



An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

ComReg Response to the National Cyber Security Strategy Consultation

Response to Consultation

Reference: ComReg 20/01

Version: FINAL

Date: 13/01/2020

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation

1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie

Additional Information

Approval

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.



By email to cybersecurityconsultations@dccae.gov.ie

1 May 2019

Internet Policy Division - Consultation
Department of Communications, Climate Action & Environment
29-31 Adelaide Road
Dublin
D02 X285

RE: COMREG RESPONSE TO THE NATIONAL CYBER SECURITY STRATEGY PUBLIC CONSULTATION

To whom it concerns,

On behalf of the Commission for Communications Regulation (“ComReg”) I wish to express support for the draft National Cyber Security Strategy, as set out in the public consultation published by the Department on 19 March 2019 (“the Consultation”).

ComReg views the cybersecurity of electronic communications networks as a matter of key importance, especially as those networks continue to grow and as services provided through those networks become ever more widespread and essential to socio-economic activity and wellbeing. Ever increasing reliance on connectivity, by Irish consumers and business alike, means that the resilience of communications networks has become a matter of critical concern, now and in future.

The European Commission makes much the same observations in its Recommendation on Cybersecurity of 5G networks, published on 26 March 2019. The Commission views future 5G networks as a priority for the Digital Single Market strategy as they will build on current 4G networks to become the backbone for essential services such as energy, transport, banking, and health. The Commission also notes that industrial control systems and even democratic elections will increasingly rely on 5G networks.

As networks are and will continue to be critical infrastructure, ComReg shares the European Commission’s concern as to the potential consequences of any systemic and widespread disruption to those networks. ComReg also agrees with the Commission that network cybersecurity is necessary to ensure European sovereignty and strategic autonomy, noting that the interconnected and transnational nature of networks is such that a vulnerability in a network in any one Member State could affect networks in any or all other Member States. Secure networks are also of central importance to the wider objective of ensuring all forms of online digital services are as robust and secure as possible.

As stated in the Consultation, the European Commission’s Digital Economy and Society Index (‘DESI’) ranked Ireland in sixth place in Europe in 2018. A key part of the DESI calculation is connectivity - that

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation

1 Lárcheantar na nDugaí, Sráid na nGildeanna, BÁC 1, Éire, D01 E4X0.
One Dockland Central, Guild Street, Dublin 1, Ireland, D01 E4X0.
Teil | Tel +353 1 804 9600 Suíomh | Web www.comreg.ie



is, the ability to exchange information using electronic communications networks and services – and key aspects of connectivity are the security and resilience of networks.

At present, all providers of public communications networks and publicly available communications services in the State are required to take appropriate technical and organisational measures, having regard to the state of the art and in order to ensure a level of security appropriate to such risks and to prevent and minimise the impact of security incidents on users and interconnected networks. In meeting their obligations, providers of such networks and services are also playing a supportive role in making internet-based information services more robust and secure. ComReg has certain powers to monitor providers' compliance with their requirements and to issue directions to providers for the purpose of ensuring their compliance with their obligations as outlined herein, where objectively justified and proportionate to do so.¹

While cybersecurity is a specialised area of information technology and is not within ComReg's competence, all credible risks to the current and future security of Ireland's public electronic communications networks and services should be identified and managed by providers of such networks and services. ComReg views a National Cyber Security Strategy as a complementary framework to its role with regard to the resilience and security of electronic communications networks and services in Ireland.

Yours sincerely

George Merrigan
Director, Market Framework
Commission for Communications Regulation

¹ Please see regulations 23 and 24 of the of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (S.I. 333/2011)