Commission for
Communications Regulation

Reporting & Guidance on Incident Reporting & Minimum Security Standards

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

Response to Consultation & Guidance

Reference: ComReg 14/02

Version: Final 1.0

Date: 8/1/2014

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
Abbey Court Irish Life Centre Lower Abbey Street Dublin 1 Ireland
Telephone +353 1 804 9600 Fax +353 1 804 9680 Email info@comreg.ie Web www.comreg.ie

Additional Information

ComReg Document 13/10	
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 Response to Consultation is not a binding legal document and also does not contain legal, commercial, financial, technical or other advice. The Commission for Communications Regulation is not bound by it, nor does it necessarily set out the Commission's final or definitive position on particular matters. To the extent that there might be any inconsistency between the contents of this document and the due exercise by it of its functions and powers, and the carrying out by it of its duties and the achievement of relevant objectives under law, such contents are without prejudice to the legal position of the Commission for Communications Regulation. Inappropriate reliance ought not therefore to be placed on the contents of this document.

Content

Section Page

Annex

Section Page

Table of Figures

Section Page

1 Introduction

1. The Commission for Communications Regulation ("ComReg") is the statutory body responsible for the regulation of the electronic communications sector in Ireland. Its activities are governed in part by a number of Directives enacted by the European Union which have been transposed into law in Ireland by means of enacting regulations. Of particular relevance to this document are the "Framework Regulations" of 2011 (The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, SI 333 of 2011) ("The Regulations"). These regulations contain provisions which set out telecommunications operators' and ComReg's respective roles and responsibilities with regard to security and integrity of networks and services.

2. Regulations 23 and 24 of The Regulations, place obligations on Operators 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.

3. Regulation 23 requires an Operator to notify the 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.

4. Where ComReg receives such reports, it is required to inform the Minister and, where appropriate, the European Network and Information Security Agency[1] ("ENISA").

5. 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. In some circumstances this may include an Operator requesting the support of ComReg, for example to assist in its coordination of the incident response with other parties such as other interconnected Operators. This request for support 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 and to enable ComReg to comply with its obligations regarding reporting of incidents.

[1] ENISA is an agency of the EU. The objectives and tasks are outline in Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004

6. This response to consultation document clarifies 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 the reporting requirements. ComReg's approach takes into consideration guidance provided by ENISA in its document: Technical Guideline on Reporting Incidents[2]

7. This document is the response to ComReg Document 13/10. It addresses ComReg's approach to assessing Operators' compliance with their obligations in respect of Regulations 23(1), (2) and (3). ComReg's approach takes into account work undertaken by ENISA and the associated document published by ENISA: Technical Guideline for Minimum Security Measures[3]

8. These two ENISA documents were produced following engagement with a number of stakeholders, including NRAs and Government bodies from Member States. Both documents are guidelines to ComReg in these areas. ComReg envisages that these documents may be amended from time to time and ComReg will be guided by the developments.

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

[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

10. This response to consultation document sets out proposals as to how ComReg interprets the Regulations having considered the views of respondents during the consultation process. The paper describes what actions ComReg expects Operators to take in order to ensure compliance in respect of the relevant obligations.

2.1 Incident Reporting

11. ENISA published thresholds which National Regulatory Authorities (NRAs) should use for defining incidents which must be reported by NRAs to ENISA and the European Commission. 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 specific ENISA threshold for reporting. The thresholds also vary from the ENISA thresholds as ComReg will use the reports to help it monitor compliance with operators to Regulation 23(1), (2) and (3) as outlines in the consultation document, ComReg document 13/10.

12. The consultation document suggested that the reports would also be used to inform ComReg to facilitate ComReg's response to consumer queries. It was noted that a reason for the short reporting timescales outlined in the consultation was that ComReg needs to have up to date information on network and service incidents to be able to deal with consumer enquiries and to maintain a general awareness of the availability of services to consumers and that incident reports will be used to facilitate this. In light of the responses received ComReg has decided, for reasons which are set out below, not to use this process in this manner. Accordingly the expedited reporting timelines originally proposed will not be required. Operators are, however, encouraged to advise ComReg of incidents which could be brought to the attention of ComReg by other means, such as media reports or consumer complaints. If such information is provided it will help to avoid the need for specific information requests from ComReg to operators relating to such incidents.

13. The revised reporting requirements that Operators are to use are outlined in Table 1 and Table 2 of this document.

14. This process is being introduced as a proportionate approach to incident reporting that allows Operators and ComReg to meet their obligations.

15. Reporting requirements are set out in Table 1 – “ComReg Reporting Thresholds for Fixed Line Services” and Table 2 – “ComReg Reporting Thresholds for Mobile Services” in Section 5 below.

16. More significant incidents should be reported by way of an initial report within 1 day of occurrence as set out in the tables. These initial reports can be brief and are likely to include details about the number of users impacted, the service impacted and indication of the likely cause and if possible the expected duration of the incident. Given the short timeline ComReg would accept reasonable estimates of the impact at this stage.

17. Upon resolution of the incident ComReg would expect to receive notification that the incident has been resolved and that services have been restored.

18. Within a reasonable timeframe ComReg would expect to receive a more comprehensive closure report providing clarification on the scale of the incident, its scale, its duration, its cause, the approach taken to resolve the incident and any lessons learned.

19. Less significant incidents are to be included in a report to be submitted at least every six months. These reports should be comprehensive and include individual incident closure reports providing clarification on the date of the incident, its scale, its duration, its cause, the approach taken to resolve the incident and any lessons learned.

20. These six monthly reports are to be provided in July and January for the periods January - June and July - December respectively.

21. Operators may choose to report on these incidents sooner rather than waiting for the July and January reporting dates.

22. Incident reports form a key aspect of ComReg’s monitoring of an operator’s compliance with Regulations 23(1), (2) and (3). In the absence of reports or where reports are not available in a timely manner it is likely that alternative approaches to monitoring compliance would be required, facilitated through Regulation 24(2) information requests or security audits.

23. 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 are shown at Annex 1 of this document.

24. All relevant incidents are to be reported to ComReg at: incident@comreg.ie. Any incident requiring notification in 1 working day or less is to be additionally 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.

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

2.2 Management of the integrity of networks

26. ComReg is not being prescriptive as to the precise measure that operators should take to manage risk in respect of network integrity and security but notes its responsibility to monitor these activities.

27. 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 pursuant to Regulation 24.

3 Background

3.1 Objective of this consultation process

28. The consultation document ComReg 13/10 sought feedback in respect of ComReg's proposals on;

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

29. In addition to the specific requirements under Regulation 23 and 24, the consultation process addressed other reporting requirements and proposed a consolidated reporting process to avoid duplicate processes where possible and avoid unnecessary duplication of work for Operators.

30. In this Response to Consultation ComReg's position on the points outlined in paragraphs 27 and 28 are given having considered the responses received to the Consultation.

Regulation 23- Security and integrity

31. 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):

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.

32. Operators have the responsibility to implement technical and organisational measures to appropriately manage the risks posed to security of networks and services and 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.

33. ENISA guidance material provides an interpretation of the use of the words “integrity” and “security” in these regulations. In this context integrity is considered “as the ability of the system to retain its specified attributes in terms of performance and functionality”. It is considered that integrity of networks would be called availability or continuity in most information security literature. The ENISA document provides guidance to ComReg on the interpretation of “security” with the provision of a single set of ‘security measures’ which addressed the issue of what constitutes appropriate technical and organisational measures.

34. The consultation addressed the concept of “significant impact” for the purpose of determining whether particular incidents should be reported to ComReg. This was addressed in the form of determining appropriate thresholds for incident reporting. Furthermore, when reporting incidents the associated timelines for reporting and the details which should be reported were discussed in the Consultation.

Regulation 24- Implementation and enforcement

35. 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.

36. In the consultation ComReg proposed that the approach to incident reporting could be used in the context of an operator providing information needed to assess the security or integrity of their services and networks. This reporting process may not be sufficient to fully satisfy the requirement for provision of such information but may satisfy a significant aspect of the requirement such that any burden on Operators regarding reporting under Regulation 24 is minimised. Respondents' views in respect to this approach were sought.

37. The consultation document suggested that the reports would also be used to facilitate ComReg's response to consumer queries. An important reason for the relatively short reporting timescales proposed in the consultation was that ComReg needs to have up to date information on network and service incidents to be able to deal with consumer enquiries and to maintain a general awareness of the availability of services to consumers and that incident reports will be used to facilitate this. Given the responses received it has been decided that this reporting process will not be dimensioned to facilitate ComReg's response to consumer queries. However ComReg may decide to use this information internally to facilitate its other functions. Operators are however encouraged to advise ComReg of incidents which are likely to be brought to the attention of ComReg by other means, such as media reports to enable ComReg to appropriately handle questions raised in the context of service integrity with an understanding of the impact or scale of the relevant incident. Such information provided in a timely manner is likely to avoid the need for specific information requests from ComReg to operators relating to such incidents.

4 Review of Responses

4.1 Respondents to the Consultation

38. ComReg received responses from the following parties and thanks all parties for their responses.

- Alternative Operators in the Communications Market ("ALTO")
- AT&T Global Network Services Ireland Limited ("AT&T")
- BT Communications Ireland Limited ("BT")
- Digiweb Limited ("Digiweb")
- Eircom Limited ("Eircom")
- Huawei Technologies Company Limited ("Huawei")
- Hutchinson 3G Ireland Limited ("H3GI")
- Magnet Networks Limited ("Magnet")
- Telefónica Ireland Limited ("O2")
- UPC Ireland ("UPC")
- Verizon Ireland Limited ("Verizon")
- Vodafone Ireland Limited ("Vodafone")

4.2 Incident Reporting Comments

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

39. The thresholds for fixed services garnered a detailed response from most respondents with only Huawei agreeing with the thresholds as proposed.

40. Eircom sought clarification of a number of points in respect to their understanding:

- *– The qualifying reporting criteria are a mixture of the minimum number of customers affected by an incident (specified in column 2 of the table) and the minimum duration of the incident (specified in column 3).* ComReg confirms that this is a correct understanding.

- *– The percentage of customers affected means the percentage of the total number of [Operator] customers that use the affected service (e.g. the number of broadband customers rather than the total of all [Operator] customers).* ComReg confirms that this is a correct understanding.

- *– The initial notification time period commences upon the expiry of the minimum duration of the service impact specified in column 3.* ComReg confirms that this is a correct understanding.

- *–The reporting timeline begins with the notification to ComReg during the maximum time allotted in column 4.* ComReg confirms that this is a correct understanding of the proposal as outlined however, based on comments from respondents; it is proposed to remove the timelines for interim reports as explained later in this document.

- *–Subsequent updates on an incident are to be made during the timeframes that are specified in column 5.* ComReg confirms that this is a correct understanding of the proposal as outlined however it is proposed to remove the timelines for interim reports as explained later in this document.

- *– eircom assumes that the criteria will apply to all fixed line networks; copper, fibre and cable alike.* ComReg confirms that this is a correct understanding and it would also include other technologies such as point to point wireless access and cable.

41. A number of comments were received from respondents in respect of the levels that were proposed as thresholds. These comments were broadly grouped into the following issues:

- The way the levels are set to meet a number of reporting requirements

- The apparent discrepancy between the percentage triggers

- The number of customers impacted which would trigger reports

- The appropriate thresholds for reports to the Minister

4.2.1 The way the levels are set to meet a number of reporting requirements

42. The principle proposed in the consultation was for reports to be used to facilitate ComReg's reporting requirements as per Regulation 23, to help assess Operators' compliance with obligations in respect of taking appropriate measures relating to security and integrity and to inform ComReg in respect of incidents that may stimulate consumer queries to ComReg.

43. Most respondents considered ComReg's approach to be pragmatic and reasonable.

44. Many respondents suggested that ComReg should not focus on using this reporting mechanism for briefing ComReg staff handling consumer calls as customer communication would be more appropriately handled by operators themselves through their communication channels. ComReg agrees that in general it would be expected that operators would be providing appropriate information and updates in respect of incidents through their own customer channels, however in the past ComReg has received requests for information from consumers where they have been unable to obtain information from their operator directly. An issue of this type may arise where an operator does not have appropriate communication channels in place for its customers or the relevant communication channels rely on the service which is disrupted. ComReg considers that as the Operator concerned should themselves be briefing their customer communications channels, such as customer support teams or press officers, it would not represent a significant overhead to also provide the information to ComReg to enable it to address queries from consumers. However, ComReg notes that many respondents felt the resultant lower threshold was too low and, in consideration of the comments that were made and the alternative proposals that were made by respondents. On balance ComReg proposes that it will not dimension this reporting process for this purpose for now and has therefore revised the thresholds and reporting timeframes. It may revisit if significant consumer problems arise.

45. ComReg notes that major operators have been providing reports on incidents on a voluntary basis to ensure ComReg is appropriately informed. ComReg would suggest that such reports should continue as they provide a more structured approach to provision of such information. It is likely that in the event of an incident coming to ComReg's attention through publicly available sources when no report has been provided to ComReg a request for information will be made. ComReg considers that such ad hoc reporting should not be a significant burden on operators as they are likely to be briefing their customer service teams and PR teams as well as having internal management reporting.

4.2.2 The apparent discrepancy between the percentage triggers

46. The proposed reporting thresholds in the consultation were expressed in terms of absolute customer numbers and percentages of an Operator's customer base (for the relevant services). One respondent claimed that there was a disparity between these two figures. For example, where proposed reporting requirements were 1,000 lines or 10% of customers it was noted by the respondent that 10% of Eircom's customer base for various services is far in excess of 1,000 customers.

47. For clarification, the threshold for reporting is the lower rate of either 1,000 customers or 10% of an operator's customer base being impacted by an incident. ComReg is aiming to receive reports from larger operators (where the effective triggers would be 1,000 customers or more) with a view to being aware of incidents that impacted this number of customers. It was also intended that ComReg would receive reports from Operators when 10% of their customer base was impacted as this would provide an insight into the effectiveness of smaller Operators' performance in respect of measures taken around integrity and security. It is considered entirely possible that smaller Operators reporting these incidents would have much lower customer bases and potentially the 1,000 customer trigger would not capture this requirement for such operators.

48. The revised thresholds outlined in this document still have this approach to reporting thresholds for the reasons stated above.

4.2.3 The number of customers impacted which would trigger reports

49. As discussed, several respondents raised concerns around the lower of the customer number reporting thresholds proposed in the consultation. The rationale for these thresholds was that ComReg considered that the benefits associated with such report thresholds would outweigh the burden that would be associated with producing such reports. While there may be a significant number of reports for larger operators it was considered that the information would already be available for operators dealing with incidents and would be of benefit to ComReg when dealing with consumer queries and for statistical analysis.

50. Based on the comments received, ComReg proposes to change the minimum customer levels associated with such reporting arrangements. These revised reporting levels are shown in Tables 1 and 2 of this document.

51. ComReg envisages that it may review these requirements in the light of experience.

52. A respondent also noted that in the event of an incident impacting a significant proportion of a small operator's customer base the focus should be on resolving the problem rather than reporting the incident to ComReg. The respondent noted that in the case of smaller operators there may not be an efficient communications channel with the regulator.

53. The respondent also noted that this requirement resulted in ComReg proposing a low reporting threshold which is significantly below the threshold that is required for reporting to ENISA.

54. ComReg notes the response in respect of this reporting requirement however such reports will form a significant input to ComReg's assessment of an operator's approach to measures for security and integrity. ComReg recognises that the timing for such reports may not be as critical as reports associated with more significant customer numbers therefore ComReg proposes to move the reporting requirement to a more extended time frame. These reporting levels are shown in Tables 1 and 2.

55. One respondent noted that it would be unusual for multiple operators to experience unrelated incidents at the same time, and that related incidents were likely to be the result of a common dependency, such as wholesale use of the Eircom network for example. The respondent's conclusion was therefore that the level of reporting that was suggested would be below that required for reports to ENISA. In response ComReg notes that the purpose of the report is not only to satisfy the ENISA requirement for reporting but to assess operators' compliance with Regulations 23(1), (2), and (3) and hence it believes the proposed thresholds are reasonable in that regard. In addition, ComReg notes that there are other external factors which could impact multiple operators at the same time, such as weather, transport restrictions, power failures and pandemic amongst others.

56. Two respondents highlighted the pan-European nature of their businesses and the need for common reporting systems. While ComReg recognises that some operators operate in other Member States and beyond, the operators are reminded that ComReg is implementing the Framework Regulations from an Irish perspective, taking both national characteristics (market size, population density) into consideration, as well as ENISA guidance. We believe that a reasonable balance between local requirements and pan EU consistency has been struck.

4.2.4 The appropriate thresholds for reports to the Minister

57. A number of respondents noted that the requirement for ComReg to inform the Minister of an incident is triggered by a report of an incident with a significant impact. The respondents raised the issue that frequent reporting of lower level incidents would "desensitise" the Minister to outages and a more reasonable and proportional level for notification to the Minister should be an incident that impacts at least 5-10% of the market, unless critical infrastructure is directly affected.

58. In this context two respondents submitted proposals for ComReg to evaluate the severity of a notified incident and based on the assessment to decide whether it is appropriate to inform the Minister.

59. ComReg considers that the revised thresholds associated with impacted customer numbers more accurately reflect the reporting requirements for significant incidents as required for reports to ENISA. ComReg therefore considers that reports to these thresholds should be notified to the Minister. The thresholds associated with percentages of customer base may not be of an overall scale that needs to be reported to the Minister. ComReg will assess this on a case by case basis.

60. Where an operator chooses to provide other reports for less significant incidents these may not be appropriate for notification to the Minister as suggested in several responses. ComReg will assess this on a case by case basis.

Question 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?

61. Eircom indicated that it felt there were disparities between the percentage figure as a threshold trigger and the actual user numbers. This was a point that was also raised by BT, Magnet, ALTO and UPC. AT&T suggested that absolute numbers of lines be used instead of percentages as a means of preventing possible distortions and maintaining consistency across the EU.

62. An example given by respondents was that 1.2% of the market size of 1.67million according to ComReg's Quarterly Key Data Report Document 12/134 would equate to 20,000 lines. Respondents felt that such a number was too small to warrant reporting to ComReg for an outage.

63. ALTO stated that an outage involving critical infrastructure should be reported immediately but that double reporting may be an issue. It suggested that at most ComReg should assume that three operators may simultaneously experience a network outage, and given the commonly used example of a market with 1.67 million users that the reporting threshold be set at greater than 5,000 users. UPC also proposed this figure.

64. Verizon submitted its own thresholds on which it bases its internal reporting. These thresholds are based on absolute figures given the pan-national nature of its business.

65. For fixed networks Eircom proposed changes to the minimum number of voice customer lines and Internet access customer lines should be increased and that reporting requirements should be relaxed for some of the voice service interruptions.

66. Having considered all of the Respondent's views and noting that the reports will also be used in the context of monitoring operators' compliance with Regulations 24(1), (2) and (3), ComReg is now amending the thresholds for reporting as presented in Tables 1 and 2.

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

67. A number of requests for confirmation were submitted by Eircom:

- *The qualifying criteria are a mixture of the scale of network infrastructure affected (column 2) and the minimum duration of the impact (column 3).* ComReg confirms that Eircom's interpretation is correct.

- *For mobile voice and broadband services, failure of any of RNC, BSC, MSC or HLR means a total failure of single instance device.* ComReg confirms that this relates to a failure of such network elements which is service impacting.

- *The initial notification time period commences upon the expiry of the minimum duration of the service impact specified in column 3.* ComReg confirms that this is a correct understanding.

- *The reporting timeline begins with the notification to ComReg in column 4.* ComReg confirms that this is a correct understanding however, based on comments from respondents; it is proposed to remove the timelines for interim reports as explained later in this document.

68. One other respondent suggested that resellers of mobile services should not be responsible for the reporting of incidents as this should be the responsibility of the underlying network operator. ComReg does not agree with this proposition as it considers that the retail service provider and the underlying network operator would both be obliged to report the incident. Whilst there may be a duplication of reporting, any burden associated with such reporting should be minimal as both operators should be aware of the incident; the reseller so that it can advise its customers and the underlying network operator so that it can advise its wholesale customers. Reporting this to ComReg at the same time should not be a significant issue.

69. Respondents made a number of comments in respect of the thresholds. A comment made by many respondents that a more appropriate metric for the thresholds would be "base stations" rather than "cells". Having considered the responses ComReg agrees with the proposals and has adjusted Table 2 appropriately.

Question 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

70. O2, Eircom and H3GI proposed changes to the thresholds as they generally considered that the thresholds were too low and reporting times for incidents were too short.

71. O2 suggested that the thresholds proposed by ComReg were too low and that ComReg should not deviate from the ENISA thresholds" *that are established"* and are "*the consensus view on events that represent a significant impact"*.

72. O2 highlighted the differences between the proposed national level threshold and the ENISA threshold suggesting that the "disparity" between both is substantial and suggested in its proposed scheme that the limits be higher.

73. O2 indicated that the requirement for lower level thresholds was due to ComReg gathering updates for consumer information. O2 believes that the operator involved in an incident should be the point of contact for the consumer and that it should be the primary point of information. A concern was raised about the generation of reports that could be both time consuming when attempting to resolve an issue and certain incidents may not warrant consumer concern but reports would be required by ComReg.

74. H3GI was not in favour of the low thresholds indicating that daily reporting of outages would be a common event as the proposed ComReg threshold of 20-59 cells would equate to 3 to 9 sites (if a six cell per sector ratio is used) or 2 to 6 sites (if a 9 cell per sector ratio is used). H3GI suggested that such thresholds could lead to daily reporting of incidents by Operators to ComReg.

75. Vodafone suggested that the ComReg thresholds would require an outage involving 4 sites to be reported and continued that certain outages may not affect customer service quality such as loss of cells in the 1800 MHz band. Such outages may not be treated as a priority repair by Vodafone and in such cases the thresholds would impose an operational overhead on Vodafone for an incident where network integrity was not an issue.

76. Eircom is in favour of a threshold that accounts for 50 base stations with an outage of 2 hours and 75 base stations for an outage lasting at least one hour.

77. Huawei favours a base station approach as opposed to a cell based approach for thresholds.

78. H3GI, O2 and Eircom all suggested that 50 base stations (sites) should be the minimum threshold for reporting as this would equate to between 300 and 450 cells.

79. Furthermore at a more granular level involving MSC, HLR, RNC and BSC failure, Eircom suggested that rather than report any impact involving these systems that a failure of minimum duration of 10 minutes be reported. Eircom sought clarification that the term “Any impact” in the consultation was intended to refer to a service impacting incident. ComReg can confirm that this is the correct interpretation.

80. O2 suggested that the minimum outage that would require reporting would be at 6 hours and for incidents that are below this time period and below 50 sites an informal reporting process is developed between industry and ComReg.

81. ComReg considers that having removed the requirement for thresholds which would be used to brief ComReg for handling consumer queries the thresholds can be more closely aligned with ENISA thresholds. In this context ComReg considers that Base Stations could be used as a proxy for customer percentages. As national coverage is available using approximately 2,000 Base Stations ComReg has used that figure as a proxy for the thresholds for ENISA reports being applied to this number.

82. Having considered the Respondent’s views in respect of reporting thresholds and the suggestion to use Base Stations rather than Cells, ComReg is now amending the thresholds for reporting as presented in Table 2.

83. The thresholds that ComReg is working with and the reasoning behind these thresholds is discussed in detail in sections 5.1, 5.3 and 5.4

Question 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.

84. A number of responses were received in respect of the reporting timelines.

85. Eircom highlighted that the severity of an outage may not be known to operators for some time as alarms and customer reports were assessed. An outage that initially may appear low level may escalate to a significant issues and an operator may not be able to predict such an escalation. ComReg considers that the reporting thresholds and timescales proposed in this response to consultation document cater for this issue.

86. AT&T suggested that there should be a consistent approach across all Member States. ComReg notes this suggestion but considers that the approach it is adopting is appropriate for Ireland and, whilst thresholds may vary from Member State to Member State due to different national circumstances, the overall approach is consistent with ENISA proposals. ComReg would also note that when considering all the objectives associated with the reporting of incidents and the associated thresholds, the approach adopted by ComReg minimises the burden on operators.

87. UPC was concerned that resources that could be employed to resolve an interruption would be diverted instead to report to ComReg on such incidents. ComReg disagrees with this view and suggests that Operators when implementing internal processes for communication of service interruption to internal teams or into the public domain should consider adding ComReg to the circulation list for such communications. ComReg has addressed this point earlier in this document.

88. A number of respondents suggested that the reporting proposals for interim would detract from the resolution of the incident. ComReg does not agree that this would be the case as it is considered that an aspect of the process of addressing an incident would include a communications channel to brief management and customers. Notwithstanding that view, having received a number of comments in that regard ComReg has decided to remove the formal requirement for interim reporting with a view to requesting interim reports on a case by case basis as considered appropriate by ComReg. This approach is reflected in Tables 1 and 2.

Question 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?

89. There was a general view among respondents that the requirement for an operator to participate in an audit should not be imposed without due consideration of the implications of such an audit. O2 suggested that audits only be used as a last resort and could only be invoked with justification. Eircom anticipates that audits should only be carried out in exceptional circumstances. H3GI stated that ComReg should exercise its statutory audit rights only where it has reasonable grounds to do so and on an exceptional basis.

90. Whilst some respondents felt that the audits would be too onerous and others were completely against them, ComReg notes that audits are provided for by the legalisation and considers that audits could be used only in a proportionate manner where ComReg deems it necessary.

Question 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

91. The majority of respondents were in agreement with ComReg's intention to monitor compliance through the use of incident reports, agreeing that the other approaches imply more intrusive investigations by ComReg through processes such as the requirement for an operator to submit to an audit or to regularly provide information on risk registers and associated measures.

92. UPC stated that ComReg's primary focus should be to put in place a more reasonable incident reporting process which is structured around meeting any formal annual EU reporting obligations which may be imposed on ComReg or which may be agreed to by ComReg. If and when the EU institutions come forward with specific proposed incident reporting timelines, ComReg should further consult the industry. ComReg should not unduly anticipate possible timelines in that process.

93. ComReg considers that there is sufficient guidance for ComReg in respect of the requirement for incident recording and reporting and the proposals as discussed, having taken on board comments as described in the consultation process are robust.

94. ComReg also welcomes the positive representation made by the majority of the respondents that an incident reporting process is an appropriate approach to monitoring the effectiveness of operators' measures around integrity and security.

95. ComReg agrees that auditing measures taken by operators would be more onerous than using incident reports. Without prejudice to its rights in this regard, ComReg would only intend to impose such requirements in justified cases, such as a failure to provide appropriate information or an Operator having a history of network incidents.

ComReg considerations of Respondents' general questions

96. A number of Respondents asked general questions in their responses that were not directly related to the questions posed by ComReg in ComReg Document 13/10. Having considered the Respondent's views ComReg is now clarifying its position on these specific points.

97. Vodafone stated in its response that the incident reporting process was "*self-defeating ... ComReg would now propose a process which would have the effect of increasing the resource demand on ComReg in return for an unquantified and loosely defined benefit.*" ComReg would note that the incident reporting process is a requirement mandated by Regulations 23 and 24 of the Regulations and that as per its official functions ComReg is the competent authority to implement the aims of the Regulations as outlined in the Communication Regulations Act 2002 as amended. ComReg considers that the proposed process is the proportionate approach to that obligation.

98. H3GI asked why wholesale broadcasting services were not included in the list of affected services where incidents have to be reported to ComReg. ComReg notes that it did not specifically include wholesale broadcasting services in document 13/10 because it is not one of ENISA's defined services that require reporting by ComReg to ENISA and the European Commission. ComReg would advise all Operators that the requirement to report on significant incidents is an obligation under Regulation 23 of the Regulations and while this consultation has sought to provide further clarification in respect of reporting for some of the relevant services it remains incumbent on operators providing public communications networks or publicly available electronic communications services to comply with this obligation. ComReg considers that wholesale broadcasting services would be captured by this requirement.

99. O2 requested clarification on the scope of services that will require notification to ComReg. O2 notes that this is an important consideration as an increasing number of consumers make use of VoIP and other OTT services. O2 notes that incidents will arise where the underlying network is operating correctly, however consumers lose voice service because of a fault in the OTT platform. ComReg would note that Regulation 23(1) and 23(4)(a) refers to "public communications networks or publicly available electronic communications services". It is therefore clear that in the context of the question from O2, the requirement is for a report in respect of incidents relating to publicly available electronic communications services. Where the OTT service is a publicly available electronic communications service and an incident as defines in Tables 1 or 2 occur, the incident should be reported.

100. Verizon stated that it already has pan-European measures in place that meet ISO27001 and that it considers that its measures would satisfy any NRA as Verizon fully complies with the requirements set out under the Framework Regulations. ComReg welcomes all measures taken by Undertakings to meet the needs of ISO27001 and have a robust network that meets the standards envisaged by the Framework Regulations. ComReg notes that the ENISA recommendations are not prescriptive on the standards to be adopted. Summary in respect of Incident Reporting

101. Having considered the responses ComReg has decided it is appropriate to modify some of the reporting thresholds for fixed and mobile incidents. In general these changes equate to higher initial thresholds based upon absolute customer numbers for reporting of some service incidents.

102. In addition ComReg considers that the timeline for reporting an incident where the trigger is based on a percentage of customers should be extended as compared to the original proposal. Such incidents will in respect of smaller operators, where there is a lower impact in terms of absolute customer numbers, be more appropriate. It should be noted that the reporting requirements will be based on the lower threshold of customer numbers or percentages of customers so larger Operators are more likely to have the reporting requirement triggered by absolute customer numbers, not percentage of customer base impacted.

103. In respect to the comments received relating to the burden associated with incident reporting, ComReg has decided to remove the requirement to provide incident reports from the relevant tables, however ComReg may require updates on incidents and such requirements will be communicated to operators on a case by case basis.

5 Conclusion on Thresholds Guidances for Reporting of Incidents

104. ComReg has carefully considered the responses and proposals offered by the Respondents in relation to the thresholds and process for reporting.

105. It should be noted that the thresholds and process for reporting that are now presented to Operators reflect ComReg's view of what is required by Operators to comply with their obligations following this consultation process.

5.1 Basis for setting thresholds for incident reports

106. 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. In this context ComReg has to report on significant incidents to ENISA, the European Commission and the Minister and requires the information from operators to facilitate such reports. In addition to this requirement ComReg has a requirement for information to be provided to assess an operator's compliance with its obligation to take appropriate technical and organisational measures to appropriately manage the risks posed to the integrity and security of networks and services. The thresholds for reporting an incident are based upon a combination of these requirements.

5.2 What constitutes a reportable incident?

107. 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."

108. 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 will be used when considering the type of incident that is required to be reported to ComReg.

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

109. 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.

110. ENISA recommends the following steps be taken by a National Regulatory Authority when an incident is being reported to a National Regulatory Authority[4] by an Operator.

a. 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. Operators should be aware that if ENISA changes its guidelines ComReg will inform Operators of the change of scope of services covered by this reporting arrangement and the accompanying thresholds.

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

111. 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.

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

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

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

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

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

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

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

	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

113. 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).

114. Document 13/10 proposed that 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 reasons for this are:

a) that the threshold to trigger an ENISA report by ComReg will be an accumulation of reports from various Operators that reflect a single outage that impacts more than one Operator;

b) having a lower threshold has the additional advantage that this will enable ComReg to use this reporting mechanism to monitor the performance of an operator in respect to management of appropriate technical and organisational measures to appropriately manage the risks posed to the integrity and security of networks and services. The use of the reports in this way was seen as beneficial by most respondents

5.4 Fixed Line and Mobile Incident Report Thresholds

115. For mobile Operators additional incident reports are required to meet the obligations contained under the Authorisation Regulations (Spectrum Rights of Usage) and the Wholesale Termination Regulations. These reporting requirements are not considered to be met by this process.

116. ComReg will advise the Minister of incidents as required. It is possible that some reports would not require notification to the Minister as they would not be considered to be significant in the context of Regulation 23(4) (a) and (b).

117. The thresholds at which ComReg considers incidents are to be reported under Regulation 24(2)(a) are outlined in Table 1 and Table 2 below. Table 1 outlines the thresholds for fixed line services and Table 2 refers to mobile services. Operators are however encouraged to advise ComReg of incidents which are likely to be brought to the attention of ComReg by other means, such as media reports to enable ComReg to appropriately handle questions raised in the context of service integrity with an understanding of the impact or scale of the relevant incident.

118. ComReg is implementing the following process for incident reporting.

a) An incident as identified in Table 1 “ComReg Reporting Thresholds for Fixed Line Services” or Table 2 “ComReg Reporting Thresholds for Mobile Services is to be reported to ComReg within the timescales identified for reporting.

b) The more significant incidents have reporting requirements of 1 day or less. These initial reports can be brief and are likely to include details of the number of the user base impacted, the service impacted and indication of the likely cause and if possible the expected duration of the incident. ComReg does not require exact information at the time of this report.

c) Upon resolution of the incident ComReg would expect to receive notification that the incident has been resolved and that services are resumed to customers.

d) Within a reasonable timeframe ComReg would expect to receive a more comprehensive closure report providing clarification on the scale of the incident, its scale, its duration, its cause, the approach taken to resolve the incident and any lessons learned.

e) The less significant incidents have reporting requirements based on half yearly submissions. These reports should be comprehensive including individual incident closure reports providing clarification on the date of the incident, its scale, its duration, its cause, the approach taken to resolve the incident and any lessons learned.

f) The half yearly reports are to be provided in July and January for the periods January to June and July to December respectively.

g) Operators may choose to report on individual incidents sooner rather than waiting for the July and January reporting dates.

h) Incident reports will form a key aspect of monitoring an operator's compliance with Regulations 23(1), (2) and (3). In the absence of reports or where reports are not available in a timely manner it is likely that alternative approaches to monitoring compliance would be required, such as audits of operators processes would be required.

i) 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.

j) All relevant incidents are to be reported to ComReg at: incident@comreg.ie. Any incident requiring notification in 1 working day or less is to be additionally 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.

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

Network/Service Type	Min number of customer lines affected (the lower either of number or percentage of users)	Min duration of service loss/disruption (clock hours)	Report to ComReg Within[5] (working hours or working days)
Fixed voice services [F01]	5,000	24 hours	Half yearly[6]
Fixed voice services [F02]	10,000	8 hours	Half yearly
Fixed voice services [F03]	15,000	6 hours	Half yearly
Fixed voice services [F04]	40,000	4 hours	1 day
Fixed voice services [F05]	80,000	2 hours	3 hours
Fixed voice services [F06]	120,000	1 hour	2 hours
Fixed voice services [F07]	10% of customer base	4 hours	Half yearly
Fixed voice services [F08]	25% of customer base	2 hours	Half yearly
Fixed voice services [F09]	50% of customer base	1 hour	Half yearly
Fixed voice services incidents with cross border impact [F10]			4 hours
Internet access service [I01]	6,000	8 hours	Half yearly
Internet access service [I02]	12,000	6 hours	Half yearly
Internet access	30,000	4 hours	1 day

[5] Or at the time the information is made public by the Undertaking
[6] The half yearly reports are to be provided in July and January for the periods January to June and July to December respectively

service [I03]				
Internet access service [I04]	60,000	2 hours	4 hours	
Internet access service [I05]	100,000	1 hour	4 hours	
Internet access service [I06]	10% of customer base	4 hours	Half yearly	
Internet access service [I07]	25% of customer base	2 hours	Half yearly	
Internet access service [I08]	50% of customer base	1 hour	Half yearly	
Internet access service incidents with cross border impact [I09]			4 hours	
Leased Line services [L01]	200	8 hours	Half yearly	
Leased Line services [L02]	400	6 hours	Half yearly	
Leased Line services [L03]	1000	4 hours	1 day	
Leased Line services [L04]	2000	2 hours	4 hours	
Leased Line services [L05]	3,000	1 hour	4 hours	
Leased Line services [L06]	10% of customer base	4 hours	Half yearly	
Leased Line services [L07]	25% of customer base	2 hours	Half yearly	

Leased Line services [L08]	50% of customer base	1 hour	Half yearly
Leased Line Services with Cross Border Impact			4 Hours

Table 1 ComReg Reporting Thresholds for Fixed Line Service

Network/Service Type	Min impact of services affected[7]	Min duration of service loss/disruption (Clock hours)	Report to ComReg Within (working hours or working days)[8]
Mobile Voice, Broadband, SMS [M01]	20 Base Stations service impacted or 1% of customer base	8 hours	Half yearly[9]
Mobile Voice, Broadband, SMS [M02]	40 Base Stations service impacted or 2% of customer base	6 hours	Half yearly
Mobile Voice, Broadband, SMS [M03]	100 Base Stations service impacted or 5% of customer base	4 hours	1 day
Mobile Voice, Broadband, SMS [M04]	200 Base Stations service impacted or 10% of customer base	2 hours	4 hours
Mobile Voice, Broadband, SMS [M05]	300 Base Stations service impacted or 15% of customer base	1 hour	4 hours
Mobile Voice, Broadband, SMS [M06]	MSC Failure or part thereof impacting service.	10 Minutes	4 hours
Mobile Voice, Broadband, SMS [M07]	HLR Failure or part thereof impacting service.	10 Minutes	4 hours

[7] The initial report should only state what is known at that stage, i.e.; what is affected, the area affected, the type and number of customers/users affected, the cause (if known) and the expected time to resolution (if possible).
[8] Or at the time the information is made public by the Undertaking
[9] The half yearly reports are to be provided in July and January for the periods January to June and July to December respectively

Mobile Voice, Broadband, SMS [M08]	BSC or RNC failure impacting service	10 Minutes	4 hours
SMS [M09]	failure >20%<40% of customer base	2 hours	1 day
SMS [M10]	failure >40% of customer base	1 hour	4 hours

Table 2 ComReg Reporting Thresholds for Mobile Services

119. It should be noted that the reporting requirements under this process do not relieve Licensees from their Obligations under their Wireless Telegraphy Licences and that where a Licence Obligation such as Network Unavailability is threatened, then the Licence requirements are not in any way fulfilled or mitigated by this reporting process.

120. The number of impacted customers associated with an incident report, where known, 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.

121. It should be noted that the threshold for reporting outlined in Table 1 and Table 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 these tables, such events may be reported. An example would be where less than 20 base stations are off air, but the geographic area affected by the incident is large.

122. 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. ComReg will inform industry in such an event.

123. ComReg is using categories (F01, F02 etc) to define an incident as this should make it easier for an Operator to report an incident to ComReg when exact numbers of impacted users may not be known.

124. Any service incident that occurs and meets the thresholds outlined that affects service in Ireland is to be reported regardless of whether the infrastructure in question is located inside or outside of Ireland.

5.5 Reporting arrangements

125. To report an incident to ComReg an Operator should email incident@comreg.ie and during the hours of 9am to 5:30pm Monday to Friday (excluding Bank Holidays) should call 01 8049600.

6 Conclusion on Minimum Security Standards

126. Operators should familiarise themselves with ENISA guidelines for Minimum Security Measures[10]. ComReg will consider the guidelines in this document as well as other specific circumstances when assessing an Operator's compliance with its obligations. If these guidelines change ComReg will expect Operators to take such changes into consideration when determining appropriate technical and organisational measures to appropriately manage the risks posed to integrity and security of networks and services.

127. ENISA proposed various standards that Operators may use and ComReg notes that an Operator may use alternative standards which achieve the same objective.

128. 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.[11]

129. ComReg is aware that not all Operators are the same, with significant variations in customer base and product portfolios which may result in different approaches to the management of risk-assessment.

130. As explained in this document ComReg will use reports from Operators as one of the tools for monitoring compliance by Operators with their obligations under Regulation 23 (1). Other formal powers are available to ComReg for information gathering including the use of external audits and ComReg will use such powers as it considers appropriate.

[10] Technical Guideline for Minimum Security Measures Version 1.9 - https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[11] Section 3.1; Scope of Technical Guideline for Minimum Security Measures Version 1.0

Annex 1: Operator Incident Reporting Template

This Template shown below is available here (please click for a pdf document).

ComReg Incident Reporting Template

Version	01-Jan
Date	30/09/2013

Commission for Communications Regulation

Fill out the fields of the incident report

Date of Incident

Year

(Please Check the approriate box)

Incident Category Description (F01, F02 etc)

Service impact

Fixed telephony duration(hours)		Fixed internet duration(hours)		Mobile telephony duration(hours)		Mobile internet duration(hours)		Service duration(hours)	
number of users		number of users		number of users		number of users		number of users	

(Please Check the approriate box)

PSTN		DSL		GSM		GPRS/EDGE	
DSL		Fiber		UMTS		UMTS	
Fiber		Cable		LTE		LTE	
Cable		other		other		other	
other							

Root cause category (Please Check the approriate box)		**Initial cause**		**Subsequent cause**		**Assets affected by initial cause**
System failures		Cable cut		Cable cut		Base stations and controllers(e.g. BTS, NodeB, RNC)
Human errors		Cable theft		Cable theft		Mobile switching(e.g. MSC, VLR, SGSN, GGSN)
Malicious actions		Flood		Flood		User and location registers(e.g. HLR, HSS, AuC)
Natural phenomena		Heavy snowfall		Heavy snowfall		Switches(e.g. local exchanges, routers, DSLAM)
Third party failures		Storm		Storm		Transmission nodes(e.g. SDH, WDM)
		Power cut		Power cut		Core network(e.g. fibre-core, cable-aggregation)
		Power surges		Power surges		Interconnections(e.g. IXPs, IP transit)
		Physical attack		Physical attack		Power supply system(e.g. transformers, power grid)
		Cyber attack		Cyber attack		Backup power supply(e.g. diesel generators, batteries)
		Bad change		Bad change		Cooling system
		Bad maintenance		Bad maintenance		Street cabinets
		Overload		Overload		Messaging center
		Fuel exhaustion		Fuel exhaustion		Switching center(MSC, VLR, e.g.)
		Policy/procedure flaw		Policy/procedure flaw		International backbone(submarine cables, interconnections, e.g.)
		Hardware failure		Hardware failure		Addressing servers(DHCP, DNS)
		Software bug		Software bug		Operator backbone(fiber, cables, e.g.)
		Human error		Human error		Area network(fiber, cables, e.g.)
		None		None		No information
		No information		No information		Other(Please indicate assets not listed)
		Other		Other		

Other impact

Impact on emergency calls Check if availability of emergency services were impacted by the incident.

Impact on interconnections Check if there was impact on interconnections, affecting other operators in the same country or abroad.

Description

General description Description of the incident.

Incident response and recovery actions Description of the actions taken after the discovery of the incident.

Post-incident actions Description of actions taken by the telco to reduce the likelihood of the incident occurring again or the impact of the incident.

Lessons learnt Desciption of lessons learnt, leading to measures or procedures implemented on the long-term.

Annex 2: Legal Basis

The European Communities (Electronic Communications Networks and Services) (Framework) Regulations, 2011, 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 [ENISA] 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, 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[12] 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.

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

Annex 3: **Consultation Responses**

To view the non-confidential responses that ComReg received for this Consultation please refer to www.comreg.ie for the documents accompanying this Consultation.