony (i.e. fixed voice communications service),

Mobile Voice - mobile telephony (i.e. mobile voice communications service),

Fixed Broadband - fixed internet access,

Mobile Broadband - mobile internet access,

"Templates" means the templates to be used by a provider in submitting a report on the incident reporting portal, in relation to a weather related security incident;

"Weather Related Security Incident" means any security incident arising from the impact of any weather event such as a Met Éireann declared named storm or when Met Éireann issues an orange or a red-level weather warning;

and

[50] A Municipal District is a local government administrative unit that governs a specific territory, which can include towns, villages, or rural areas. They exist as a tier of local governance below the county level.

Terms used in this Decision Instrument have the same meanings as set out in any of the following as applicable: the Act of 2022; the Regulations of 2022; the Act of 2023; the Numbering Conditions of Use and Application Process document (ComReg 15/136R3) as amended from time to time; and Commission Document 26/NN of which this Decision Instrument forms a part.

PART II – STATUTORY POWERS AND DECISION-MAKING CONSIDERATIONS

ComReg,

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

(b) pursuant to its objective under section 12(1)(a) of the Act of 2002 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 Act of 2002, 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 Act of 2002, 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 Act of 2023 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) of the Act of 2023 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 Regulations of 2022 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 Regulations of 2022 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 Act of 2023 for providers to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services;

(j) having, pursuant to section 13 of the Act of 2002, 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 the Consultation [ComReg Document No. 25/84], 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.25/84 to which this Decision is attached;

PART III – THE DECISIONS

ComReg hereby makes the following decisions:

Reporting Thresholds for Significant Security Incidents

(1) A "significant security incident" for the purposes of reporting to ComReg under section 11 of the Act of 2023, is a security incident that falls within the following thresholds, or meets the matters detailed in section 11(2) (c to g inclusive) of the Act of 2023, where:

(a) 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 the incident duration in hours (hrs), and the y-axis represents the percentage of the national user base affected:

	1hrs->2hrs	2hrs->4hrs	4hrs->6hrs	6hrs->8hrs	>8hrs
1%-2%	🟩	🟩	🟩	🟩	🟥
2%-5%	🟩	🟩	🟩	🟥	🟥
5%-10%	🟩	🟩	🟥	🟥	🟥
10%-15%	🟩	🟥	🟥	🟥	🟥
>15%	🟥	🟥	🟥	🟥	🟥

(b) any security incident impacting greater than or equal to one million (1,000,000) User Hours[51], has or is taking place:

(c) 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; or

(d) the security incident affects the provision of the ECN or ECS in a specific geographic area (the municipal area or island), that it affects is more than 50% of the provider's users in that area.

National User Base Calculations and Calculation of Impacted Users

(2) To determine the service's national user base and the percentage number of users for each service associated with any outage, a provider must reference

[51] User Hours is the product of the Number of Users affected and the Duration of the security incident;

relevant figures in the most recent Quarterly Key Data Report ("QKDR") or any equivalent successor document found on ComReg's webpage[52], 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, 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 Broadband, 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 replaces "Machine to Machine Subscriptions" in the QKDR or equivalent successor document as may occur from time to time.

- Once the overall National User Base ("NUB") for the mobile service (as detailed above) is known, the number of users affected must be calculated as a percentage of the overall NUB. This is necessary in order to compare the thresholds described in section "Reporting Thresholds for Significant Incidents" (1) (a) above. The number of users affected is calculated by measuring actual daily unique users per base station (averaged over a three month rolling period) and sum these figures for all impacted base

- [52] Quarterly Key Data Report | Commission for Communications Regulation stations during an outage, delivering a more realistic and reliable count of consumers affected.

Information Required for A Notification of any Security Incident

(3) Under the Act of 2023[53]; 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 and in the case of the Root Cause Analysis this is more explicitly matched to the ENISA sub-categories of Human errors, System failures, Natural phenomena, Malicious actions and Third party failures[54];

(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.

In relation to (3)g above the geographical area is the Municipal District or an island. For weather related security incidents items 3 (e) to (h) above are expanded upon in

[53] Sections 11 (2) c, d and f, and section 11(3).

[54] For weather related incident reporting this RCA categorisation must be done within the text description RCA document as opposed to the RCA excel template that forms part of said text description document.

the reporting templates as documented in section “Exception: Weather Related Security Incident Reporting” items (6) to (8) below.

Reporting Significant Security Incidents to ComReg

(4) Providers must use ComReg’s incident reporting portal[55] to report significant security incidents to ComReg.

Timings and Frequency for Reporting A Significant Security Incident

(5) (a) Excluding weather related security incidents, 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 incident reporting portal, advising that the security incident has been resolved and that services have been restored.

For significant security incidents ComReg must receive a comprehensive report update within 30 calendar days of the significant security incident confirming the circumstances of the security incident. If not a weather related security incident, the RCA will contain:

- 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;

[55] At data.comreg.ie: ComReg Data

- categorisation 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.

Further details for weather related significant security incidents are expanded upon in Decision **(8)** below.

The root cause of any security incident can be categorised into one of five sub-categories; 1. Human errors; 2. System failures; 3. Natural phenomena; 4. Malicious actions; and 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.

(d) Reporting timing, frequency and cessation for weather related events if further detailed in section “Exception: Weather Related Security Incident Reporting” Decisions **(6)** to **(8)** below.

Exception: Weather Related Security Incident Reporting

(6) Notwithstanding the thresholds given in Decision **(1)** and timings given in Decision **(5)** of this Draft Decision Document above; the following exceptional security incident type, weather related security incidents including those related to storms, requires the following notification timescales.

(7) Weather related security 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 of the need to report and noting the any further details and the required use of the reporting template (see A 2.1 below). -

(a) The timing for reporting the effect on the providers' ECN or ECS to ComReg will be daily at 09H00;

(b) Such reports will continue, using the prescribed templates, until ComReg is satisfied that the ECN and ECS are operating on a Business as Usual ("BAU") basis, there are no specific geographic concentrations of faults[56], and tells the provider concerned that reporting on this security incident is no longer required.

(c) This notwithstanding and in relation to 7(b) above, ComReg reserves the right to ask for further information under section 11(3)g of the Act of 2023 to ensure that providers are taking the appropriate measures under section 6(3) of the Act of 2023 in order to prevent and minimise the impact of security incidents on users and on other networks and services; and to help ensure the availability of services required by Regulation 92(1) of the Regulations of 2022.

(d) In the case of weather related security incidents the reporting templates breakdown fault reporting to a geographical reference area which is the Municipal District.

(8) As with other security incident types (malicious, isolated) a Root Cause Analysis report is to be created in the case of weather related security incidents also. This is the tabular formatted document contained in Annex 2.2 and is to be uploaded to the incident reporting portal. The contents of the first table in the report is a summary of the incident and is to contain at least the following:

(a) [56] Where the security incident affects the provision of the ECN or ECS in a specific geographic area, that is it affects more than 50% of the provider's users in that area, such as, but not limited to a county or island.

- 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;
- Root cause summary statement for reported security incident;
- Security incident 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 of the security incident's root cause matched to the ENISA sub-categories of Human errors, System failures, Natural phenomena, Malicious actions and Third party failures, 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.

The remaining tables of the completed RCA excel template (see A 2.2 below) should be completed as follows:

(a) Fixed network providers will complete Tabs "1.Incident Summary", "2. Fixed ECN", 3. "Fixed ECN Premises" and "6.Affected Network Elements";

(b) Mobile network providers will complete Tabs "1. Incident Summary", "4. Mobile ECN" and "6.Affected Network Elements"; and

(c) Other providers will complete Tabs "1. Incident Summary", "5.ECS (Fixed Retail MVNO NIICS)" and "6.Affected Network Elements".

Thirty days after the weather related security incident has ended, the RCA above should be submitted. However, should service impacts still be affecting services more than 30 days after the incident, this will be seen as an Interim RCA with a final RCA due after the restoration of all affected services is complete.

PART IV– EFFECTIVE DATE

Decisions **(1)** to **(8)** above shall apply to providers as from the date of the making of this Decision Instrument plus three (3) months to allow providers to implement the new reporting templates within their organisation, processes and tools.

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

[Commissioner Name]

Commissioner, Commission for Communications Regulation

6 Making a submission and next steps

6.1.1 Submitting Comments

169. All input and comments are welcome. Please set out your reasoning and all supporting information for any views expressed. It would make the tasks analysing responses easier if comments were referenced to the relevant section/paragraph number in each chapter and annex in this document.

170. In light of the timing of the publication of this consultation, the consultation period will run for 5 weeks until **17:00 Irish Time on Friday 9 January 2026** during which time ComReg welcomes written comments on any issues raised in this paper.

171. Responses must be submitted in written form (email) to the following recipient, clearly marked – Submissions to ComReg 25/84:

Suzanne O'Toole

Commission for Communications Regulation

Email: marketframeworkconsult@comreg.ie

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

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

174. In this regard, respondents should submit views in accordance with the instructions set out below. When submitting a response to this notification that contains confidential information, respondents must choose one of the following options:

- Preferably, submit both a non-confidential version and a confidential version of the response. The confidential version must have all confidential information clearly marked and highlighted in accordance with the instruction set out below and include the reasons as to why they consider any particular material to be confidential. The separate non-confidential version must have actually redacted all items that were marked and highlighted in the confidential version.

OR

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

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

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

6.1.2 Next Steps

177. When it has concluded its review of all submissions received and other relevant material, ComReg’s intention would be to publish a Response to Consultation, and Final Decision(s).

Annex: 1 Legal Basis

A 1.1 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[57];
- contribute to the development of the internal market[58];
- promote the interests of users within the Community[59];
- ensure the efficient management and use of the radio frequency spectrum in Ireland in accordance with a direction under Section 13 of the Act of 2002[60]; and
- promote efficient investment and innovation in new and enhanced infrastructures[61].

A 1.2 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 of 2023"), and by means of the European Union (Electronic Communications Code) Regulations 2022 ("Code Regulations").

A 1.3 Section 11(1) of the Act of 2023 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". [62]

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

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

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

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

[61] 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").

[62] This transposes Article 40(2) of the EECC.

A 1.4 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 of 2023.

A 1.5 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 1.6 A further new element of the security provisions of the EECC, now transposed in the Act of 2023, 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.

A 1.7 Article 2(7) of the EECC defines "number-independent interpersonal communications service" as meaning "an interpersonal communications service[63] 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"[64].

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

[64] For guidance on how the security provisions of the EECC apply to NIICS, see Recital 95.

A 1.8 Section 11(3) of the Act of 2023 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. ComReg's power under section 11(3)(g) to specify such other information should be noted in particular.

A 1.9 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 1.10 Further to section 11(5), of the Act of 2023, 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 1.11 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 1.12 It should be noted that further to section 11(8) of the Act of 2023, 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.

A1.13 Under section 13 of the Act of 2023, ComReg shall take reasonable steps to ensure that providers comply with the obligations placed on them by or under Part 2 of the Act.

A1.14 This consultation is without prejudice to any future developments in the legislative framework, including any regulatory changes brought about by the transposition of the NIS2 Directive[65]. This consultation is also without prejudice to the implementation of the Critical Entity Resilience Regulations[66].

[65] Directive 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.

[66] S.I. No. 559/2024 – the European Union (Resilience of Critical Entities) Regulations 2024.

Annex: 2 Updated Templates

A 2.1Initial and Update report template

A single template is used for initial and update reporting for weather related events and is referenced as “Weather Event Initial and Update Reports Template Draft for Consultation ComReg 25/84a”.

A 2.2 Root Cause Analysis report template

A more expansive template is used for the final or Root Cause Analysis (RCA) report for weather related events and is referenced as “Weather Event RCA Template Draft for Consultation ComReg 25/84b”.

Annex: 3 Definition of Terms

A 3.1Fixed ECN/ECS

The fixed network overview is attached in Figure 1 below. The exact deployment will vary dependent on whether the access network is wholesaled or not, the exact equipment used on the end user's premises, the technology employed to deliver the service and the location of the network components.

For example, in dense urban areas underground ducting may be used for cable runs, while in remote rural area such cable runs may be strung overhead along pole infrastructure. Service deployed on DOCSIS technologies in urban areas may well be eave strung from house to house directly as opposed to across a pole infrastructure.

Traditional PSTN equipment in the end user premises is a standard telephone cabled using a copper connection directly to the local node from where power is delivered to the phone. DSL services would have powered units in the end user premises such as an Network Termination Unit (NTU) and Home Gateway or router. Fibre based services will have powered units such as the Optical Terminal Unit (ONT) and Home Gateway. Depending on the Retail/Wholesale split of the topology the NTU/ONT may belong to the Wholesale provider network while the Home Gateway could belong to the Retail provider. In some deployments the ONT and Home Gateway may be combined in a single unit. Depending on these topology variances the equipment is visible or managed by a provider may change.

In the case of Fixed Retail providers the deployed network may only consist of Core Network, some transmission interconnects and the Customer Premises Equipment (CPE) deployed beyond the Wholesale/Retail demarcation point.

For NI-ICS providers this may further reduce to Core Network and interconnection points.

The network architecture shown in Figure 1 below is broken into three main sections, namely, the Core Network, Transport Network and Access Network.

Core network includes the central nodes of functions for management of customer identity and associated services available, billing capability, traffic management and routing, and operational platforms for overall management of these network functions. As this is the heart of the network, the core network is usually deployed in secure data centres with full power back-up due to UPS, batteries and generators as well as a geo-redundant high availability configuration. This means if any one node or even a location should suffer a service interruption the end user services should remain operational.

The transport network includes the interconnection between Core nodes, other networks and the access network. The transport network is also, where possible, deployed with redundancy so if one connection fails another can take over. This is generally the case higher up in the core network but becomes more costly and problematic to deploy in the access network.

Finally the access network includes the infrastructure to connect the end user to the core network for the provision of services. As the access network is likely the most exposed part of the network and suffered the greatest impact from storm Éowyn this has been drawn in greater detail in Figure 1. The physical access path is the route between main access network nodes such as the DSLAMs, MSAN's, ONT's (depending on the technology used for access) and the user CPE. How the CPE is deployed depends on the Retail/Wholesale demarcation architecture and this also results in what elements along the physical access path the Wholesale provider can see and manage and what elements the Retail provider can see and manage.

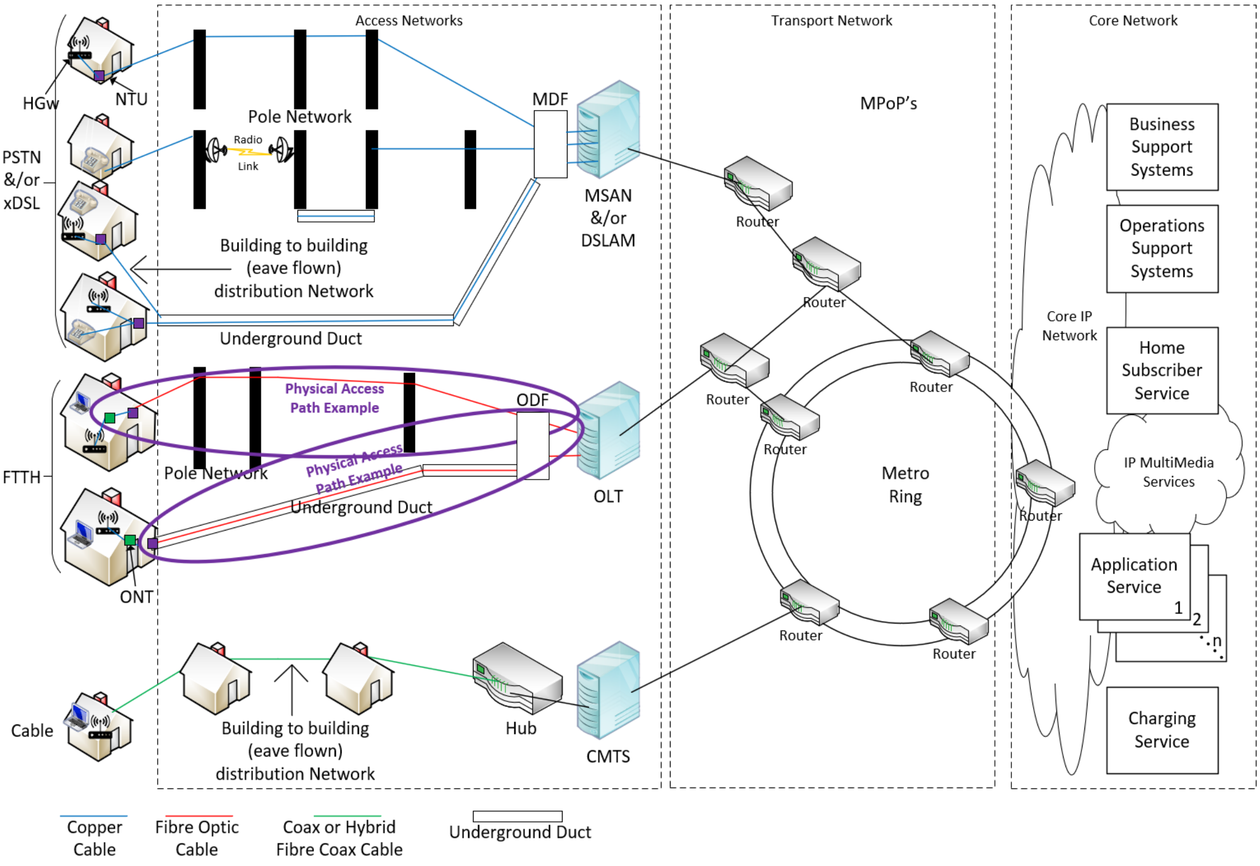

Figure 1: Fixed network architecture

The following is a list of the terms used in the templates for the fixed network and services including a definition:

Term	Definition
Total Number of Service Users Affected Per Area (all faults including those related to node faults and/or those related to physical access path faults)	This is the total number of users in the stated geographical reference area that lost service for any reason across the full extent of the network due to the incident.
Number of users with mitigations to minimise the impact of the incident	This is the number of users who had partial of full service restored by workaround or alternative methods while awaiting repair of the affected service.
Fixed Access Network, Number of Connected Physical Access Paths affected	This is the number of access paths per area based on the access path identity that were affected by the incident.
Access Network: No. of CPE's (HGw, ONT, NTU etc.) affected	This is the total number of CPE's affected by the incident but not including those lost due to a general loss of power to the premises. This is typically where power is established to the premises but for some reason (software lock up or power surge) the CPE (HGw, ONT, NTU etc.) was damaged and did not recover. It results in some recovery action being needed on the part of the provider.
Fixed Access Network, No. of Nodes/Exchanges affected	This is the total number of access network nodes per area affected by the incident .
Fixed Transport Network: No. of Nodes affected	This is the total number of transport network nodes per area affected by the incident.
Fixed Core Network: No. of Nodes affected	This is the total number of core network nodes per area affected by the incident.
Fixed Access Network, No. of Nodes/Exchanges at Risk	This is the total number of access network nodes per area that are currently functioning but may be at risk of going off air if some other action is not taken. Such action may be clearance of site access to allow generator refuelling or restoration of power before on site batteries discharge and the node is lost.
Number of Users at Risk	This is the total number of users that would lose service if the identified action needed to prevent loss of service to nodes "**at Risk**" above is not taken.
Utility Power input cause (affected and at risk)	This is the total number of nodes per area where the root cause of the service loss is loss of power from the utility provider to the node. It should be

	the addition of both nodes with service lost already plus nodes at risk due to power loss.
Access cause (affected and at risk)	This is the total number of nodes per area where the root cause of the service loss is due to loss of the access normally facilitated by the site provider to the node. It should be the addition of both nodes with service lost already plus nodes at risk.
Other main causes of outages	This a summary of other causes of service loss from access nodes, such as major transmission outage due to loss of a hub or interconnection site.
Estimated time to repair (ETR) 95% of issues	This is the estimated time to recover 95% of the faults or service interruptions in the area.
Service	This is the service affected by the incident (One of Fixed Voice or Fixed Broadband).
Notes	This is a free text field that can be used to add further information that may be useful to the response and recovery agencies. i.e. it may add further information to the activities needed to secure the nodes at risk just as one example.
Total number of user hours lost	This is the number of users affected multiplied by the duration of the service impact.
Total Number of Nodes (e.g. PoP, Exchanges, DSLAMs etc.) Deployed Per Municipal District	This is the total number of nodes that are deployed in the network broken down per geographical reference area. It includes all nodes, those impacted by the incident and those that are not.
Total number of Nodes affected	This is the total number of nodes per geographical reference area in the network that are affected by the incident.
Number of Nodes impacted by Power Failure	This is the total number of nodes per geographical reference area in the network that are affected by power loss from the utility service.
Number of Nodes Physically Impacted	This is the total number of nodes per geographical reference area in the network that are directly impacted by the incident. This can be a pole or cable broken by a storm event, a node that is physically impacted by debris or flooding, a transmission hub lost due to structural damage etc.
Number of Access Path Faults	This is the total number of access paths faults per geographical reference area.
CPE Outage (Router/Home Gateway, ONT, NTU, etc.)	This is the total number of CPE’s affected by the incident but not including those lost due to a general loss of power to the premises. This is typically where power is established to the premises but for some reason (software lock up

	or power surge) the CPE (HGw, ONT, NTU etc.) was damaged and did not recover. It results in some recovery action being needed on the part of the provider.
Number of Poles Affected	This is the total number of poles in the network damaged by the incident and counted per geographical reference area.
Number of Nodes with TXN Damage	This is the total number of nodes per geographical service area that suffered service impacts by loss of transmission to the node but the node itself was not damaged by the incident.
Number of Nodes where Access Issues limited Repair Capability	This is the total number of nodes per geographical service area that suffered service impacts and where recovery of the node was hampered due to access restrictions resulting from the incident.
Average Time to Repair for All Faults	This is the average time taken to repair all faults per geographical area and is calculated as the sum of repair time for each fault divided by the number of faults.
Maximum Time to Repair all faults	This is the time to repair all faults within the geographical reference area resulting from the incident measured from the start of the first fault created by the incident to the time of recovery of the last fault to be repaired.
Fixed Core: Number of nodes affected	The total number of Core Network nodes that were affected by the incident.
Fixed Transport: Number of nodes affected	The total number of Transport Network nodes that were affected by the incident.
X	ITM Easting Coordinate of network element or customer premises expressed in IRENET95 format (minimum 6 digits).
Y	ITM Northing Coordinate of customer premises or network element expressed in IRENET95 format (minimum 6 digits).
Eircode	Eircode of the customer premises for which service is impacted

A 3.2Mobile ECN/ECS

The mobile network overview is attached in Figure 2 below. Unlike the fixed network, mobile networks deployed in Ireland follow the same high level architecture as standardised by 3rd Generation Partnership Project (3GPP) and so all three deployed mobile networks have similar basic structure and use well understood and common terminology.

As with the fixed, however, this architecture can be broken down in Core, Transport and Access Network segments. The main differences will be Core Network nodes that are required to manage the mobility of the customer devices and the fact that the access is over the air instead of copper or fibre. Therefore, the local access node, known generally as the radio base station, serves a varying number of users due to their mobility whereas the fixed network access node will have a clearly defined number of users served based on the number of circuits physically cabled to the node[67].

The mobile core network includes nodes for handling customer account information and billing, subscriber identity management and security, user mobility and service management (establishment, continuity and release) as well as the operation platforms for network and node management. As with the fixed network, the mobile core is also usually deployed in a high availability, georedundant configuration across two or more data centres.

The transport network is similar in nature to that of the fixed network and in some cases they may even be the same.

In mobile networks the access network is known as the Radio Access Network (RAN) and this is based on an air interface connection between the end user devices (mobile phones and Subscriber Identity Module (SIM) enabled laptops etc.) and the access network itself. The network side node of the RAN is the mobile base station and these are deployed throughout the geographical area to be served. Base stations are connected back to the core typically over fibre but where fibre is not available other radio technologies may be used. Base station transmission links may be chained together from one base station to the next in order to reach more remote areas.

[67] This applies to fibre and copper networks. While fixed services may be delivered using radio through a Fixed Wireless Access product, the number of users will still be known as the end user device, while radio based, will not be mobile.

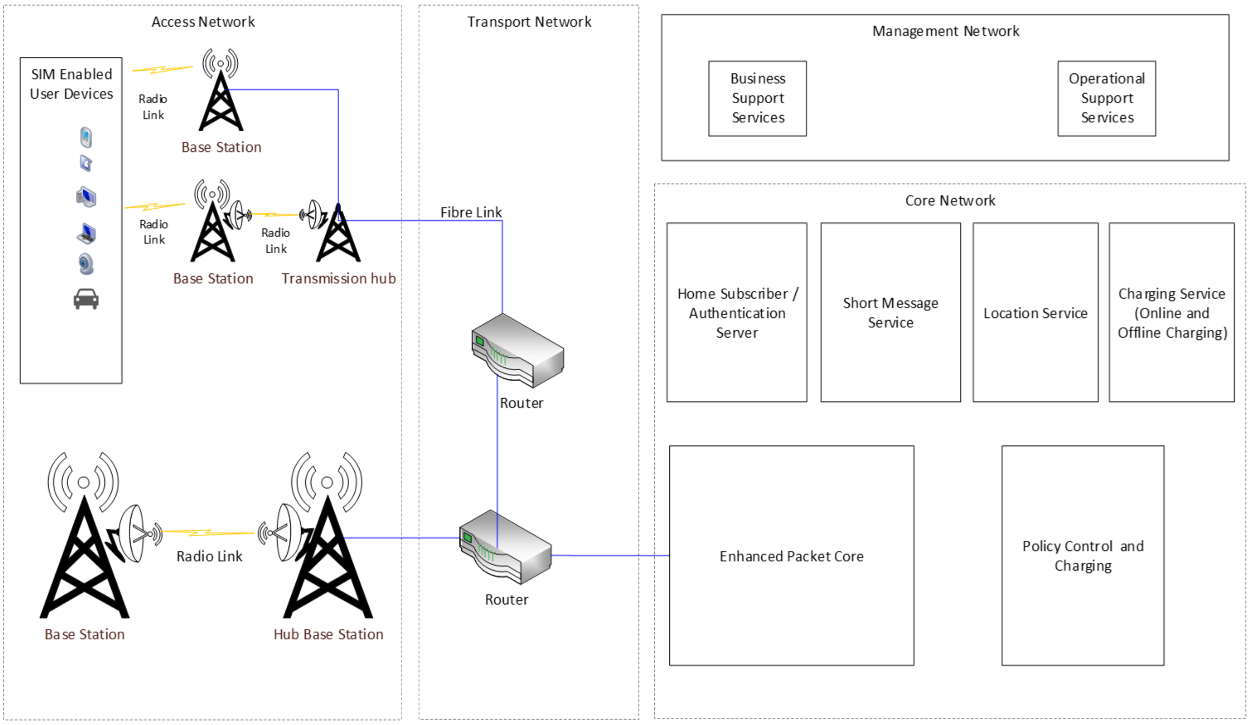

Figure 2: Mobile network architecture

The following is a list of the terms used in the templates for the mobile network and services including a definition:

Term	Definition
Total Number of Service Users Affected Per Area (all faults) [as per agreed calculation methodology]	This is the total number of users in the stated geographical reference area that lost service for any reason across the full extent of the network due to the incident. In the case of mobile base stations the number of users affected by the loss of a base station is calculated as the average number of unique users served per day by that bases station trended over a three month period prior to the incident. It is understood that where two neighbouring base stations are lost there may be double counting of the users affected where a single user is regularly served by the two neighbouring base stations.
Total number of users with mitigations to minimise impact of incident	This is the number of users who had partial of full service restored by workaround or alternative methods while awaiting repair of the affected service.
Radio Access Network, No. of Sites (e.g. Base Stations or TXN Hub sites) affected	This is the number of radio access network nodes per area that were affected by the incident.
Mobile Transport: No of nodes affected	This is the number of transport network nodes per area that were affected by the incident.
Mobile Core Network: No of nodes affected	This is the total number of core network nodes per area affected by the incident
Number of Nodes (all types Base Stations, Transport or Core) at Risk	This is the total number of mobile network nodes per area that are currently functioning but may be at risk of going off air if some other action is not taken. Such action may be clearance of site access to allow generator refuelling or restoration of power before on site batteries discharge and the node is lost.
Number of Users at Risk	This is the total number of users that would lose service if the identified action needed to prevent loss of service to nodes "**at Risk**" above is not taken.

Utility Power input cause (affected and at risk)	This is the total number of nodes per area where the root cause of the service loss is loss of power from the utility provider to the node. It should be the addition of both nodes with service lost already plus nodes at risk due to power loss.
Access cause (affected and at risk)	This is the total number of nodes per area where the root cause of the service loss is due to loss of the access normally facilitated by the site provider to the node. It should be the addition of both nodes with service lost already plus nodes at risk.
Other main causes of outages	This a summary of other causes of service loss from access nodes, such as major transmission outage due to loss of a hub or interconnection site.
Estimated time to repair (ETR) 95% of issues in area	This is the estimated time to recover 95% of the faults or service interruptions in the area.
Service	This is the service affected by the incident (One of Mobile Voice or Mobile Broadband).
Notes	This is a free text field that can be used to add further information that may be useful to the response and recovery agencies. i.e. it may add further information to the activities needed to secure the nodes at risk just as one example.
Total Number of Users Affected Per Area (all faults including those related to Access, Transport and/or Core faults)	This is the number of users per geographical reference area impacted by the incident. In the case of service from multiple base stations being lost it is the sum of the number of users per each base station (as defined earlier).
Total Number of User Hours lost	This is the number of users affected multiplied by the duration of the service impact.
Total Number of Base Stations/Nodes Deployed Per Area	This is the total number of nodes that are deployed in the network broken down per geographical reference area. It includes all nodes, those impacted by the incident and those that are not.
Number of Base Station/Node Impacted	This is the total number of nodes per geographical reference area in the network that are affected by the incident.

Number of Base Stations/Nodes impacted by Power Failure	This is the total number of nodes per geographical reference area in the network that are affected by power loss from the utility service.
Number of Base Stations/Nodes with Mast/Tower Damage	This is the total number of nodes per geographical reference area that suffered structural damage due to the incident.
Number of Base Stations/Nodes Antenna, Remote Radio Unit, Active Antenna Unit and/or Mounting Damage	This is the total number of nodes per geographical reference area that suffered damage to the radio equipment but excluding structural damage.
Number of Base Stations/Nodes with Mobile Backhaul TXN Damage	This is the total number of nodes per geographical reference area that suffered damage to transmission serving the node due to the incident.
Number of Base Stations/Nodes where Access Issues limited Repair Capability	This is the total number of nodes per geographical reference area that suffered restrictions to access to the site or the equipment due to the incident.
Average Time to Repair for all faults	This is the average time taken to repair all faults per geographical area and is calculated as the sum of repair time for each fault divided by the number of faults.
Maximum Time to Repair (start time of first fault till recovery time of last fault)	This is the time to repair all faults within the geographical reference area resulting from the incident measured from the start of the first fault created by the incident to the time of recovery of the last fault to be repaired.
Mobile Core: Number of nodes affected	The total number of Core Network nodes that were affected by the incident.
Mobile Transport: Number of nodes affected	The total number of Transport Network nodes that were affected by the incident.
X	ITM Easting Coordinate of the network entity expressed in IRENET95 format (minimum 6 digits).
Y	ITM Northing Coordinate of the network element expressed in IRENET95 format (minimum 6 digits).