An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Response to Consultation and Decision on the Network Incident Reporting Thresholds

Non-confidential Submissions to Document 23/36

Submissions to Consultation

Reference: ComReg 24/23a

Version: Final

Date: 02/04/2024

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

Submissions Received from Respondents

Document No:	24/23a
Date:	02 April 2024

Consultation:	23/36
Response to Consultation:	24/23

Content

1 eir

eir

Response to ComReg Consultation:

Network Incident Reporting Thresholds

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

ComReg Document 23/36

25 May 2023

DOCUMENT CONTROL

Document name	eir response to ComReg 23/36
Document Owner	eir
Status	Non-Confidential

The comments submitted in response to this consultation document are those of Eircom Limited and Meteor Mobile Communications Limited (trading as ‘eir’ and ‘open eir’), collectively referred to as ‘eir Group’ or ‘eir’.

Response to consultation

1. eir welcomes the opportunity to contribute to the consultation process. eir notes that ComReg is seeking to build on the existing pragmatic approach to incident reporting and welcomes that intent.

2. eir is generally supportive of the proposed changes for the new regime subject to certain clarifications suggested below.

Q.1 Do you support the proposed thresholds, further information requirements and incident typification outlined in this document?

3. eir has no objection to the reporting regime being expanded to include security incidents, the proposed thresholds, and formalise existing arrangements for storm reporting. eir requests clarification as to whether ComReg will assume a single point of contact role for reporting of all incidents or whether Providers will continue to be required to report some incidents to NCSC (CSIRT) in addition. A single point of contact would seem to be a more efficient and pragmatic approach.

4. eir agrees with ComReg's proposed aim to maintain consistency with the ENISA guidelines setting qualitative thresholds by reference to the National User Base. In the interest of clarity eir believes it would be helpful if ComReg could clearly identify and publish the relevant National User Bases each time the Quarterly Key Data Report is published.

5. eir requests clarification on how the National User Base for Number Independent – Interpersonal Communications Service (NI-ICS) will be calculated. At paragraph 115 ComReg states "*For NI-ICS, providers may sum the number of active users, within the State, of the services in the end of a period*". This suggests that NI-ICS providers will be responsible individually or collectively to calculate the National User Base. This does not seem appropriate as it raises questions of impartiality and commercial confidentiality. The ENISA Technical Guideline states on page 21 that "*For NI ICS **CAs** may sum up the number of active users of the services in the end of a period*" [emphasis added]. This places the responsibility on the national Competent Authority, i.e. ComReg, which we believe is the correct place for this responsibility to sit. The NI-ICS National User Base should be published alongside the other National User Bases on a quarterly basis.

Q.2 Do you agree with the proposed timelines and processes for reporting incidents outlined in this, and the draft Decision, document?

6. eir agrees with the proposed timelines and processes subject to the following comments.

7. eir assumes the reporting template will be rejigged consistent with the proposed Decision and existing required information that is now redundant, such as the number of mobile sites impacted, will no longer be mandatory fields. We look forward to ComReg's confirmation.

8. Section 3 of the proposed Decision Instrument sets out the information required to be contained in a notification to ComReg. The categories of information are uncontroversial with the exception of "*(i) the impact of the incident on economic and societal activities*". eir does not agree that this should be included in the notification requirements. Provider Service Management Centres (SMC) do not have the skillset to assess the socio-economic impacts of an incident. Nor is it appropriate that they should have to undertake such analysis as the SMC focus should correctly be on resolving incidents.

9. There appears to be some confusion regarding this category of information. As noted in the ENISA Technical Guidelines the consideration of socio-economic impact is relevant to determining the significance of an incident and whether reporting should be triggered. The European Electronic Communications Code also makes reference to this consideration in the context of determining significance thresholds in Article 40 but is silent on this category being a mandatory feature for every incident report. eir notes that section 11(2) of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 lists this as a feature in determining significance but also, in section 11(3) requires this information to be included in individual reports. However this raises questions of proportionality both in terms of whether Providers have the necessary skillsets to conduct such assessments, and whether the need for an impact assessment could negatively impact on a Provider's ability to report incidents in a timely manner. From a Provider's perspective we believe the operation of the incident reporting regime should be maintained on objective criteria. Hence consideration of socio-economic impact should be inherent in the reporting thresholds in section 1 of the proposed Decision Instrument.

10. If, in the alternative, an obligation is to be maintained on Providers to include "*the impact of the incident on economic and societal activities*" in an incident report, ComReg must

develop and publish for consultation a draft Guideline on how the socio-economic impact is to be assessed for inclusion in an incident report.

11. eir notes sections 8 to 10 of the proposed Decision Instrument relate to how ComReg will address Information Required by the Minister, European Commission, Other NRAs and ENISA. Whilst this is important to know in the context of the overall incident reporting regime it is not clear if this text is appropriate in a Decision Instrument that is addressed to Providers.

2 ENEA

Submission to ComReg Consultation on Network Incident Reporting thresholds

Enea AB

Date: May 25 2023

Commission for Communications Regulation

Ireland

Via: marketframeworkconsult@comreg.ie

May 25th, 2023

Dear Commissioners,

Enea AB commends ComReg for providing the opportunity for public consultation to the development of network incident reporting thresholds and is pleased to make this submission for consideration.

As an acknowledged world leader in software for telecoms and cybersecurity, we appreciate the opportunity to contribute our international perspectives on the security of mobile networks and mobile communications.

Enea is frequently called on to share insights and expertise with governments, regulators and at industry events, and we are pleased to make our team available for follow up briefings or clarifications at the pleasure of ComReg.

Sincerely,

Rowland Corr, VP Government Relations, Enea

Rowland.corr@enea.com

Phone +353 1 524 9059

CORPORATE HEADQUARTERS

P.O. Box 1033

Jan Stenbecks Torg 17

SE-164 21 Kista

Sweden

Phone: +46 8 507 140 00

www.enea.com

Table of Contents

1. About Enea AB

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

Enea's software portfolio includes:

• Signalling, messaging and voice protection trusted by the world's largest Mobile Network Operators and CPaaS providers to secure communications infrastructure and services. The portfolio includes signalling, messaging, and voice managed firewalls, A2P (application to person) revenue protection and commercial traffic management solutions, as well as signalling & messaging intelligence services.

• 5G Data Management solutions to unify subscriber and session data across network functions, and policy and access control products for efficient utilization of network resources and authentication of subscribers. The portfolio includes the Enea Stratum Cloud Data Manager, the Enea Unified Data Manager, the Enea Policy Manager, and the Enea Access Manager.

• Traffic Management – Enea mobile video traffic management solutions alleviate radio network congestion, accelerate video delivery, reduce network energy consumption, and improve subscribers' quality of experience. The portfolio supports 5G and includes the Enea Encrypted Video Manager, the Enea RAN Congestion Manager, and the Enea TCP Accelerator.

• Enea's embedded traffic intelligence products classify traffic in real-time and provide granular information about network activities. The portfolio includes the Enea Qosmos ixEngine and the Enea Qosmos Probe. The products support a wide range of protocols and are delivered as software development kits or standalone network sensors to network equipment manufacturers, telecom suppliers, and vendors of cybersecurity software.

Enea's industry leadership in mobile network security

Enea is an active member of the GSMA Fraud and Security Working Group, and key contributor to development of industry standards including the *GSMA Fraud and Security Group's (FASG's) FS.36 "5G Interconnect Security" reference document for GSMA members, as well as FASG's FS.11 "SS7 Interconnect Security Monitoring and Firewall Guidelines".*

In March 2023, Enea was invited to present to the European parliamentary enquiry into Pegasus Spyware. The representation by VP Government Relations Rowland Corr can be viewed here https://multimedia.europarl.europa.eu/en/webstreaming/committee-of-inquiry-to-investigate-use-of-pegasus-and-equivalent-surveillance-spyware_20230316-0900-COMMITTEE-PEGA

Recent white papers and research publications include:

https://info.adaptivemobile.com/defending-telecoms-against-nation-state-cyber-threats

https://info.adaptivemobile.com/mobile-network-enabled-attacks-in-hybrid-warfare

Further reports and insights can be found on www.enea.com and www.adaptivemobile.com

2. Introduction : Enea's response to the Consultation.

Enea makes this submission to ComReg in response to indication in the Consultation document (reference: ComReg 23/36, dated 24th April 2023) that ComReg do not intend to consider qualitative reporting thresholds for inclusion in the new framework. This submission sets out why the inclusion of qualitative reporting thresholds is essential for:

- Alignment with ENISA's recommendation in its Technical Guidance for incident reporting under the European Electronic Communications Code (2021) that both qualitative and quantitative thresholds "should be applied" in order to capture significant security incidents today;
- Alignment with ENISA's call in 2018 for National Regulatory Authorities to: "consider revising the national legislation (if needed) so that signalling security should be covered in terms of reporting incidents and adopting minimum security requirements"[1];
- Enabling vital lessons to be learned and shared with ENISA, supporting improved resilience of networks through the EU and helping to mitigate further propagation of incidents.
- Avoidance of leaving a gap in reporting by operators to ComReg of security incidents which involve the threat of significant societal or economic harm which could not be captured by purely quantitative reporting thresholds such as the suggested 1% of operator's national user base.
- Avoidance of any adverse knock-on effect on operators' approaches to resourcing threat detection capabilities which could arise from such a gap in reporting requirements;
- Avoidance of a resultant potential deficiency in ComReg's Network Operations function in respect of:
    - "evaluating the resilience, security and integrity of electronic communications networks and services;
    - managing and collating the reporting of network incidents across all electronic communications networks and services;
    - liaising with State and International agencies – such as the European Union Agency for Cybersecurity (ENISA), as appropriate, on matters related to network incidents";[2]

To illustrate the necessity of including qualitative reporting thresholds, this submission highlights the relevance of security incidents involving mobile signalling-related threats which form a distinct but far from discrete area of telecom security risk today and one of potentially profound societal and economic impact moreover which cannot be captured by quantitative reporting thresholds alone.

The signalling threat landscape is dynamic in nature and global in scope. All too often it is also an unreported and, worse, an uncontested landscape as threat actors exploit access to mobile signalling resources to manipulate network operations in targeting activities worldwide. Access to mobile signalling systems is abused by threat actors to remotely exfiltrate personal information in the form of unique identifiers for subscribers and other exploitable

[1] ENISA (2018) Signalling security in telecom SS7/Diameter/5G: EU level assessment of the current situation.
[2] https://www.comreg.ie/about/our-team/market-framework/

information. An important element of this risk is the relative powerlessness of subscribers to protect themselves against unauthorized intrusions or data leakage over mobile signalling vectors as such threats manifest at the network level.

Mobile subscribers take for granted that phones can seamlessly switch between 3G, 4G and 5G, however a downside of this layered approach is that some legacy vulnerabilities persist. A signalling system (SS7) deployed since the 70's for legacy networks, is notoriously open to abuse and remains in operation and targeted by newer surveillance tools. Other signalling protocols too such as Diameter and GTP are also at risk. Indeed, advanced attackers have the ability to conduct cross-protocol attacks. While 5G networks are designed to be more secure across network interfaces and with user identity management, the upcoming ubiquity of 5G means the attack surface has drastically spread. Malicious inbound signalling could penetrate the core or "brain" of networks, leading to user meta-data theft, call rerouting, or even hijacking location tracking services.

The global nature of the attack surface is owed to the fact that signalling infrastructures enable, support, and control interconnection between networks nationally and internationally, primarily governed by commercial agreements where security has not been a primary focus. This was the natural result of deregulation and opening of the telecom markets wherein the ability for operators to open their networks and to partner with multiple service providers served as an important business enabler for operators, and service enabler for consumers.

The exploitation of this openness, and an absence of protective measures to mitigate the technical vulnerabilities to attack have made the interconnect environment perilous, putting all countries at risk of hostile targeting efforts by external state-level threat actors.

3. Addressing a potential blind spot in reporting, capabilities, and resilience.

It is stated in the Consultation document that "ComReg does not propose to include qualitative thresholds at this time, although it may revisit this matter in the future"[3]. Accordingly, the two policy options outlined in the draft recommendation comprise (1): maintaining the status quo (para.76), and (2): the setting of exclusively quantitative thresholds per Section 6.2.2 of the ENISA Revised Guidelines (para.81).

Enea urges ComReg to reconsider its position regarding qualitative thresholds for incident reporting on the basis that their exclusion risks leaving Ireland blind to mobile signalling-borne threats. These include, inter alia: the unlawful surveillance of citizens, data exfiltration, and data leakage, which would not be captured by the suggested quantitative reporting thresholds yet could pose potentially significant impacts on societal security. Moreover, such a position would fall short of ENISA's clear recommendation in the updated Technical Guideline (2021) which states that:

> *"Quantitative thresholds are clear and easy to understand, but they do not always apply to all situations. The total size of the incident, the number of users, or hours, is not always the main significance factor. Sometimes a small incident, in terms of users, or hours, can be very significant.* ***Therefore, qualitative thresholds are needed in addition to the quantitative thresholds. Overall, all thresholds should be applied****". (ENISA, 2021, emphasis ours).*

The import of ENISA's recommendation that "all thresholds should be applied" is clear. It is not merely to suggest that for some incidents there may be a qualitative significance factor to consider in addition to the requisite level of quantifiable impact, but that there can occur

[3] para. 80

today significant incidents which might only be captured by qualitative reporting thresholds because the numbers of victims (and/or hours of duration of attack) falls below quantitative thresholds (such as the cited threshold of 1% of the impacted operator's national user base, which in the case of Vodafone Ireland would amount to approx. 20,000 subscribers based on publicly available data for Q4 2022).

ENISA illustrate the necessity in several examples, such as the following:

> *'For example, Illegal tapping of more than 100 mobile phones on the XX network belonging mostly to members the government and top-ranking civil servants it is categorised as an incident with impact on economy and society'. (p.27).*

Another example involves a single victim subject to data theft through interception over an unprotected network (p.30). It is clear from the examples that ENISA's call for the consideration of qualitative and quantitative thresholds is not meant to present an either/or choice, but a matter of *both-and* necessity.

These examples are consistent with attacks observed today over signalling networks which pose potentially significant threats to Confidentiality, Integrity, and Authenticity of networks and services with potentially profound societal and economic impact.

The nature of the potential threat posed by signalling-enabled attacks has been highlighted in recent media reporting[4] in respect of a private company alleged to have utilised signalling systems access to facilitate election interference worldwide. Enea AdaptiveMobile Security's Threat Intelligence Unit has observed malicious traffic consistent with the social media account hijacking described in the reporting, confirming that this potentially severe societal threat is a very real part of the security landscape today.

The exclusion of qualitative reporting thresholds risks effectively precluding any possibility for the reporting by operators of this kind of targeting and other significant incidents compromising the Confidentiality, Integrity, and Authenticity of networks which do not reach quantitative thresholds for reporting.

4. Interconnect attacks - an increasingly recognised societal threat:

The exclusion of qualitative thresholds from the new incident reporting framework would largely exclude **interconnect attacks** altogether as a category of threat despite it being one of 10 major industry threats currently identified by the GSMA. The sum of such an exclusion is more than simply one of many types of attack however, since interconnect attacks are also relevant to wider threats such as spyware, as has been recently been recognised in 2023 both by the GSMA[5] and by the European Parliament[6].

For the very same reason moreover, there is also a distinct risk that the exclusion of qualitative reporting thresholds would result in a reduced likelihood that operators will resource the necessary capabilities to be able to detect signalling-borne threats, leaving Ireland vulnerable to significant security risks. Today, amid an environment in which data leakage and data manipulation in addition to data breaches are increasingly relevant as highlighted by the latest ENISA Threat Landscape report[7], this would leave a growing blind spot in Ireland's national network security.

[4] https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000

[5] https://www.gsma.com/security/resources/gsma-mobile-telecommunications-security-landscape-2023/

[6] https://www.europarl.europa.eu/doceo/document/B-9-2022-0664_EN.pdf

[7] https://www.ENISA.europa.eu/publications/ENISA-threat-landscape-2022

The risk of a suppressive effect on operators' capabilities arising from the absence of explicit obligations necessitating their provision is acknowledged by ComReg itself in the consultation document. This is acknowledged with regard to Option 1 (status quo), where it is stated, by way of highlighting this very risk, that "operators would not be required to report incidents that relate to confidentiality, authenticity, and integrity and could lead to under provisioning of such factors." (para. 96). It is notable moreover that ComReg highlight, if implicitly, how this might be avoided where operators are incentivised through explicit reporting requirements to resource the relevant factors.

For the very same reason that the absence of an express requirement regarding confidentiality, authenticity, and integrity could lead to a deficiency in reporting capability, the exclusion of qualitative reporting requirements could lead to under-provisioning of factors pertaining to potentially significant impacts which the suggested quantitative threshold cannot capture.

Importantly moreover, where there has historically been no such reporting requirement in effect, it holds that the very same potentially suppressive effect may have left signalling protection already underprovisioned, that is to say, deficient. Here too therefore, there is an imperative to address this incentive deficit.

Explicit qualitative reporting requirements may provide the key incentive for operators to ensure they have the capability to detect and report significant incidents with societal impact which are not captured by the suggested quantitative thresholds. At the same time, this would enable the vital learning and development of best practices that is also emphasised by ComReg in the Consultation document.

As part of ComReg's explanation of why qualitative thresholds are not proposed for inclusion, reference is made to the existing monitoring capabilities of operators which have historically enabled them to voluntarily provide reporting beyond the letter of their obligations. This is cited by ComReg by way of indicating assurance of effective, suitably comprehensive capture of threats. No such assurance can hold however in the case of signalling borne threats having qualitative impacts on Confidentiality, Integrity, and Authenticity, where conditions conducive to underprovisioning have prevailed up to the present time, as they arguably have based on Comreg's own rationale as cited above.

This is important because it means that unlike in the case of availability focused incidents quantitative impacts on availability where ComReg express confidence that operators already possess sufficient detection capability to provide reporting, there can be no such basis for confidence in respect of signalling borne threats to Irish networks and subscribers. ComReg cannot be confident therefore that operators will voluntarily report incidents they deem to be significant if it is not clear that they possess the requisite capability to detect them in the first place.

This is particularly salient at this time when the European Parliament PEGA Committee of Inquiry, recognising this very risk, have called expressly for national competent authorities promote the strengthening of operators' capabilities in respect of incident reporting, as reflected in para. 87 of the adopted report, which:

> *Calls on the competent national authorities to actively promote strengthening the capabilities of providers, as well as response capabilities, to better support the identification of persons illegally targeted, notification and incident reporting, in order*

to provide ongoing, measurable assurance and mitigation of the exploitation of security gaps by non-EU and domestic malicious actors (para. 87)[8]

While it is certainly possible for signalling-borne threats to confidentiality, integrity or authenticity to impact hundreds of thousands of users on a single network in a single incident, and meet quantitative reporting thresholds, and such instances have indeed been observed by Enea in the past, deliberate attacks tend to involve much smaller numbers today.

In other words, in most cases today attackers have no need to go near let alone to exceed typical quantitative thresholds to achieve their aims. The exclusion of qualitative thresholds can therefore effectively signal to attackers the safe upper limit for any single unauthorised intrusion in any single incident, where they might be assured that so long as their targeting remains below, for example, 1% of the national user base (which can be accurately calculated based on publicly available data) their activity will remain "off the radar" of operators and regulators.

5. Increasing relevance of signalling attacks requiring qualitative reporting thresholds:

In its most recent Threat Landscape Report, the EU's cybersecurity agency ENISA remarks on the increasing relevance of data manipulation and data leakage in addition to data breaches as components of threats to data which are also the basis for many other threats[9] posed to operator networks today.

This characteristic holds true of mobile signalling security threats which are fundamentally threats to data involving breaches, leakages, and manipulation of core network databases and functions by attackers exploiting security weaknesses in the interconnect environment.

The wide range of attacks enabled by signalling has been previously highlighted by ENISA in 2018:

- Interception.
- Location tracking.
- Infiltration attacks.
- Denial of Service.
- Spoofing.
- Subscriber Fraud.
- Spam.

It merits remarking that at that time, ENISA called for national regulatory authorities to: "consider revising the national legislation (if needed) so that signalling security should be covered in terms of reporting incidents and adopting minimum security requirements"[10].

Now 5 years on, we can add further threats to this list. The intersection between signalling-enabled threats and other forms of cyberattack has been increasingly recognised by industry and government stakeholders worldwide. Perhaps of prime importance in this regard is the intersection between signalling security threats and spyware-related threats in terms of the actors, attacks, and ecosystem involved.

[8] https://www.europarl.europa.eu/doceo/document/B-9-2022-0664_EN.pdf
[9] Page 8, ENISA Threat Landscape Report 2022
[10] ENISA (2018) Signalling security in telecom SS7/Diameter/5G: EU level assessment of the current situation.

Recognition of this wider relevance of the interconnect environment is reflected in the GSMA Security Landscape Report for 2023 where it states with regard to spyware attacks that: "[f]or network operators, close attention to SS7 signalling traffic, including the deployment and correct configuration of signalling firewalls, is crucial." (p.17). Moreover, it is notable also that mobile signalling attack capability is a central element in 3 of the 6 cited examples of spyware-related threats in this section of the GSMA report (p.16).

So while interconnect attacks form a distinct category of threat, their potential impact is far from discrete from other categories of threat. Interconnect attacks are therefore important not simply as a single type among several, but as a fundamental threat to data implicating multiple areas of cybersecurity.

The resultant gaps in incident reporting left by the exclusion of qualitative incident reporting thresholds would ultimately restrict ComReg's ability to evaluate network security. By the same token however, their inclusion can serve as a prime enabler for operators to ensure they have the requisite capabilities to identify and report significant impacts and security incidents that might otherwise be missed.

Enea urges ComReg to include qualitative thresholds for reporting for consideration at this time as a vital element of an effective new framework which:

> "*contributes to the collection of reliable and up-to-date data on security incidents […] facilitates the rapid dissemination of information among interested parties, [and] provides valuable transparency to society*"[11]

ENDS

[11] https://www.comreg.ie/media/2023/04/ComReg-2336-2.pdf

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm. For more information: www.enea.com

CORPORATE HEADQUARTERS
P.O. Box 1033
Jan Stenbecks Torg 17
SE-164 21 Kista
Sweden
Phone: +46 8 507 140 00

www.enea.com

3 Imagine

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

Imagine agrees with the principle of the proposed thresholds, further information requirements and incident typification but has the following comments:

1. With regard to the requirements of Article 40 and specifically,

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

In terms of reporting security incidents relating to, "Confidentiality, Integrity, Authenticity or Availability" and "related services offered by, or accessible via those electronic communications networks or services ", such reporting can only be provided by the Operator for **incidents directly attributable and related to**, the network and systems within the Operator's direct control, namely those that are provided by the Operator. As such they should not include any services accessible via, or carried over the top of the Operator provided services for which the Operator has very limited or no control/visibility.

2. With regard to Section 4.2.2, para 111.

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

Imagine agrees with the requirement to report security incidents relating to Confidentiality, Integrity, Authenticity or Availability, but is of the opinion that the presentation of such within the document[1] has meant that many of the requirements remain vague and/or open to interpretation. As such, Imagine are of the view that further work is required to clarify same, perhaps in the form of industry workshop(s) with a brief to create more detailed guidelines/templates using the examples provided within Annexes A and B of the ENISA Technical Guideline document[2]. It's Imagines considered opinion that this would facilitate clear, consistent as well as practical reporting of such incidents, across all Operators and Service providers, whilst at the same time addressing for example, issues such as:

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

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

Imagine agrees with the proposed timelines and processes for reporting incidents outlined, subject to the comments provided above relating to the categorisation of incidents.

[1] ComReg 23-36 Network Incident Reporting Thresholds, A consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum-Security Standards)

[2] ENISA, TECHNICAL GUIDELINE ON INCIDENT REPORTING UNDER THE EECC, March 2021

4 Microsoft

Non-confidential Submission to ComReg Document 23/36

MICROSOFT CORPORATION

COMMENTS ON COMREG'S CONSULATION TO REVISE COMREG DOCUMENT 14/02 – REPORTING & GUIDANCE ON INCIDENT REPORTING & MINIMUM SECURITY STANDARDS

Microsoft appreciates the opportunity to comment on the proposed changes to ComReg's requirements for incident reporting and minimum security standards. We support ComReg's efforts to provide industry with clear and practical guidance regarding its expectations for incident reporting.

Microsoft provides widely-used internet-based communication services in Ireland and throughout Europe. Our customers depend on our services to originate millions of telephone and VoIP calls and app-based messages per month. We appreciate the importance of security and availability for communications services and have a particular perspective on incident reporting for those communications applications that are newly subject to reporting obligations under the EECC.

We recognize the need for telecom regulators to understand the severity and causes of disruptions to communications services and their availability on a timely basis. Likewise, as is reflected in the proposal, we recognize the importance of identifying those incidents that can have an impact beyond a standalone service or provider, for example, where there is a loss of a provider's ability to ensure the confidentiality, integrity, or authenticity of a service. However, within the broader scope of reporting requirements, where some types of services are more mission-critical than others, reporting thresholds and timelines should reflect those differences. For example, many internet-based services, particularly Number-Independent ICS, are not relied upon for availability in the same way as traditional telephone calling services or internet access services.

In these comments, we have provided recommendations for tailoring the guidance to incident reporting for internet-based services as well as addressing some of the challenges our operations would face if the current proposed rules were implemented. We hope that our input provides useful perspective to ComReg in modifying the final guidance to best reflect prioritizing incident thresholds for the most critical services and reporting timeframes that are realistic to allow providers an opportunity to focus on service restoration and incident response.

1. 'Significant Incident' Reporting Thresholds (Part III, Section (1))

1.1. Number-independent services (Availability Impact Reporting)

As noted above, availability reporting thresholds should reflect the differences between services that are relied upon for vital time-sensitive communications and those that are not. While Number-Independent ICS, such as email, instant messaging and non-PSTN VoIP, qualify as communications services under the EECC, they are not as mission-critical as, for example, telephone calling services that can be used to contact the emergency services. Moreover, they are often multi-homed, such that if one NI-ICS is not available, an alternative NI-ICS can be used. This is distinct from the features of traditional fixed and mobile voice lines and internet access lines. Finally, if a service is provided free of charge it suggests that it is less critical. Such services provided free of charge are basic, entry-level services with many readily

available substitutes that do not support vital societal functions. If there is an outage to a service that is provided free of charge, it is far less likely that there will be a material harm to the public interest because users can easily move – on a temporary or permanent basis – to another service.

Availability reporting thresholds should reflect these important distinctions and be narrowly tailored to ensure that reporting is only required where it is necessary to ensure access to vital communications services and protect consumers. Specifically, paid NI-ICS services should be subject only to ComReg's proposed absolute threshold of an impact to one million or more user hours. The reporting threshold for free of charge NI-ICS services should reflect the high degree of substitutability across these services and less-vital nature of free of charge NI-ICS, and as described below, should be based on the total Irish population. For example, Microsoft suggests that an availability impact to 15 percent or more of the Irish population for at least eight hours would be an appropriately tailored threshold for free of charge NI-ICS services to report an outage. We believe these NI-ICS impact thresholds more effectively account for the unique characteristics of NI-ICS services and are appropriately tailored to capture only those outages that are likely to have a significant impact on societal functions or harm the general public interest.

1.2. Enterprise services (Availability, Authenticity, Integrity, and Confidentiality Impact Reporting)

The draft decision guidance does not address enterprise services. Microsoft suggests that ComReg recognize explicitly that enterprises (not their employees) are the customers for purposes of counting thresholds. For example, the terms "User" and "User Hours" should be interpreted as referring to subscribers, at least with respect to enterprise customers (see footnote 92).

2. National User Base Calculations (Part III, Section (2))

2.1. Number-independent ICS

We ask that ComReg provide more clarity on the NI-ICS user base metric as there is no such figure in the Quarterly Key Data Report. We note that ComReg's proposed rules for the NI-ICS user base calculation appear to diverge from the other service categories by calculating impact based on the individual provider's total user base, rather than the national user base for the NI-ICS market as a whole. This would materially distort NI-ICS reporting obligations as it would overstate the user impact by significantly reducing the user-base denominator. Such an approach is not technologically neutral, as it would effectively impose a much lower threshold for NI-ICS than that for NB-ICS. Further, as previously discussed with respect to impacts to the availability of services, many of the public interest concerns underpinning availability impact reporting requirements do not apply equally to NI-ICS as they do to NB-ICS, as NI-ICS are generally less mission-critical and unlikely to result in significant societal harm.

Conversely, we also have concerns about trying to calculate a national user base for the NI-ICS market. First, because different types of services – ranging from email to app-based voice or messaging – are potentially captured within the NI-ICS definition, calculating the user base for NI-ICS as a whole would significantly overstate the market size and result in under-reporting. For example, if the impact of an email service outage is determined with a user base denominator that includes the wide range of non-email services that fall under the NI-ICS definition, the calculation would result in a much smaller user impact percentage than the actual impact to the email services. Also, unlike fixed or mobile voice services, many people subscribe to multiple services of the same type (e.g., email), so the size of the market would be further overstated if, as an example, the national user base for email services were to equal the aggregate

of all email service customers in Ireland. Finally, because these services often do not have fixed service term periods and free of charge NI-ICS do not have paid subscriptions at all, NI-ICS user bases are susceptible to larger fluctuations across time and events, making it more difficult to accurately capture a reliable user base metric.

Microsoft respectfully urges ComReg to adopt modified user base calculations for NI-ICS that rely on the best available proxies for the market size of each specific NI-ICS service type and are therefore more commensurate to user base calculations applied to NB-ICS. Specifically, instead of attempting to define a market where it can be difficult to ascertain actual users across competing services, ComReg should base thresholds on a percentage of the total Irish population. This approach would avoid under- or overstating the market size for NI-ICS and effectively reflect the multi-homed nature of the NI-ICS user base. By accounting for the high degree of substitutability across these services and considering the less-vital nature of NI-ICS, determining the user base according to the national population would result in a user impact threshold that is more equivalent to those applied to NB-ICS.

2.2. Voice services that are not fixed or mobile services

Microsoft urges ComReg to provide additional guidance on reporting for network-independent telephone calling services as internet-based services do not fall within either the fixed or mobile categories.

The proposed incident reporting guidance does not indicate which national user base should be used for telephone calling services that can be accessed from any internet connection. Such services can be used through a fixed or mobile data network. ComReg should clarify how the thresholds apply to nomadic/internet-based VoIP telephone calling services, for example, if the fixed voice calculation should be used.

In addition, the incident reporting requirements should recognize that some applications with limited telephone calling features are sufficiently different from fixed or mobile voice services that another threshold should apply. Apps that permit outbound calls to telephone numbers but cannot receive calls from telephone numbers (or vice versa) may qualify as Number-Based ICS, but they are generally not critical lifeline services as fixed or mobile voice services may be and therefore should not be subject to the same reporting thresholds as typical fixed or mobile voice services. The guidance document should reflect this difference in the incident reporting thresholds. For example, VoIP services that are within the definition of Voice Communications Services[1] could be subject to the reporting thresholds for fixed services because they are used in a similar way to fixed voice services as they permit subscribers to both make and receive telephone calls. In contrast, applications with NB-ICS features that do not qualify as a VCS could be subject to a different threshold, perhaps by applying a definition of 'significant incident' that is more aligned with NI-ICS reporting.

[1] 'Voice communications service' is defined as a publicly available electronic communications service for originating and receiving, directly or indirectly, national or national and international calls through a number or numbers in a national or international numbering plan. See European Union (Electronic Communications Code) Regulations 2022 (S.I. No. 444/2022), sec. 2.

3. Timing for Significant Incident Reporting (Part III, Section (5))

3.1. Initial reporting

We support the prompt reporting of significant incidents, but short reporting deadlines may delay the primary goal of service providers to restore service and respond to incidents. A 24-hour deadline for an initial report is too prescriptive and is not practical in most cases. Particularly for services that are not network-based, it may take time to gather enough information to determine that the relevant reporting threshold has been met. Instead of a 24-hour timeframe, we recommend requiring an initial report be provided within 72 hours of determining the incident qualifies as a significant incident.

We suggest that reporting requirements should reflect that incident response and service restoration must be the priority. In the event of a service disruption, a provider's engineers work diligently to restore service, an effort that should be paramount. Attempts to gather information from engineers for regulatory reporting during an active outage or incident detracts from the mission-critical necessity of incident response, particularly with a 24-hour deadline when response efforts are still ongoing, and in many cases with global implications. In addition, within 24 hours there often is not sufficient information to accurately report the nature or magnitude of an incident. Imposing an obligation to provide an initial incident report in advance of 72 hours after confirmation – prioritizing speed over quality – carries significant risk, not just for the reporting entity but also for the public authorities consuming or actioning such potentially erroneous or heavily qualified information. Premature reports can trigger false alarms and activate response teams unnecessarily, especially if entities err on the side of caution and over-report, distracting both reporting organizations and government consumers of a report. Organizations may also appropriately report a confirmed incident but have no useful information to share, triggering a myriad of questions that detract from responders' ability to focus on critical incident response activities.

In our experience, a 72-hour reporting timeframe is consistent with what our enterprise and government customers require and with the reporting deadlines imposed by the vast majority of authorities throughout Europe. Therefore, Microsoft recommends that providers be given up to 72 hours to report a significant incident with the window for reporting beginning with confirmation that an incident triggers the threshold for significance.

3.2. Follow-on reporting

Microsoft further recommends that additional reporting should only be required if all the relevant information was not available in the initial report. The relevant information would be a description of the incident (as set out in Sec. 3 of the proposed guidance) as well as an explanation of what measures the service provider has taken to prevent recurrence of the incident.

If a detailed final report is required, it should be due after the investigation is complete or within six months of confirmation that the incident is significant, whichever is sooner, to ensure sufficient opportunity for investigation and accurate reporting. To the extent that a nearer term deadline is maintained, ComReg should allow organizations to defer the deadline if internal investigations are ongoing or amend final reports if their investigations are incomplete and their analysis changes. While some incident investigations may be completed relatively quickly, investigations for complex incidents may extend for months. Additionally, it would be efficient if ComReg provided a streamlined reporting mechanism, to allow providers to report an incident by identifying it as either an initial or final notification,

so as to eliminate the need for unnecessary additional reporting or resubmitting previously reported information, after fully reporting an incident as resolved or completed.

— — —

Microsoft appreciates ComReg's effort to ensure that communications providers take appropriate steps to manage risks to the security and reliability of their systems and respond to incidents efficiently in the event of service disruptions. Accordingly, we encourage ComReg to implement network incident thresholds and reporting requirements that are not too prescriptive but recognize the wide variety of services now covered and consider the provider perspective regarding how to best restore service and integrity as soon as possible while providing relevant information to ComReg within realistic timeframes.

5 National Broadband Ireland

National Broadband Ireland

Network Incident Reporting Thresholds

Response to ComReg's Consultation and Draft Decision 23/36

25th May 2023

BUILDING A LIMITLESS IRELAND

Table of Contents

1 Introduction

National Broadband Ireland (NBI) is pleased to provide its response to ComReg's consultation and draft decision on the Network Incident Reporting Thresholds (Reporting & Guidance on Incident Reporting & Minimum Security Standards) (the Consultation Document).[1]

In November 2019 NBI signed a Project Agreement with the Minister for the Environment, Climate and Communications committing it to roll out a full-fibre network to those areas of the country that had been identified as unserved by commercial broadband providers. NBI's Fibre to the Home (FTTH) network deployment is now well advanced – at mid-May 2023, the NBI network had passed just over 140,000 premises, with in excess of 41,000 end-users connected to the network and availing of retail broadband services from a variety of Retail Service Providers (RSPs).

Under the Project Agreement, NBI has committed to completing the NBP network deployment within seven years. The deployment is now in its fourth year and NBI is on target to complete it in line with its contractual obligations.

NBI is aware of the heightened focus on network security within the electronic communications sector and this is an issue that NBI monitors closely on an ongoing basis. NBI accepts that prompt and full reporting of security incidents is an important part of a fit-for-purpose national and EU-wide approach to network security and this response to ComReg's Consultation is framed with this in mind.

[1] ComReg Consultation and Draft Decision, Document No. 23/36, 24th April 2023.

2 Responses to ComReg's consultation questions

In this Section, NBI provides its response to each of the questions posed by ComReg in its Consultation Document.

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

NBI, although positively disposed towards the principles underpinning the measures outlined in the Consultation Document, perceives some practical challenges in supporting the proposed thresholds, further information requirements and security incident typification.

Incident Types and Definitions

The consultation makes regular but varied references to what are referred to as 'incidents'. The inconsistency in the use of the term introduces ambiguity and, in turn, creates a degree of confusion about what exactly is being referred to in some instances. Sometimes referred to as the 'fog of war', confusion is the enemy of effective and decisive security incident management and so it is important to be clear about exactly what is meant by the various terms used in the consultation.

As an example of this, NBI notes that, in the Consultation Document, ComReg makes reference solely to 'incident' the majority of the time, 'security incident' some of the time and also makes a number of references to 'any incident'. NBI notes that the consultation refers to Article 40 (Security of Networks and Services) and Article 41 (Implementation and Enforcement) of Directive (EU) 2018/1972 (European Electronic Communications Code, the 'EECC') and Part 2 (Security of Networks and Services) of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (the 'Act'), the scope of which is exclusively security incidents.

The inclusion of reporting requirements for weather storms further adds to the confusion. Storms are not security incidents and should not be treated by ComReg, in this Consultation or more generally, as such. In light of this, NBI would welcome clarification from ComReg that where it refers in the Consultation to an 'incident', this is a reference to a 'security incident' and not to any other issue, including weather-related events.

Further Information Requirements

NBI would appreciate clarification from ComReg on the following:

- Category of incident: security incidents may satisfy the definition of multiple categories simultaneously. The reporting process and portal should support the ability for providers to report one security incident categorised under more than one category without having to duplicate submissions;
- Date and time the incident occurred and its duration: clarification is sought around the term 'incident occurrence.' Security incidents are detected at a point in time but the date and time of occurrence often predates detection and is unknown at the point of detection. Identifying the date and time of a security incident occurrence within the reporting timelines set out in the consultation is likely not to be possible or if so accurate. This, in turn, impacts the accuracy and completeness of reporting to ComReg, incident duration and the absolute threshold calculations;

- The impact of the incident on economic and societal activities: the content, the nature of the content and the detail to be reported to satisfy ComReg's requirements are sufficiently unclear that NBI requests ComReg provide clarity and guidance as to what is expected by way of a return; and
- Information concerning any or any likely cross-border impact with another EU Member State; NBI requests clarification as to whether or not Northern Ireland is to be considered a Member State or, in light of the UK's decision to leave the EU, to be viewed as outside the EU for the purposes of the Consultation.

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

24 Hour Security Incident Reporting Requirement

NBI, although positively disposed towards the principles underpinning the measures outlined in the Consultation Document and having regard to its obligations relating to the reporting information requirements, is concerned by the very short 24-hour reporting timeline that is being proposed. NBI's view is that:

- 24 hours is too short a time window to provide a security incident report compliant with the requirements set out in the Consultation Document;
- Anticipating that ComReg will not be participating in security incident response and does not operate a 24-hour or 'on-call' type service, there is no practical security incident management need for such a short timeline;
- Rushed reporting within the 24-hour timeline will result in incomplete and/or unintentionally inaccurate reporting due to the short timeline, in particular in relation to incidents whose impact continues to evolve beyond the proposed 24-hour window; and
- Submitted reports will likely require correction/revision as a result of a rushed initial report.

Inaccurate and/or incomplete security incident reporting results in an inaccurate view of a security incident and can lead to incorrect remedial and regulatory action being taken. NBI suggests that 72 hours is a more appropriate timeframe for an initial security incident response by providers to ComReg.

Reporting Timelines of Security incidents with Significant Impact

NBI notes the requirement to report security incidents of significant impact to ComReg 'as soon as possible'. NBI requests more clarity with regards to:

- The definition of a security incident with a 'significant impact'; and
- Whether the criteria listed in para. 124 of the Consultation Document is a guideline for determining security incidents of significant impact or all security incidents.

6 Sky

Response to Network Incident Reporting Thresholds

ComReg 23/36

25 May 2023

Introduction

Sky Ireland welcomes the opportunity to respond to this consultation and the specific questions outlined by ComReg.

Sky Ireland appreciates the need for increased monitoring by ComReg in order to satisfy the enhanced incident reporting obligations contained in the European Electronic Communications Code (EECC) that are applicable to Providers of public electronic communications networks and services.

Question 1

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

The proposed thresholds for 'availability' are generally supported for the range of fixed line services covered by the regulations. However, Sky Ireland highlights the following comment in relation to the thresholds.

There are no apparent differences between the reporting of incidents impacting the availability of fixed line and mobile services. If it is desired that incident within a mobile RAN are reportable, further guidance would be required to identify incident thresholds as there is no fixed relationship between RAN site and subscribers as in the fixed network.

In relation to 'Incidents impacting confidentiality, integrity, and authenticity', such incidents are likely to have a root cause of a cyber-nature and the extension of the reporting obligations to such incidents should also take into account that operators will also have cyber monitoring obligation under the Electronic Communications Security Measures (ECSMs). Sky Ireland highlights that there may be lead-in time required for operators to implement these new reporting obligations.

Question 2

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

The proposed timeliness and process for reporting are generally supported in so far as reporting a significant incident should be done as soon as reasonably possible. There are some considerations that need to be understood as follows:

- The reporting of a loss of availability incident which includes the duration of the incident can only be made once the incident has been resolved and the outage rectified.

- The reporting of a cyber-incident impacting confidentiality, integrity, and authenticity can only be reported once the Provider becomes aware of the incident.

- It may not be possible to determine when a security compromise that results in a reportable incident actually occurred. As an example, if a threat actor gains unauthorised access using valid credentials to the network and the Provider only becomes aware of the compromise on receipt of a ransom demand. The threat actor may have had access for some time, perhaps looking to escalate their privileges.

Sky would propose an alternative arrangement where a Provider 'notifies' ComReg as soon as they become aware of a significant cyber-compromise impacting confidentiality, integrity and authenticity. The notification would be limited to the initial information associated with the breach. The Provider can subsequently follow up with more detailed reporting once the incident has been managed and finally resolved. An early notification would allow the Provider and ComReg to involve the NCSC organisation in Ireland to assist as appropriate. This is the approach that, for example, the regulator in the UK has adopted under their UK Telecommunications (Security) Act: 2021.

May 2023

7 Three

Three

Three's response to the Consultation by ComReg on Network Incident Reporting Thresholds

25th May 2023

Contents

1 Introduction

The digitisation of all aspects of the economy continues apace. No area of life or the economy is untouched, from real time departure information for public transport, streaming content services, e-money, remote working, smart metering, etc.

These advances are increasingly blurring the traditional sectoral lines with more complex supply chains, having higher degrees of integration. There are more fundamental dependencies within these supply chains affecting the integrity of the overall end-to end service should any element of the supply chain suffer an incident.

For example, energy suppliers are more dependent on communications to be able to monitor and manage their networks and communications providers are more dependent on energy supply as their core networks are consolidated into fewer nodes. Both are dependent on cloud service providers who host the BSS and OSS software and databases which underpin their businesses.

The increasing level of integration referenced above is mirrored in an increase in the scale and scope of the mandatory reporting of "incidents" to bodies charged with market supervision and monitoring. This can be seen not only in the changes between the Framework Regulations and the corresponding provisions of the European Electronic Communications Code (EECC) but also in the differences between the NIS Directive and the NIS-2 Directive.

The expansion in the scale and scope of these reporting requirements means that there is also an increasing potential for overlapping reporting obligations to different supervisory stakeholders in connection with the same incident.

If the reporting thresholds are properly set, then a reportable incident has material effect and requires urgent resolution. Increasing the volume of Supervisory Authorities that have to be reported to in respect of the same underlying incident runs a significant risk of requiring the operator suffering the incident to divert resources away from incident management and resolution and into this additional reporting.

Communications Service Providers have existing reporting obligations under a variety of statutory regimes, including those associated with the General Data Protection Regulation (GDPR), the e-Privacy Directive, the Framework Regulations, and the Network and Information Security (NIS) Directive.

Three notes that ComReg's consultation does not set out an assessment of how the current ComReg proposals interact with reporting obligations under other adjacent and relevant regulation. Absent this assessment the probability of the parallel reporting obligation outlined above is increased.

In the interests of transparency, certainty, and operational efficiency in the management of incidents Three would urge ComReg to set out how the proposed

reporting requirements set out in this consultation will interact with other reporting requirements that Service Providers are subject to.

It would also be useful for ComReg to outline what liaison mechanisms (if any) are in place with other supervisory authorities to avoid parallel reporting requirements and associated imposition of operational overhead at the time that operator resources should be focussed on incident resolution.

Three notes in this regard that the e-Privacy Regulations provide that "*The Commissioner* [the Data Protection Commission] *and the Regulator* [ComReg] *shall, in the performance of their functions under these Regulations, cooperate with and provide assistance to each other*"

Three believes that there is merit in Supervisory Authorities looking at a consolidated reporting mechanism for the reporting of network incidents. This is with a view to reducing the operational overhead on operators who are trying to manage and resolve incidents.

2 Consultation Question 1

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

Three Response:

Three notes that there are three distinct elements to this question and proposes to respond to each separately.

Proposed Thresholds

Three believes that there is significant merit in aligning the national ComReg reporting thresholds to the ENISA reporting thresholds. Given that most of the ENISA reporting thresholds are based on a percentage of National User Base these are scalable to the relative impact of an incident on an individual market basis.

In relation to the absolute reporting threshold of 1 million user hours Three notes that the ENISA guidelines set out that "*…very small incidents, which affect less than 25.000 user connections, as well as very short incidents, which last less than 1 hour...*" are to be excluded[1]. If it is ComReg's intention to align with the ENISA guidelines, then these exclusions should also be reflected in the final ComReg Decision.

Further Information Requirements

Three is broadly of the view that the further information requirements are not unduly burdensome.

Incident Typification

Three notes that the expanded set of reportable incident categories (Confidentiality, Integrity and Authenticity) potentially have significant overlap with the reportable incident categories under the NIS and the e-Privacy Directive.

As outlined in our introduction, this overlap creates the potential for the creation of parallel and distinct reporting obligations to different Supervisory Authorities. This is particularly the case where e-Privacy already requires reporting of a high volume of usually relatively minor incidents. ComReg should assess the extent to which the additional categories of reportable incidents (Confidentiality, Integrity and Authenticity) might create a parallel reporting obligation. Unless there is a clear need for parallel reporting interfaces into multiple Supervisory Authorities in respect of the same incident Three believes that ComReg should only impose additional reporting requirements to the extent that is necessary. This is in the interests of allowing Service Providers to focus on incident resolution rather than reporting administration.

[1] Section 6.2.2.2 of the ENISA Technical Guideline on Incident Reporting Under the EECC

3 Consultation Question 2

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

Three Response:

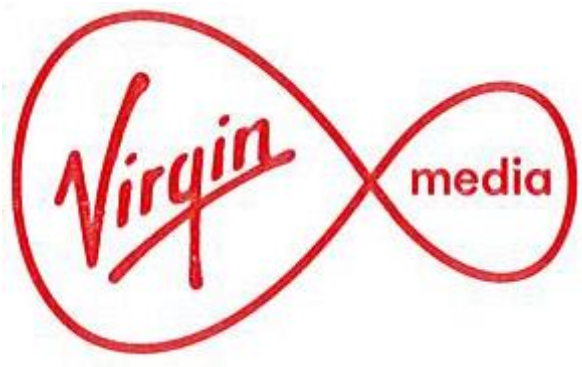
Three welcomes that ComReg is not proposing to alter the current mechanism for reporting incidents via the e-licensing portal. In addition, Three welcomes the rationalisation of the reporting timelines.

However, Three notes that ComReg sets out that "...*ComReg operates between 09H00 and 17H30 and does not operate a 24Hour or 'on-call' type service...".*[2] In light of this it is not clear that the imposition of a "clock hours" rather than working hours target for reporting incidents to ComReg is either justified or proportionate. This is particularly relevant where the administrative and operational burden of meeting this clock hours target applies at a time when operator resources should be primarily focussed on incident resolution. In an out of hours situation, when non-operational staff may not be at work, and when ComReg is not available to take any action on foot of the reports this burden will fall on the resources primarily tasked with incident management. Three would ask ComReg to review the necessity for the reporting timeline being expressed in clock hour terms.

[2] Paragraph 123 of the Consultation document

-End-

8 Virgin Media



Virgin Media response to:

Consultation on ComReg's "Network Reporting Incident Thresholds. A Consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards)".

25 May 2023

Introduction

- Virgin Media Ireland Limited ('Virgin Media') welcomes the opportunity to respond to ComReg's Consultation Document 23/36, "Network Reporting Incident Thresholds. A Consultation to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum Security Standards)".

- From the outset it is important to state that Virgin Media considers network security to be critical and implements technical and organisational measures to ensure the security and integrity of our networks and services.

- Cybersecurity is essential for consumer confidence particularly when cybersecurity considerations have never been more important. Virgin Media participated and contributed to the working group, resulting in the development by the National Cyber Security Centre ("NCSC") of the series of ten documents known as the Electronic Communications Security Measures or ECSMs, which reflects on our commitment with the industry to safeguard against cyber threats. This is an area of focus for all and we look forward to continued engagement with ComReg on it.

- In addition, preventative maintenance and continuous investment in network upgrades, ensures the resilience of our network and mitigates against external factors such as climate change.

- Virgin Media is very supportive of the Nuisance Communications Industry Taskforce set up by ComReg. The Taskforce led by ComReg has resulted in much positive work to address issues undermining confidence in telecommunications such as spoof text messages and calls. Virgin Media will continue to play a key role in this taskforce.

- Virgin Media supports ComReg's approach not to be overly prescriptive on specific measures that providers should employ when managing the integrity of networks given that that such measures will inevitably vary between providers.

- Technological neutrality is a cornerstone of the principles of better regulation enshrined in the European Electronic Communication Code ('EECC'). Virgin Media would reiterate that it is of the utmost importance that ComReg takes into account that networks are constructed in unique or different ways. Specific requirements therefore may not work or be feasible in all scenarios. The provision of more general guidance with a focus on outcomes rather than on specific measures should be the preferred approach.

- We make a number of suggestions in our response which we believe will generally enhance the process of incident reporting.

- Virgin Media believes it would be very helpful if ComReg were to hold a workshop updating all Providers on the revised reporting obligations, including timelines and the process for making submissions.

- Please find set out below Virgin Media's response to the specific questions asked in ComReg's consultation paper.

Q1. *Do you support the proposed thresholds, further information requirements and incident typification outlined in this document? If not, please provide a well supported, justified and evidenced-based explanation for your view.*

- Yes, Virgin Media supports ComReg's approach to the proposed thresholds, further information requirements and incident typification.
  We believe that reporting of incidents under the expanded categories of confidentiality, integrity, authenticity and availability will be of benefit in terms of gaining valuable lessons and sharing learnings/insights.
- Virgin Media believes it would be very helpful if ComReg were to hold a workshop updating all Providers on the revised reporting obligations, including timelines and the process for making submissions shortly after ComReg issues its Decision Notice.

Q2. *Do you agree with the proposed timelines and processes for reporting incidents outlined in this, and the draft Decision, document? If not, please provide a well-supported, justified and evidenced-based explanation for your view.*

- Virgin Media in principle agrees with ComReg's proposed timelines for reporting incidents. However, Virgin Media would make some suggestions regarding the the proposed minimum information requirement within a 24-hour timeframe.

- We note that the Communications Regulation and Digital Hub Development Agency Amendment Act 2023 provides that Providers are to notify ComReg of any incident of significant impact on networks or services "*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".*

  The Act does not specify an initial incident report time frame of 24 hours. We agree that Providers should report the incident as soon as possible without undue delay once they become aware of it. If there is a 24 hour reporting obligation this should only be for an initial report. The first 24 hours of an incident is likely to be a period when the incident is being evaluated, mitigating actions are taken to close down the incident, minimise it and is a period when not all information will be known about the incident. Providers should be able to follow up subsequently with further updates to the incident as further facts emerge.

- ComReg propose that the initial report contain all the information available at the time the incident report is made and that the report should contain the following information at the minimum:

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

- We believe that an initial report of an incident of significant impact on a Providers network or services could be reported to ComReg within 24 hours. However, it may not always be possible or feasible to provide the details as listed above. For example, the exact number of users impacted may not be known, or the likely cause of the incident could still be under investigation. It would seem more prudent to provide an initial interim report with the information that is available and thereafter follow up with other information such as the likely cause when this is known. For all of these reasons we believe it would be more helpful and practical to have some flexibility around the minimum information requirement.

  When reporting a data breach to the Office of the Data Protection Commissioner ("DPC") for example an initial notification can first be made before filing a full report. We believe that an initial report could be made to ComReg within 24 hours with the circumstances and facts that are known or available at the time with more detail on the incident following at a later date.

- This flexibility will ensure that ComReg are notified with the known facts of any incident of significant impact on a Providers networks or services without delay and Providers could also initially notify ComReg of a significant impact within 24 hours as proposed.

9 Vodafone

Vodafone Response to Consultation

Network Incident Reporting Thresholds Update

Public Consultation

Reference: ComReg Doc 23/36

Version: Non-Confidential

Date: 25/05/23

Introduction

Vodafone welcomes the opportunity to respond to the Commission for Communications Regulation (ComReg)'s consultation on proposals to revise and replace ComReg Document 14/02 (Reporting & Guidance on Incident Reporting & Minimum-Security Standards). In principle the regime which ComReg has established since 2014 is working effectively. Vodafone have provided some comments on revisions below

Purpose of network reporting: A general comment relates to purpose and use of network incident data. The overriding objective of all stakeholders should be to ensure resilience, security, and continuity in the delivery of connectivity for Ireland. The reality is Ireland has a relatively modern mobile and fixed infrastructure which will be fully replaced in line with digital targets over the coming 5 years.

When developing a reporting regime and other security measures the Regulator and the industry need to ensure interventions requiring reporting and data provision are balanced and that we avoid micro-management or multiple agency reporting on network incidents or storm events. We would encourage ComReg to be ready to adapt this document further to avoid any duplication especially given the increased focus in the coming year on Security matters through the implementation of ECSMs. The objective should be to ensure reporting through one channel on any incident.

A further point on the purpose of network reporting relates to ComReg use of the data provided. Article 40 requires that providers of public electronic communications networks and/or services take appropriate and proportionate technical and organisational measures –to appropriately manage the risks posed to the security of their networks and services. Operators are required under regulation to report incidents, and this may be reported to the Minister and to ENISA. We note the recent use of the Network Incident Reporting to inform the policy approach in the Customer Charter consultation which highlighted *"In 2020, more than 50.7 million user hours were reported lost to incidents such as software bugs, poorly implemented software updates, hardware failures and weather events causing power outages. "*

Most customer hours lost in incidents will relate to power outage incidents outside the control of the operator and the sector. In fact in many cases networks mitigate of such events with battery back-up facilities. The concern arising is the use of Network Incident Reporting data in this headline manner has the potential to mislead customers and impact the perception of the actual quality of service delivered by Irish networks.

Changes to the Definition of a Security Incident: In response to question 1 we note the change to include availability within the definition of a Security Incident. This will cause confusion when educating and re-educating operational teams on incidents that need to be reported. An availability incident due to a power outage, that is defined as a security incident will cause some confusion and we would encourage some refinement in guidance to avoid the questions arising.

E-licensing portal: A final comment relates to the e-licensing portal. Vodafone welcome recent changes on the system. In the next round of update we would request a simple template for storm reporting enabling an operator to maintain a tracker of 10am and 4pm reports. We would also request that mandatory fields such as customer number figures should only be mandatory for submission of a final report with root cause analysis and remedy.

ENDS