Rialtas na hÉireann
Government of Ireland

Technical Stakeholder Consultation on Proposed Electronic Communications Security Measures (ECSMs)

Response to issues raised in consultation

2022

Prepared by the Department of the Environment, Climate and Communications
www.decc.gov.ie

Table of Contents

1 Introduction

1. Ireland published the National Cyber Security Strategy in December 2019. Measure 7 of this Strategy sets out how government will introduce a new and specific set of security requirements for the telecommunications sector, with detailed risk mitigation measures to be developed by the National Cyber Security Centre (NCSC) to assist the Commission for Communications Regulation (ComReg) in fulfilling its statutory functions under existing European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011, S.I. No. 333 of 2011 ("Framework Regulations"), the European Electronic Communications Code (Directive 2018/1972) and the new Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, which provides a mechanism for the Minister to specify security measures by Regulation and to make guidelines relating to network security and to provide a legislative basis to enforce the Electronic Communications Security Measures to ensure that electronic communications services and networks are required to ensure the security of their systems.

2. The European Commission, in 2019, recognised 5th generation (5G) deployment of network technologies as a major enabler for future digital services, through its Commission Recommendation on Cybersecurity of 5G networks. This Recommendation addressed cybersecurity risks in 5G networks by setting out guidance on appropriate risk analysis and management measures at national level, on developing a coordinated European risk assessment and on establishing a process to develop a common toolbox of best risk management measures.

3. Ireland's national risk assessment was conducted in the early part of 2019. This work was led by the NCSC in collaboration with ComReg and received input from the mobile network operators, the Defence Forces, the Department of Foreign Affairs and Trade as well as other EU and International partner nations.

4. In parallel to this process, EU Member States published the EU 5G Security Toolbox in January 2020 which represents our coordinated approach to securing 5G networks. One of the major recommendations of the toolbox was that Member States implement strategic and technical security measures which *"strengthen the security of 5G networks and equipment by reinforcing the security of technologies, processes, people and physical factors".*

5. In Ireland, the Electronic Communications Security Measures (ECSM) working group was established in March 2020 to design a set of security requirements for the electronic communications sector. The working group was co-chaired by the NCSC and the Network Operations Unit (NOU) of ComReg. The group also had membership from selected providers of electronic communications networks and services.

6. The group held a series of thematic workshops focussing on the areas identified as presenting the highest risk in the National and EU risk assessments. The workshops included presentations by guest speakers from industry, academia, and relevant public bodies, as well as detailed technical discussions and submissions, which provided insights on the key risks, challenges, and best practices in the relevant security topics. The workshops resulted in the development by the NCSC of the series of documents known as the Electronic Communications Security Measures or ECSMs. In total, ten ECSMs have been drafted:

   - ECSM 001 General
   - ECSM 002 Risk Management
   - ECSM 003 Physical and Environmental Security
   - ECSM 004 Training, Awareness and Personnel Security
   - ECSM 005 Network Management & Access Control
   - ECSM 006 Signalling Plane Security
   - ECSM 007 Virtualisation Security
   - ECSM 008 Network, Monitoring and Incident Response
   - ECSM 009 Supply Chain Security
   - ECSM 010 Diversity, Resilience & Continuity

2 Purpose of consultation and questions asked

7. The Department of the Environment, Climate and Communications (DECC) conducted a public consultation on these proposed ECSM's. The consultation was launched on 23rd November 2021 and closed formally on 28th January 2022.

8. The purpose of the consultation was to gather the views of interested parties, third parties who are directly affected, such as providers of public electronic communications networks and publicly available electronic services, equipment manufacturers and suppliers, and cybersecurity professionals.

9. In gathering submissions, the Department sought to evaluate the technical merit of the proposed security measures and the impact that their implementation will have on the security and networks and services. Stakeholders were asked to consider the following questions in their responses:

   - *Are the identified risks to the security of electronic communications networks and services appropriate?*
   - *Do the recommended security measures adequately address the identified risks?*
   - *Does the implementation guidance and relevant references provide sufficient guidance to implement the security measures?*
   - *What impact will the measures likely have on the overall security of networks and services?*
   - *What costs or challenges may be associated with the implementation of the security measures?*

10. The consultation was published online. Members of the public were able to respond through the submission of general observations and/or detailed drafting suggestions to a Departmental email address. The Department also held a stakeholder information session in December 2021 to answer initial queries in relation to this consultation.

11. There were 17 responses to the consultation in total. These responses came from several sources including telecommunications operators, manufacturers, ICT communications service providers, broadband providers, and various representative associations. The Minister would like to thank all those who submitted responses to the consultation for their valuable contributions.

12. What follows is a high-level summary of these consultation responses organised on at thematic basis and the Government's response to these.

3 Summary of submissions

3.1 Proportionality

13. Several respondents expressed satisfaction that the ECSMs are broadly appropriate and proportionate and that they align with established security practice. However, there were also contrasting views from other respondents who expressed their concern that a "one-size-fits-all" approach to security will not work. They expressed a belief that the measures were overly prescriptive and lacked enough flexibility to adapt to operators of different size, focus, risk profile, or criticality.

14. Some respondents also advised on the importance of finding a balance to allow network operators to implement measures in a manner that is commensurate with and proportionate to their own circumstances.

15. It was proposed that an assessment of compliance should be informed by a view of what operators can reasonably be expected to do in their own individual circumstances. Guidelines or constructive dialogue were also proposed as examples that could be provided for or encouraged between the regulator and operators so that individual operator circumstances can be taken into consideration.

16. A tiered approach within the rules to categorise undertakings and avoid overloading smaller operators was also strongly advocated by respondents. It was further stated that any information obtained from network operators during compliance monitoring needs to be treated with the highest level of confidentiality and security.

17. The need for any restrictions on vendors to be carefully balanced considering the potential impacts on competition and the supplier ecosystem was articulated by respondents, notwithstanding the merits of a standards-based approach to cybersecurity certification.

18. One respondent advocated a wholly technical assessment when it comes to supply chains and discouraged any notion that's some suppliers may be inherently trustworthy and would receive less scrutiny.

19. The challenges for a telecommunications operator to impose security requirements on an external provider if the operator only accounts for a small proportion of the provider's business was articulated by another respondent.

20. Some respondents advocated for any decisions to intervene in the market for supply of network equipment to be measured and proportionate.

3.2 Implementation and engagement

21. Many respondents welcomed what they consider to be a non-prescriptive approach to the measures, noting that the ECSMs are outcome based and each operator has some flexibility on how to achieve those outcomes. Some respondents also opined that implementing further measures in line with the ECSMs may be complex and require time. This would, in their view, require a reasonable implementation or transition period before enforcement action could be considered.

22. The importance of permitting network operators to implement the measures in a manner that is commensurate with and proportionate to their own circumstances, as provided for in the European Electronic Communications Code was also highlighted by a respondent.

23. It was suggested by one respondent that some further practical guidance would be needed for smaller operators. This respondent also contended that further guidance could be provided on how the ECSMs would be updated in the future, including how the Department would remain engaged with industry on developments and how the lead time for implementation for any updates would be addressed.

24. It was further considered by a respondent that measures should ensure that all suppliers are assessed against clear and non-discriminatory criteria.

25. A risk-based approach by policymakers and regulators in planning and implementing the new security requirements was considered necessary by one respondent to ensure the focus is on the areas of greatest risk.

26. It was further contended that the threat model contained in ECSM 001 General, to be used to identify risks, needs to consider all networks equally given what the respondent considers the general applicability of the security measures. Measures should not, in the respondents' view, be focussed solely on mobile networks or specific technologies such as 5G.

27. One respondent further suggested that a review of all the security measures may be necessary, in its view, to ensure that they are written in a high-level way with an appropriate level of generalisation so that they can be compatible with international standards and operators' own security policies.

28. Some respondents would welcome further engagement in advance of the implementation of the ECSMs to best ensure that network infrastructure is secure and so that expectations are clearly understood. Respondents further opined that collaboration and engagement rather than enforcement would be the desirable route to reduce risk, and where there is a holistic approach involving Government, regulators, MNOs, and vendors to ensure security related risks are mitigated.

29. One respondent contended that ECSMs should also apply directly to vendors rather than via contractual obligations with operators.

30. A further respondent would welcome clarification and delineation in relation to the various roles that would be undertaken by the various bodies involved in the future, (including DECC, NCSC and ComReg) in relation to regulation and enforcement.

3.3 Diversity

31. Some respondents expressed an uneasiness in relation to how vendor diversity will work in practice, given that there are a limited number of vendors that are out there and how vendors and operators trade in competitive markets. The concern was that any intervention that restricts the supply further (by for example prohibiting a particular

supplier) would likely concentrate the market further, leaving operators with little choice or bargaining power. This could in turn lead to higher costs and a loss of innovation.

32. There was a view expressed by some respondents that any supply chain diversity assessment should be based on objective criteria that facilitates equal treatment for all vendors.

33. Respondents generally expressed a view that Non-Technical Assessment should focus on transparent standards and fairness with a view to improving supplier diversity.

34. Some respondents expressed concern that any requirement for supplier diversity for any one network element might also leave operators in a weakened position consequently. For example, if there are only two or three suppliers available and a network operator is required to have supplier diversity then they have little or no bargaining power.

35. One respondent opined that while the ECSMs are viewed as generally appropriate, the industry is not yet at the point where end to end networks can move from proprietary elements to virtualised or open-source ones. It would be necessary therefore in its view to understand how the deployment of virtualised elements evolves to best appreciate the appropriate security measures to deploy.

36. One respondent expressed a view that because of the small size of the Irish market, it would be prohibitive from a cost perspective for telecommunications network operators to enjoy complete supplier redundancy across their networks.

3.4 Transition period

37. There was notable feedback from respondents regarding ECSM implementation timeframes. While ECSM 001 outlines that “Legacy networks or equipment which are expected to be decommissioned within the medium term (5 years / 2027) are not expected to have the same level of security as current and future network

deployments", some respondents contended that this timeframe is insufficient. In their view, the 5-year proposal would be better aligned with the life cycle of relevant equipment, which is typically 7 - 10 years.

38. In a similar vein, another respondent maintained that the life expectation of telecoms equipment can be much longer than 5 years and that any measures should be considerate of older legacy equipment.

39. Another respondent contends that a reasonable implementation / transition period should afforded to operators before enforcement action is considered. This respondent opined that in its view, the process for regulatory oversight where an operator proposes risk mitigation rather than full compliance with the ECSMs is unclear and that organisations must have greater certainty on this issue to enable compliance planning.

3.5 Costs

40. The likely weighty cost associated with ECSM implementation was raised by many respondents. Primarily, there was concern expressed regarding the cost of implementing these measures, time it will take and the associated requirement, in respondents views, for what was described as intensive allocation of scarce resourcing. The challenges in being able to recruit qualified, trained, and experienced resource to assist in the implementation of the ECSMs was also highlighted.

41. Some respondents further opined that the retirement of legacy network equipment could lead to a significant cost for operators and even customers in some cases. Matters of functionality and cost overhead, which it was contended would arise from the mixing of equipment from different vendors in a single network, was also raised.

42. One respondent was of the view that there should perhaps be a greater emphasis for policymakers and regulators on understanding that there must be a positive return on overall investment so that sufficient funds are generated for future investment. This it believed should be reflected in economic policies and regulations that put a premium on telecommunications quality and prioritises investments in security.

3.6 Supply chain security

43. Some respondents proposed that assessments be primarily based on technical assessment, supplemented by certain important non-technical assessment factors that are fact based.

44. Some respondents highlighted that, in their view, no regulatory framework or standard could be expected to address all security risks and that operators would likely identify more specific risks specific to their operations. Such matters would need to be discussed with the regulator and mitigations prioritised in addition to compliance with the provisions of the ECSMs.

45. A further respondent believed that a level playing field should apply to ensure that critical national infrastructure is consistently protected from cybersecurity threats. This party considered that this could be best achieved by ensuring that all relevant legislation regarding cybersecurity risks extends to all entities in the supply chain for critical national infrastructure and not telecommunications network elements alone.

46. Finally, some respondents maintained that, in their view, policies should be risk-based, flexible, robust, embrace collaboration and promote innovation-friendly and technology-neutral solutions. Policies should also foster voluntary public private partnerships and draw on existing best practices.

4 Departmental reply

47. The Department is very grateful for the engagement of interested parties in this important consultation.

48. The Security Measures captured by the ECSMs are done so in a high-level manner to ensure compatibility with both international standards and the security policies of

network operators. As such, the ECSMs should perform well as the minimum baseline of security. We would advise network operators to utilise the outcomes described in the Security Measures section of the ECSMs to aid in the examination and confirmation of the effectiveness of their own security policies, processes, and procedures. The high-level approach of the ECSMs serves to facilitate their compatibility generally with international standards and network operators' own security policies.

49. Regarding some concerns expressed with regard to fragmentation, the ECSMs are based on international standards, and also aligned with ENISA guidelines. The ECSMs will be applicable to all publicly available Electronic Communications Networks and Services regardless of platform. However, the ECSMs are not directly applicable to vendors. Respondents will be aware that the legislation places these obligations on providers of publicly available electronic communications networks and services.

50. ECSM001 sets out the risk-based approach that operators should consider in the implementation of appropriate levels of security controls. This section usefully provides four separate examples to help profile operators of different size and consequently the level of security controls that would be appropriate to the operators' risk profile. It should be noted that the categorisation detailed within ECSM001 is for example only. ComReg may assess the risk profile of operators on the evidence provided to it while executing its duties.

The proportionate approach to the implementation of ECSMs is set out in ECSM 001 and usefully provides some examples of factors which could vary the risk profile of individual operators where appropriate. Cognisant of the requirement of operators to implement a risk-based approach to the security of networks through risk assessment, it is expected that operators with varying risk profiles will likely implement varying but nonetheless appropriate levels of security controls ranging from basic to advanced security controls. This proportional implementation of the security measures is also outlined for convenience at the beginning of Section 7 of each of the other ECSMs (ECSM 002 to ECSM 010). While Basic, Industry Level, and State of the Art security measures are not defined in the ECSMs, they are detailed in the ENISA "Guideline on Security Measures Under the EECC" and will be further specified by ENISA's "5G Security Measures Matrix". This will be further addressed in the ECSMs to be issued

under the Communications Regulation (Enforcement) Bill once passed into law this year.

The tiered approach for proportionate regulatory supervision, monitoring and compliance of ECSMs, commented on by many respondents will likely be revisited by ComReg in its future public consultations.

51. The matter of costs featured in many consultation responses; a matter addressed in ECSM 001. The Department acknowledges that implementation of the ECSMs will be a complex programme that will in some cases require significant investments in time, financial and human resources as well as costs necessitated by compliance. However, such costs will need to be managed by operators to meet the requirements set out in the ECSMs. As we are all only too aware, the value of investment in the security and resilience of networks and services can dwarf the costs of recovering from an attack, particularly when one has regard to the reputational risks and damage that such attacks can cause society at large, including operators and consumers.

52. Guidance on what may qualify as legacy equipment or infrastructure will be addressed by the ECSMs to be issued under the Communications Regulation Bill when passed into law this year. In cases where operators contend that equipment is not feasible or available to comply with ECSM requirements, they will be required to provide sufficient evidence to support any case put forward to ComReg in respect of a temporary exception to compliance.

    Similarly, should an operator contend that it is not feasible to comply to ECSMs due to legacy equipment, infrastructure, or any other reason, it will be required to provide sufficient evidence to support such a case. For example, this could include detailed evidence including but not limited to equipment swap out/sunset plan; technical specifications as to why equipment is defined as legacy; and / or evidence that the equipment is not growing in utilisation or use. ComReg will assess any such case on its merits and based on the evidence put forward before any such equipment is deemed to be legacy for the purpose of exception to compliance of the ECSMs. Any such cases will need to be made in full to ComReg in accordance with the timelines it provides.

In such circumstances, an operator will also be required to complete a risk assessment on equipment or infrastructure defined as legacy and to put in place interim alternative security measures in the event it cannot meet the ECSM requirement.

53. Several respondents have highlighted the importance of a reasonable implementation / transition period in advance of any enforcement action being taken. As such, the Department and ComReg are pleased to provide for further engagement with respondents on this matter.

54. The Department notes the need for the information obtained from network operators during compliance monitoring to be treated with the highest level of confidentiality. This is of course a standard practice for both Department and ComReg given the nature of the task. Interested parties can find further information on ComReg's treatment of confidential information in its document 05/24, available at www.comreg.ie.

55. Some respondents have called for further stakeholder consultation to include other key stakeholders. The existing consultation on these measures has been extensive and the Department is very appreciative of all that contributed at this stage. There will of course be further consultation regarding draft legislation that will follow these measures when finalised.

56. The Department acknowledges that measures will need to be updated from time to time and as addressed in ECSM 001. This is best practice and so ECSMs must remain open to review to ensure they are updated and adapted as new risks emerge. Any such amendments will be provided for under section 7 of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 which deals with 'Security measures guidelines' of which the ECSMs will form part of guidance that the Minister may provide to providers.

57. The Department notes some concerns regarding how vendor diversity may work in practice. Respondents are reminded that, in keeping with the EU 5G Toolbox which sets out a coordinated European approach based on a common set of measures, Ireland is required to maintain a diverse and sustainable supply chain in order to eschew any prospect of long-term dependency.

58. The Department welcomes the broad support for the ECSMs and is very appreciative of the time taken by respondents in outlining their views on the challenges ahead.

Apart from changes highlighted in this response to consultation, the Department currently envisages that there may be some material changes to the current version of the ECSMs. Any further changes, if required, will be incorporated in further releases of the ECSMs.

Following the commencement of Part 2 of the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, the Department will update the ECSMs and review the detailed drafting suggestions which were kindly submitted by respondents with a view to inclusion in this update

.