Commission for
Communications Regulation

Consultation on Incident Reporting & Guidance on Minimum Security Standards

Regulations 23 and 24 of The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011

All responses to this consultation should be clearly marked:-
"Reference: Submission re Consultation on Incident Reporting & Guidance on Minimum Security Standards, 13/10" as indicated above, and sent by post, facsimile, email or online at www.comreg.ie (current consultations), to arrive on or before 17:00 on 25 February 2013, to:

Mr. Neil Redmond
Commission for Communications Regulation
Irish Life Centre
Abbey Street
Freepost
Dublin 1
Ireland
Ph: +353-1-8049600
Fax: +353-1-804 9680
Email: neil.redmond@comreg.ie

Please note ComReg will publish all respondents' submissions with the Response to this Consultation, subject to the provisions of ComReg's guidelines on the treatment of confidential information – ComReg 05/24.

Consultation

Reference: ComReg 13/10

Date: 28/01/2013

Additional Information

EU Directive 2009/140/EC	
Regulations 23 and 24 of The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011 ("the Regulations")	

Legal Disclaimer

This draft information memorandum 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

Section Page

Table of Figures

Section **Page**

1 Introduction

1 Regulation 23 of the new Framework Regulations of The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011) ("The Regulations"), places obligations on undertakings providing public communications networks or publicly available electronic communications services (referred to in this paper as "Operators") in respect of the management of the integrity and security of networks and services.

2 Regulation 23 also requires that an operator shall notify the Commission for Communications Regulation ("ComReg") in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services.

3 Where ComReg receives such reports, it is required to inform the Minister and, where appropriate, the European Network and Information Security Agency[1] ("ENISA") of the said notification. Management of an incident is the responsibility of the Operator concerned, calling upon resources as appropriate to assist in the efficient handling of the issue. Such resources may include internal technical expertise, external technical support from other bodies such as suppliers or consultants with specialist knowledge in the area of equipment or cyber issues. In certain circumstances an Operator may request the support of ComReg, for example to assist in its coordination of the incident with other parties such as other interconnected Operators. This should not be confused with the reporting process to ComReg which will be used by ComReg for its function of ensuring compliance by Operators with their obligations, to enable ComReg to comply with its obligations regarding reporting of incidents and to inform users of the services of the situation as appropriate.

4 The purpose of this consultation and guidance is to clarify the appropriate thresholds for reporting incidents and the requisite timing for submission of these reports. It should be noted that the thresholds and process for reporting are provided as guidance to Operators and reflect ComReg's view of what is required by Operators to comply with their obligations.

[1] ENISA is an Agency of the EU which has an objective to assist the Commission and Member States in the area of network and information security.

5 This consultation also addresses ComReg's approach to assessing Operators' compliance with their obligations in respect of ensuring the integrity of their networks and provides some clarity around the reporting requirements of Operators. The consultation takes into account work undertaken by ENISA and two associated documents published by ENISA:

- Technical Guideline on Reporting Incidents[2]
- Technical Guideline for Minimum Security Measures[3]

6 These two documents have been produced by ENISA following engagement with a number of stakeholders, including NRAs and Government bodies from Member States. Both documents are guidelines to ComReg in these areas.

7 While the ENISA Guideline on Reporting Incidents outlines reporting requirements at a national level, this consultation aims to define the reporting requirement to the level of individual Operators to enable ComReg to report on the national impact of an incident.

8 In addition this Consultation aims to provide clarity about the interpretation of the new requirements.

[2] Technical Guideline on Reporting Incidents Article13a Implementation Version 1.0 - https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0

[3] Technical Guideline for Minimum Security Measures - https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-for-minimum-security-measures-v1.0

2 Executive Summary

9 The Framework Regulations have introduced a number of requirements around the management of the integrity of networks and the reporting of incidents through Regulations 23 and 24.

10 This consultation sets out proposals as to how ComReg would interpret the Regulations and seeks views for respondents in this regard. The paper also describes what actions ComReg expects Operators to take in order to ensure compliance.

2.1 Incident Reporting

11 ENISA has published thresholds which National Regulatory Authorities (NRAs) should use for defining incidents which must be reported by NRAs to ENISA and the European Commission. This consultation gives guidance on appropriate thresholds for incidents which must be reported by Operators to ComReg to facilitate ComReg's reporting requirements as defined by these ENISA thresholds. The proposed thresholds for Operators are lower than the national thresholds specified by ENISA in part because a combination of smaller local incidents could equate to a significant impact nationally that would trigger the specific ENISA threshold for reporting.

12 The thresholds proposed by ComReg for the trigger of an incident report can be found in Tables 1 and 2 of this document.

13 Tables 1 and 2 also address the timing for the reporting by operators as the timeliness of provision of information is important as it will enable ComReg to use the information appropriately. ComReg therefore needs periodic updates even if not all information about an incident is available at a point in time.

14 The reporting process will serve a number of purposes including enabling ComReg to monitor the compliance by an Operator in respect of its obligations around the management of the integrity and security of its networks. In addition, ComReg requires information to be provided in a timely manner in relation to incidents to ensure consumers can be made aware of incidents which impact a significant number of consumers. The time by which information should be provided is dictated mainly by the seriousness of the incident.

15 In order to facilitate a common reporting format which contains the information required by ComReg, ENISA and the European Commission the proposed format and guidelines for reporting incidents is shown at Annex 1 of this document.

16 All relevant incidents are to be reported to ComReg at: incident@comreg.ie. Any incident requiring notification in 4 working hours or less is to be notified to the ComReg wholesale operations/ compliance team on **01 804 9600**. All callers reporting such an incident should request to speak to a member of ComReg's telecommunications incident management team.

17 This phone number can be used during ComReg's office working hours: 9am to 5:30pm, Monday to Friday.

2.2 Management of the integrity of networks

18 ComReg does not intend to be prescriptive in this consultation around specific measures that Operators should employ when managing the integrity of networks as these may vary between Operators. Nonetheless under Regulation 23(1) Operators are required to take appropriate technical and organisational measures to appropriately manage the risks posed to the security of networks and services.

19 This consultation refers to the guidance material which is provided by ENISA for an NRA when considering the measures that have been taken by an Operator. ComReg envisages that in the event of an investigation into an Operator's compliance in this area it would be guided by the ENISA document.

20 ComReg may require Operators to provide information that would be used to assess the security and integrity of the services and networks of that Operator and where necessary to submit to a security audit that would be carried out by an independent professional body nominated by ComReg (Regulation 24(1)).

3 Background

3.1 The new Regulations

21 With the introduction of the Framework Regulations[4], a number of obligations were imposed on both ComReg and Operators. This consultation relates to the obligations relating to Framework Regulations 23 and 24.

3.1.1 Regulation 23- Security and integrity

22 The provisions of Regulation 23 are as follows:

Regulation 23 (1):

> *Operators providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.*

Regulation 23 (2):

> *The technical and organisational measures referred to in paragraph (1) shall, having regard to the state of the art, ensure a level of security appropriate to the risk presented.*

Regulation 23 (3):

> *Operators providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, thereby ensuring the continuity of supply of services provided over those networks.*

Regulation 23 (4) (a):

[4] Framework Regulations of The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011)

An operator providing public communications networks or publicly available electronic communications services shall notify the Regulator in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services.

Regulation 23 (4) (b):

Where the Regulator receives a notification under subparagraph (a), it shall inform the Minister of the said notification and, with the agreement of the Minister, it shall also, where appropriate, inform the national regulatory authorities in other Member States and ENISA.

Note: ComReg will advise the Minister of an incident when such an incident is reported to ComReg initially and also at the time when the incident is closed.

Regulation 23 (4) (c):

Where it is considered that it is in the public interest to do so the Regulator, with the agreement of the Minister, may inform the public in relation to the breach notified under subparagraph (a) or require the operator to inform the public accordingly.

Regulation 23 (5):

The Regulator shall annually submit a summary report to the Minister, the European Commission and ENISA on the notifications received and the actions taken in accordance with paragraph (4).

Regulation 23 (6):

An operator that fails to comply with the requirements of paragraph (4)(a) or (c) commits an offence.

23 Accordingly, Operators have the responsibility to implement technical and organisational measures to appropriately manage the risks posed to security of networks and services and also to report incidents to ComReg. ComReg's role in this context is to monitor compliance within these obligations and to report or publish details of these incidents as required. The question therefore arises as to what constitutes appropriate technical and organisational measures. Also it is necessary to determine what is to be described as a significant impact for purpose of determining whether particular incidents should be reported to ComReg. These points are considered in this consultation.

24 Furthermore, when reporting incidents the associated timelines for reporting and the details which should be reported are defined.

3.1.2 Regulation 24- Implementation and enforcement

25 The provisions of Regulation 24 are as follows:

Regulation 24 (1)

> *For the purpose of ensuring compliance with Regulation 23 (1), (2) and (3), the Regulator may issue directions to an operator providing public communications networks or publicly available electronic communications services, including directions in relation to time limits for implementation.*

Regulation 24 (2)

> *The Regulator may require an operator providing public communications networks or publicly available electronic communications services to—*
>
> *(a) provide information needed to assess the security or integrity of their services and networks, including documented security policies, and*
>
> *(b) submit to a security audit to be carried out by a qualified independent body nominated by the Regulator and make the results of the audit available to the Regulator and the Minister. The cost of the audit is to be borne by the operator.*

Regulation 24 (3)

An operator in receipt of a direction under paragraph (1) shall comply with the direction.

Regulation 24 (4)

An operator that fails to comply with a direction under paragraph (1) or a requirement under paragraph (2) commits an offence.

3.1.3 Objective of this consultation

26 This consultation presents ComReg's view on;

- The appropriate management of risks by Operators;
- The level of incident that must be reported to ComReg;
- The process for communicating an incident to ComReg;
- The approach that will be followed by ComReg under Regulation 24 to monitor Operators compliance with the obligations imposed under Regulations 23.

27 In addition to the specific requirements under Regulation 23 and 24 this consultation will address other reporting requirements and proposes a consolidated reporting process to avoid duplicate processes where possible and hence to avoid any unnecessary duplication of work for Operators.

3.2 Work undertaken by ENISA

28 ENISA has developed guidance material in the form of 2 documents on a common implementation approach across Member States in respect of Article 13(a) and 13(b) of the Framework Directive[5]. Article 13(a) and 13(b) in the Directive relate to Regulations 23 and 24.

[5] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) As amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities and 2002/20/EC on the authorisation of electronic communications networks and services.

29 The first of these documents is the “Technical Guideline on Reporting Incidents”. This document gives “guidance to NRAs about the implementation of Article 13(a) and, in particular, the two types of incident reporting mentioned in Article 13(a): the annual summary reporting of significant incidents to ENISA and the European Commission and ad hoc notification of incidents to other NRAs in case of cross border incidents. The document defines the scope of incident reporting, the incident parameters and thresholds. The document also contains a reporting template for submitting incident reports to ENISA and the European Commission, and it explains how the incident reports will be processed by ENISA.” It should be noted that there may be changes to this document from time to time and where this consultation may currently differ from some aspects of this document it is because of anticipated changes contained in a revision document which is soon to be published.

30 The second document is the “Technical Guideline for Minimum Security Measures”. This document gives “guidance to NRAs about the implementation of Article 13(a) and in particular about the measures that providers of public communications networks must take to ensure security and integrity of these networks”.

31 These documents will provide guidance to ComReg and Operators and as such Operators are invited to provide comments to ComReg on them. Aspects of this consultation are based on these guidelines.

4 Definition of an incident and thresholds

4.1 What constitutes a reportable incident?

32 In its document on Technical Guideline on Reporting Incidents, ENISA uses a working definition of an incident as follows: An incident is “an event which can cause a breach of security or a loss of integrity of electronic telecommunications networks and services.” A reportable incident is defined in that document as: “A breach of security or a loss of integrity that has a significant impact on the operation of electronic telecommunications networks and services.”

33 The initial requirement for reporting to ENISA has been identified as a more narrow definition: “Network and information security incidents having a significant impact on the continuity of supply of electronic communications networks or services.” ComReg proposes that this definition should be used when considering the type of incident that is required to be reported to ComReg.

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

34 ENISA has defined the threshold for annual summary reporting to be based on the duration and the number of users of a service affected as a percentage of the national user base of the service.

35 ENISA recommends the following steps be taken by a National Regulatory Authority when an incident is being reported to a National Regulatory Authority[6] by an Operator.

[6] S3.2 Describing the reporting mechanism: Technical Guidelines on Reporting incidents (Version 1.0 – 2011-12-10)

35.1 Assess the impact of the incident; by ascertaining whether it affected a service which is in the scope of Article13a and whether the incident falls under the scope of the reporting requirements. The services ComReg considers appropriate for reporting on are: Mobile services – voice, data and SMS, Fixed Line - PSTN and Broadband, Cable - telephony and broadband, Leased Lines & Fixed Wireless. It should be noted that this list is not consistent with the current version of the ENISA Guidelines as it is understood by ComReg that the proposed services in the document are subject to change. Operators should be aware that as ENISA changes its guidelines it may be necessary for ComReg to change the scope of services covered by this reporting arrangement.

35.2 Determine if the incident is significant; according to the parameters and thresholds set by ENISA determine if this incident triggers the reporting scheme.

36 According to the guidelines, ComReg should report to ENISA on an annual basis on incidents that have the service impacts shown in figure 1 below.

37 ComReg should send an incident report, as part of the annual summary reporting, if the incident

37.1 lasts more than an hour, and the percentage of users of that service affected is more than 15%,

37.2 lasts more than 2 hours, and the percentage of users affected is more than 10%,

37.3 lasts more than 4 hours, and the percentage of users affected is more than 5%,

37.4 lasts more than 6 hours, and the percentage of users affected is more than 2%, or if the incident

37.5 lasts more than 8 hours, and the percentage of users affected is more than 1%.

38 In figure 1 the High impact area (red) represents incidents which should be reported. The parameters shown in this figure relate to the duration of the incident against the number of consumers impacted by the incident as a percentage of national usage (not individual operator customer base).

	1h<...<2h	2h<...<4h	4h<...<6h	6h<...<8h	>8h
1%<...< 2% of users					
2% < ...< 5% of users					
5% <...< 10% of users					
10% <...<15% of users					
> 15% of users					

Figure 1 ENISA thresholds for NRA reporting to ENISA as presented in the Technical Guidelines document

4.2.1 National level thresholds for Operators

39 Regulation 23 introduces a requirement for an Operator to report to ComReg an incident that has a significant impact on the operation of its networks or services. The proposed threshold for reporting an incident is based upon the approach adopted by ENISA in a national context with the thresholds adjusted to make them relevant to operators.

40 An Operator providing public communications networks or publicly available electronic communications services[7] shall notify the Regulator in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services. For the purposes of meeting these reporting requirements the level at which ComReg considers incidents are required to be reported under Regulation 24(2)(a), are outlined in the tables 1 and 2 below. Table 1 outlines the thresholds for fixed line services and table 2 refers to mobile services.

41 The elements of the thresholds related to Regulation 23(4)(a) reports are set at a level that is lower than that proposed for ComReg reporting to ENISA. The reason for this are

[7] European Communities (Electronic Communications Networks and Services((Framework) Regulations 2011

41.1 that the threshold to trigger an ENISA report by ComReg will be an accumulation of reports from various Operators,

41.2 having a lower threshold has the additional advantage that this will enable ComReg to use this reporting mechanism to maintain a more detailed picture of an Operators network performance, and

41.3 the associated effectiveness of an Operators approach to management of risks as required in Regulation 23(1).

42 Once the incident threshold has been reached an Operator must report the incident to ComReg within the defined period specified in the tables below.

43 In addition, there may be incidents of significant public interest that do not necessarily meet the thresholds which should be reported, for example the loss of service to a number of banks which results in an inability for customers to make point of sale payments or public services for example in a wider geographic area. Such incidents should be reported due to particular public interest to enable ComReg to be able to communicate appropriately with consumers and other appropriate parties.

44 Tables 1 and 2 set out the thresholds for incident reporting and define the timing for these reports. The timing is expressed in working hours and working days.

Q. 1 Do you agree with the proposed thresholds for fixed services? If not please advise the basis of your concern.

Q. 2 If you do not agree with the fixed services proposed thresholds what alternative thresholds would you consider more appropriate, what reporting periods to use and what is the basis for that approach?

Network/Service Type	Min number of customer lines affected (lower of number or percentage of users)	Min duration of service loss/disruption (clock hours or mins)	Report to ComReg Within (working hours or working days)	Interim Report to ComReg (working hours)
Fixed voice* services	1,000 10% of customer lines	24 hours	2 days	Every 4 hours
Fixed voice* services	10,000 20% of customer lines	1 hour	4 hours	Every 4 hours
Fixed voice* services	20,000 50% of customer lines	10 minutes	2 hours	Every 4 hours
Internet access service	10,000 10% of customer lines	1 hour	4 hours	Every 4 hours
Leased Line services	500 10% of customer base	30 minutes	1 day	Every 4 hours
Leased Line services	500 10% of customer base	12 hour	4 hours	Every 4 hours
Leased Line services	1,000 50% of customer base	10 minutes	2 hours	Every 4 hours

Table 1 Reporting Thresholds for Fixed Line Service

*Voice provider for fixed location

45 The approach to determining the reporting threshold for mobile services differs from that for fixed line services as it is more difficult to assess the number of customers impacted in a scenario such as a mobile base station failure. The reason for this is that an individual customer is not necessarily only capable of obtaining a service from a particular base station as there will be an overlap with other bases stations and a customer may automatically benefit from this. It is however possible that customers will have a service failure associated with an individual bases station failure therefore a simple approximation is needed to assess the significance of such an incident. For example the number of customers varies from time to time and an incident affecting a base station means that the impact on customers will be more difficult to determine. A number of options were considered:

46 One option is to have a mobile operator define the peak load of a network element and as an approximation of the significance of the incident relate the number of customers that are impacted to this figure. This has the advantage of simplicity but requires an operator to maintain a database associated with network usage of its network elements and reference this database in the event of a network outage.

47 A second option is similar to the first option with a record of the design capacity for each network element identified. This would again have the difficulty of cross referencing the network elements impacted in an incident to the design parameters in order to assess the significance.

48 A third option, which is the proposed approach, is to report on an incident by the number of base stations which are impacted where this is the key characteristic of an incident. E.g. where a transmission network failure results in 6 bases stations losing service this will suggest the scale of the incident. In addition to this measure there are some network elements which are important to the service provision of a large number of customers, such as a Home Location Register (HLR). For such significant elements an individual failure should be reported.

Network/Service Type	Min impact of services affected	Min duration of service loss/disruption (Clock hours)	Report to ComReg Within (Working hours)	Interim Report to ComReg (Working hours)
Mobile Voice, Broadband, SMS	20-59 cells off air	2 hours	1 hour of operator becoming aware of the issue	4 hours
Mobile Voice, Broadband, SMS	>60 cells off air	1 hour	1 hour	4 hours
Mobile Voice, Broadband, SMS	MSC Failure	Any impact	1 hour	4 hours
Mobile Voice, Broadband, SMS	HLR Failure	Any impact	1 hour	4 hours
Mobile Voice, Broadband, SMS	BSC or RNC failure	Any impact	1 hour	4 hours
SMS	failure >20%<40% of base	2 hours	8 hours	4 hours
SMS	failure >40% of base	1 hour	4 hours	4 hours

Table 2 Reporting Thresholds of Mobile Services

49 The number of impacted customers, where known, associated with an incident report will provide ComReg with an indication of the significance of the incident on end-users as a whole as well as the scale of the incident for the individual Operator. The percentage of the customer base as a threshold will provide ComReg with an indication of the scale of the incident on customers of the relevant operator.

50 The threshold for reporting outlined in tables 1 and 2 does not preclude voluntary reporting of incidents that fall below the threshold levels outlined. Where an operator considers that an event is significant, even if not covered by the thresholds described in tables 1 and 2, such events may be reported. An example would be less than 20 cells off air but the geographic coverage of the incident being large.

51 In the event of a change of requirement of the structure of the report that ComReg sends to ENISA, ComReg may update the formats and thresholds of reports sent to ComReg.

Q. 3 Do you agree with the proposed thresholds for mobile services? If not please advise the basis for your concern.

Q. 4 If you do not agree with the mobile services proposed thresholds, what alternative thresholds would you consider more appropriate, what reporting periods to use and what is the basis for that approach?

5 The incident reporting process

5.1 Timing for provision of information

52 As outlined in Tables 1 and 2, in some circumstances the appropriate timescale for the reporting of an incident can be short. It is highly likely that at that stage of an incident information regarding its cause, its impact and the planned remedy may be limited. ComReg recognises that it may take some time to fully understand the circumstances around some incidents and consequently the final report on an incident may be delayed until the required information is available.

53 ComReg therefore considers that an initial report may be made within the timescale identified above (Table 1) with a final report being produced at a later time. As an indication, ComReg would expect interim updates between the initial report and the time of the resolution of the problem at appropriate reporting intervals.

54 This requirement presents a need for timely information in respect of problems with services that directly affect customers. ComReg proposes that the reporting requirements for Regulation 23 should also address the information required by ComReg to deal with these consumer queries. These reports will be used to assist with monitoring compliance with Regulation 23 (see Section 7.1)

55 The principal reason for the timings outlined in the Tables is that ComReg needs to have up to date information on network and service incidents, as reported under Regulations 23 and 24, to be able to deal with consumer enquiries and to maintain a general awareness of the availability of services to consumers and these reports will be used in this regard.

56 When the incident has been resolved, the Operator shall submit a final report, or further interim reports, as appropriate to agreed timelines

Q. 5 Do you agree with the timelines for reports associated with an incident? If you disagree with the reporting periods please provide alternative proposals for reporting periods with the basis for the recommendation.

5.2 Reporting arrangements

57 All incidents are to be reported to ComReg using this email address: incident@comreg.ie and any incident which requires notification in 4 hours or less is to be notified by phone to the ComReg wholesale operations/ compliance team on **01 804 9600**. All callers reporting such an incident are to request to speak to a member of ComReg's incident management team.

58 ComReg does not anticipate being involved in the operational management of the incident. For major incidents ComReg may be able to provide assistance, for example, to assist in the coordination with other entities within Ireland or other Member States as appropriate.

59 An Operator may not consider an incident as sufficiently serious to warrant reporting to ComReg at the outset, but as the incident develops it may become apparent to the Operator that a report is necessary. ComReg would expect to be made aware of the incident as soon as the Operator becomes reasonably aware of the severity of the incident, and where the threshold of reporting has been or is likely to be passed. At such a stage, precise data on the incident may not be available, but Operators should be in a position to provide educated estimates around the implications of the incident.

60 ComReg recognises that providing detailed information during an incident resolution may take resource from, and hence impact upon, the resolution itself by removing resources from the management of the incident. Therefore the information required at the first stage of reporting may be at a high level, and will include the date and time of the incident, the impact of the incident and a general description of the incident. Other information may be requested by ComReg during the course of the incident, such as anticipated time to resolution of the incident.

5.3 Provision of information to Minister, European Commission, Other NRAs and ENISA

61 Regulation 23(4) (b) requires that where the Regulator receives a notification under subparagraph (a), it shall inform the Minister of the said notification and, with the agreement of the Minister, it shall also, where appropriate, inform the national regulatory authorities in other Member States and ENISA. ComReg considers that the circumstances under which it would be appropriate to inform other NRAs or ENISA under this regulation are likely to involve incidents with cross border significance. In the case of the majority of incidents ComReg would anticipate that reporting to ENISA and the European Commission will be through the annual reporting required under Regulation 23(5). This states that: "The Regulator shall annually submit a summary report to the Minister, the European Commission and ENISA on the notifications received and the actions taken in accordance with paragraph (4)".

62 Regulation 23 (4)(c) states that where it is considered that it is in the public interest to do so the Regulator, with the agreement of the Minister, may inform the public in relation to the breach notified under subparagraph (a) or require the operator to inform the public accordingly.

63 As identified in paragraph 61 ComReg will each year submit a summary report to the Minister, the European Commission and ENISA on significant incidents as defined in ENISA guidelines as per Regulation 23(5). Furthermore where ComReg is notified of a significant incident, as per the thresholds identified in this consultation applicable to Operators, it will notify the Minister as required under Regulation 23(4)(b).

5.4 Reporting Template

64 The incident reporting template is contained in Annex 1.

5.5 Confidentiality

65 ComReg shall, subject to the Freedom of Information Acts 1997 and 2003, accept as confidential any information provided to the Regulator which is expressed to be confidential, except where the Regulator has good reason to consider otherwise[8].

[8] Regulation 15 of the Framework Regulations 2011

66 Such Information will be treated subject to the provisions of ComReg's guidelines on the treatment of confidential information as set out in ComReg Document No. 05/24

67 Confidential information that is reported by an Operator will be dealt with in a confidential manner by ComReg and ComReg will request that ENISA also treats the information confidentially.

68 ENISA has highlighted[9] the means by which it will handle information that has been classified as Confidential by the Regulator and the Operator. Article 5(3) of Directive 2002/2110 states "Where information is considered confidential by a national regulatory authority in accordance with Community and national rules on business confidentiality, the Commission and the national regulatory authorities concerned shall ensure such confidentiality."

69 Where an incident affects a large number of end users or an important institution, the incident itself is unlikely to be classified as Confidential, whereas information relating to aspects of the incident and associated report may be considered as Confidential.

70 For Information that will be exchanged with Government departments, agencies and the European Commission, ComReg is guided by Article 3 (5) of the Framework Directive[11]. In respect of the information exchanged, the receiving authority is to ensure the same level of confidentiality as the originating authority.

[9] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-for-incident-reporting-v1.0
[10] Framework Directive 2002
[11] Directive 2002/21 Regulatory Framework for Electronic Communications networks and services

6 Minimum security standards

71 Regulation 23(1) imposes an obligation on “Operators providing public communications networks or publicly available electronic communications services to take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.”

72 Regulation 23(2) notes that “The technical and organisational measures referred to in paragraph (1) shall, having regard to the state of the art, ensure a level of security appropriate to the risk presented.”

73 Regulation 23(3) requires that “Operators providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, thereby ensuring the continuity of supply of services provided over those networks.”

74 Interpretation of regulation 23(1) requires an Operator to consider the meaning of “appropriate” technical and organisational measures and the meaning of “appropriately” in “appropriately manage the risks posed”. Similarly regulation 23(2) identifies the need for an operator to a level of security appropriate to the risk presented. This again suggests the need to consider the term “appropriate” as well as understanding the risk that exists. Finally, Regulation 23(3) also requires all appropriate steps be taken.

75 ComReg recognises that not all Operators are the same and therefore the correct degree of risk-management will be a decision for each Operator to make. This decision will involve a number of considerations such as the size of a network, the number of users involved, the service involved, the importance of the service to customers and the area affected.

76 ComReg considers that any investigation into the compliance by an Operator in respect of these regulations will have to consider the proportionality of the approach by the operator and this will include consideration of the costs and benefits of maintaining availability in the context of the network or service in question.

77 ComReg does not intend to be prescriptive in this consultation around the interpretation of these terms as it considers that what is appropriate will vary according to the network and service.

78 ComReg would bring to the attention of Operators the ENISA guidelines for Minimum Security Measures. ComReg will consider the guidelines in this document as well as other specific circumstances when assessing an Operator's compliance with its obligations and as such Operators may wish to comment on aspects of those Guidelines.

79 ENISA has proposed various standards[12] that Operators may use but notes that an Operator may use alternative standards which achieve the same objective. ENISA has taken the security requirements in the most common standards and created a single list of control domains.

80 These controls include

80.1 Governance & Risk Management;

80.2 Human Resources Security;

80.3 Security of systems and facilities;

80.4 Operations Management;

80.5 Incident Management;

80.6 Business Continuity Management; and

80.7 Monitoring, auditing and testing.

81 ComReg would expect that Operators review on a frequent basis the security and integrity of their networks.

82 ENISA advises that Operators should perform risk assessments; specific for their particular setting, to determine which assets fall under the scope of security measures (the assets to which they should be applied). These assets include assets which, when breached and or failing, can have a negative impact on the security or continuity of electronic communications networks.[13]

83 To ensure compliance with the Regulations ComReg intends to use incident reports as an indication of performance of network security.

[12] Technical Guideline for Minimum Security Measures Version 1.0 - https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/technical-guideline-for-minimum-security-measures-v1.0

[13] Section 3.1; Scope of Technical Guideline for Minimum Security Measures Version 1.0

Q. 6	ComReg in addition to monitoring compliance through incident reporting may initiate audits from time to time to ensure Operators' compliance with obligations. Do you agree with this? Please provide your reasoning for your view if you disagree.

7 Implementation & Enforcement

7.1 ComReg monitoring of security and resilience management

84 There are a number of options available to ComReg for monitoring Operators' compliance, such as regular audits, requiring regular reports from Operators and monitoring of incidents through the subsequent reports from Operators.

85 ComReg intends to use reports from Operators as one of the tools for monitoring compliance by Operators with their obligations under Regulation 23 without prejudice to any of its powers. It is ComReg's view that the thresholds set for reporting incidents to ENISA would be inappropriate for this monitoring and it therefore intends to identify through this consultation the appropriate level of reporting, together with the timing for that reporting which can satisfy the three requirements:

- to inform ComReg in respect of its communication with consumers;
- taking appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and service; and
- reporting an incident to ComReg.

86 It is ComReg's view that this approach to monitoring compliance with Regulation 23 will be a lower burden on Operators than regular inspections or other similar methods to ensure compliance, but still effective, however such inspections or audits may be undertaken by ComReg if considered appropriate.

87 The risk of under reporting is low as significant incidents will be in the public domain and a failure by an Operator to report appropriately may be investigated by ComReg and may suggest that an alternative approach to monitoring the compliance by that Operator with the obligations is necessary.

Q. 7 Do you agree with ComReg's position on monitoring Operators' compliance primarily through the use of incident reports submitted to ComReg by Operators? Alternatively, should ComReg monitor compliance through regular analysis of work undertaken by operators, e.g. annual review of risk registers, or through spot checks and reviews from time to time as may be triggered by concerns raised such as the level of incidents reported? Please provide your reasoning for your view if you disagree

88 Under Regulation 24 (2) ComReg may require Operators to provide information that would be required to assess the security or integrity of the services and networks of that Operator, including documented security policies and to submit to a security audit that would be carried out by an independent professional body nominated by ComReg, the results of which would be available to ComReg and the Minister. The cost of such an audit would be borne by the Operator.

89 Accordingly ComReg has the power to issue directions in respect of Operators taking appropriate technical measures and notifying ComReg in the event of a breach of security or loss of integrity that impacts upon the network and to monitor compliance with such a direction. This raises the question as to what the nature of such a direction might be and when it might be appropriate.

90 Without prejudice to the circumstances under which ComReg may consider requiring an audit be undertaken under this regulation, ComReg is likely to issue a direction to an Operator where it believes there is a lack of compliance with Regulation 23 as indicated through incidents which are reported to ComReg.

91 ComReg may also commence investigations as a result of complaints received or disputes brought by Operators or by its own initiative. As examples, an investigation may be triggered if;

91.1 Operators fail to report an incident or fail to report an incident within the time period specified;

91.2 ComReg observe a pattern of incidents occurring on a network or with a service that would lead ComReg to believe that network integrity had been compromised; and/or

91.3 A series of consumer complaints are made involving a high number of users complaining over a short of period of time.

92 An Operator that fails to comply with a direction or the Regulations commits an offence per Regulation 24(4) of the Framework Regulations.

8 Next Steps

93 ComReg is publishing this Consultation and Guidance to inform Operators about the Guidelines attached to Regulations 23 & 24 of the Framework Regulations; specifically the reporting of incidents and the integrity of networks and services.

94 Respondents have 4 weeks from the date of publication to submit any observations to ComReg.

95 Following this period of observations ComReg will publish a response to consultation aspects of this paper.

Annex: 1 ENISA Incident Reporting Template to be used by Operators reporting to ComReg

ELECTRONIC COMMUNICATIONS SECURITY BREACH REPORT Country: Ireland	
Date and Time of occurrence	
Date:	Time:
Executive Summary	
Root cause: Natural Disaster ☐ Human Error ☐ Malicious Attack ☐ Hardware/ software Failure ☐ Third Party Failure/ External ☐ Other(Explain) ☐ Type of Security Breach: NRAs contacted: Security Breach Handling and Response measures: Post Security Breach Measures:	
Impact Description	
Affected Asset: Affected Service:	

Mobile: Voice ☐ Data ☐ SMS ☐ Fixed : Voice ☐ Broadband ☐ Cable : Voice ☐ Broadband ☐ Leased Line ☐ Fixed Wireless ☐ Time to restore: Interconnections Affected: Users Affected:
Short Description, Analysis and Lesson Learnt
Short Description, Analysis and Lesson Learnt

Description of the fields

Country	
Description:	Ireland
Date and time of occurrence	
Description:	Details of the date and time when the security breach took place (in National time). It can be interpreted as the time of discovery of the incident. Time should be expressed in both GMT and BST when appropriate.
Data sets/ values:	Example. 07022012/10:45 BST/GMT (All times are to be local, either BST or GMT depending on the time of the year of the report)
Type of Security Breach	
Description:	The type of the security breach is the category where this breach belongs to e.g. DoS attack causing security breach of congestion in data services. Even though this will provoke the degradation of the quality of service and not its interruption, this will remain an incident that needs to be reported since it will have an effect on the continuity of the service. These could be subcategories of the root causes listed in the according section.
Root cause	
Description:	The initial cause of the security breach (human error, malicious attack etc)
National Regulatory Authorities contacted	
Description:	The competent NRAs in other countries which were notified about the occurrence of the security breach. If authorities from other Member States (“MS”) or third countries are involved in the response action, they should be mentioned as well. Further information (voluntary): The reason a country contacted another MSs competent NRA (this can be also added in the “Additional Information” field).
Security Breach handling and response	

Description:	All the actions taken after the discovery of the security breach and the measures adopted to restore the service to initial conditions/ level.
Post Security Breach Measures	
Description:	Include a description of any arrangements that were made to minimize the level of risk, and comment on how effective you thought these measures were.
Affected Asset	
Description:	An asset's loss potentially stems from the value it represents and the liability it introduces to an actor (organization-provider). Affected asset is the initial target of the security breach. The incident causing chain effects will end in the unavailability of a service to the end user. In this field the starting point of this chain is requested.
Data sets/ values:	Usually involves the catastrophe/ change of a physical asset. Example. Cut cable
Affected Service	
Description:	The affected service is the service which is made unavailable to the end user. In this field a description of the service which value and availability relates to the impact level.
Data sets/ values:	Given through check boxes – you can choose more than one
Time to restore/resumption	
Description:	The time span from the discovery of the security breach (different from the time the security breach happened) until the service is back to the initial level. Further information (voluntary): The time span from the discovery of the security breach (different from the time the security breach happened) to the full service recovery.
Data sets/ values:	Example. 5 hours.
Affected interconnections	
Description:	If the affected service can cause damage/ change to an asset (or service) of another Operator or provider then this is an affected interconnection. In case of a cross border security breach, it would be possible one MS can affect assets of

	another “interconnected” MS. Some concentrations of infrastructure are vulnerable and significant disruption can be caused by localised failure; cascading technical failures can be caused to interconnected systems.
Affected Users	
Description:	The total number of users affected when a security breach occurs.
Data sets/ values:	Absolute number / Percentages
Short Description, Analysis and Lessons Learnt	
Description:	Describe any actions that were taken after the security breach to improve the security of the asset and what procedures will be followed (or measures taken) from then on.

Annex: 2 Legal Basis

The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011 ("the Regulations"), Regulation 23 states:

23. (1) Operators providing public communications networks or publicly available electronic communications services shall take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks.

(2) The technical and organisational measures referred to in paragraph (1) shall, having regard to the state of the art, ensure a level of security appropriate to the risk presented.

(3) Operators providing public communications networks shall take all appropriate steps to guarantee the integrity of their networks, thereby ensuring the continuity of supply of services provided over those networks.

(4) (a) An operator providing public communications networks or publicly available electronic communications services shall notify the Regulator in the event of a breach of security or loss of integrity that has a significant impact on the operation of networks or services.

(b) Where the Regulator receives a notification under subparagraph (a), it shall inform the Minister of the said notification and, with the agreement of the Minister, it shall also, where appropriate, inform the national regulatory authorities in other Member States and ENISA.

(c) Where it is considered that it is in the public interest to do so the Regulator, with the agreement of the Minister, may inform the public in relation to the breach notified under subparagraph (a) or require the operator to inform the public accordingly.

(5) The Regulator shall annually submit a summary report to the Minister, the European Commission and EINSA on the notifications received and the actions taken in accordance with paragraph (4).

(6) An operator that fails to comply with the requirements of paragraph (4)(a) or (c) commits an offence

The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011 ("the Regulations"), Regulation 24 states

Implementation and enforcement

24. (1) For the purpose of ensuring compliance with Regulation 23 (1), (2) and (3), the Regulator may issue directions to an operator providing public communications networks or publicly available electronic communications services, including directions in relation to time limits for implementation.

(2) The Regulator may require an operator providing public communications networks or publicly available electronic communications services to—

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

(b) submit to a security audit to be carried out by a qualified independent body nominated by the Regulator and make the results of the audit available to the Regulator and the Minister. The cost of the audit is

to be borne by the operator.

(3) An operator in receipt of a direction under paragraph (1) shall comply with the direction.

(4) An operator that fails to comply with a direction under paragraph (1) or a requirement under paragraph (2) commits an offence.

Functions of ComReg

The functions of ComReg outlined in the Communication Regulations Act 2002[14] as amended, include:

- 10(1)(a) to ensure compliance by operators with obligations in relation to the supply of and access to electronic communications services, electronic communications networks and associated facilities and the transmission of such services on such networks,
- 10(1)(d) for the purpose of contributing to an open and competitive market and also for statistical purposes, to collect, compile, extract, disseminate and publish information from operators relating to the provision of electronic communications services, electronic communications networks and associated facilities and the transmission of such services on those networks.

[14] http://www.irishstatutebook.ie/2002/en/act/pub/0020/index.html

Questions

Section Page