



CONSULTATION DOCUMENT

Measures towards enhancing the security and integrity of Electronic Communications Networks and Services

Outline Document

MCA Reference: MCA/C/23-4803

Publication Date: 6th January 2023

 (+356) 2133 6840  info@mca.org.mt  www.mca.org.mt/


 Valletta Waterfront, Pinto Wharf, Floriana FRN1913, Malta

TABLE OF CONTENTS

1	Introduction.....	1
2	The Objectives and the Principles Underpinning the Proposed Security Framework.....	3
3	The Key Proposals.....	4
3.1	Minimum Security Measures.....	4
3.2	Security Audits.....	4
3.3	Incident Reporting.....	4
3.4	CSIRTS	5
4	The Legal Basis	6
5	Schedule of rolling out the framework	8
6	Key Definitions.....	9
6.1	Definition of Critical Assets	9
7	Invitation to Comments	11

1 Introduction

The security of Electronic Communications Networks and Electronic Communication Services (collectively referred to as Electronic Communication Networks and Services or ECNS) is critical to foster trust in the technology which nowadays features in every aspect of our day-to-day lives. Advanced forms of communication technologies, such as mobile services and high-speed fixed broadband services, have repositioned themselves from mere commodities a couple of years ago to become vital services.

Electronic Communications Networks and Services are key pillars to the development of the digital society and its economy. During the recent pandemic period, when physical mobility was restricted in an effort to curb the spread of the SARS-COV-2 virus, the ECNS sector has proved itself vital in providing the necessary connectivity letting businesses, schools, entertainment services to operate, thus enabling different sectors of the economy running. It also showed its robustness in the form of agility to meet sudden changes in demand for network resources. It also showed that fast and efficient connectivity might enable members of society to seek opportunities that lie far and beyond where they are physically located.

Nevertheless, the connected and global nature of the ECNS sector renders it also vulnerable to attacks and security and integrity issues. Moreover, ECS are also a common component of other critical and essential services delivered in Malta. Therefore, any security and integrity risks may be propagated to other essential services, thus increasing the importance of ensuring the security of the ECNS sector.

The role that the ECS sector has played in sustaining economic and societal activity during the peak period of restrictive measures intended to curb the spread of the SARS-COV-2 virus is just one example of the essential requirements to maximise the availability, security and resilience of electronic communications networks and services. Electronic communication networks and their services are an instrumental part of our everyday life, whether to keep offices running, enable students to receive their education online, or keep families entertained.

The European Commission has also recognised the relationship between communication networks, society and the advancement of its economy. Together with the co-legislative bodies, the European Commission has invested significant resources in advancing the regulatory toolbox to address the security of networks and services across the whole Union. The key documents in this field remain the European Electronic Communications Code (hereafter referred to as the “EECC”), where security provisions applicable to electronic communications are presented as a critical instrument to safeguard the interests of the consumer. The Recommendation on Cybersecurity of 5G networks focuses on recognising and addressing those threats which are specific to 5G Networks and related services. Other

key legislative instruments are the Network and Information Systems Directive (NIS)¹, which focuses on the security of network and information systems intrinsic to key sectors of the economy and the Cybersecurity Act², which amongst others, assigns key roles to the ENISA, the European Union Agency for Cybersecurity as a centre of expertise for cybersecurity in Europe. ENISA is also entrusted to help the EU and its members to be better equipped and prepared to prevent, detect and respond to information security problems.

This consultation paper, spread across three documents, proposes a security framework (hereafter the 'Framework') that targets electronic communication networks and services. At face value, it could be argued that the motivation for the development of this framework is an administrative one, that of providing an interpretation of the national law³ that transposes Articles 40 and 41 of the EEC Directive and thereby establishing the details of its implementation. However, the Authority notes that the primary driver for this initiative is to recognise the instrumental role of electronic communications, primarily the importance of reliable and secure electronic communications in modern society. The proposals are also presented in recognition of the security risks inherent with advanced and globalised communication systems and the need to address these complexities.

The Framework presented in this consultation aims at establishing the foundations upon which future regulatory incentives will be built. As a first step, this framework will also establish a baseline to which all operators of electronic communication networks and services shall be required to achieve. This is also a technology-neutral framework which shall be applicable to all types of electronic communication networks and services. The Authority may, in the future, also issue guidelines or decisions as it may consider necessary which are more technology-specific.

¹ Regulation (EU) 2016/1148 <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32016L1148>

² Regulation (EU) 2019/881 - <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

³ Articles 40 and 41 of the EEC Directive are transposed in Part VII of SL 399.48 of the Laws of Malta

2 The Objectives and the Principles Underpinning the Proposed Framework

In view of the recent technical, strategic and legislative developments both in Malta as well as across the European Union, the Authority is seeking ways to upgrade the current regulatory approach with regard to the security and integrity of the ECNS. While ECNS providers have a general obligation at law to ensure the security of their networks and services, there is no formal framework that establishes how this obligation is to be met, assessed, and measured. The Authority is hereby presenting a security framework to address this.

The following are the primary objectives of the proposed framework:-

- Provide a common framework applicable to all providers of electronic communications networks and services shall apply to determine and document the risk associated with operating the Electronic Communication Networks and Services.
- To contribute towards a high level of security and integrity of Electronic Communication Networks and Services, which safeguards consumer interest, eventually resulting in enhanced demand and calls for further growth in the sector.
- To harmonise measures that provide clear and comprehensive tools necessary to assess and address those security risks associated with existing technologies and future ones. In particular, attention is given to latent vulnerabilities inherent in current technologies as these become increasingly at risk of being discovered and exploited by malicious actors.
- To support and facilitate both the implementation of the security measures initially laid down in the European Electronic Communications Code (EECC) directive and transposed in national law, as well as the Recommendation towards the Cybersecurity of 5G Networks,
- To provide the Authority with incident monitoring tools and mechanisms that assist the Authority in assessing the effectiveness of the proposed framework. Such assessment is necessary for the Authority to tailor the regulatory measures, thus ensuring efficiency in meeting its objectives without causing unnecessary burdens to the market.

3 The Key Proposals

This section presents the key highlights of the proposed framework.

3.1 Minimum Security Measures

Regulation 28(1) of the S.L 399.48 of the laws of Malta (hereinafter the ECNSR or Regulations) requires that providers of publicly available Electronic Communication Networks and Services shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and services. In its proposal, the Authority considers the details of the technical and administrative operations to understand the inherent risks and the relevant mitigation measures indicated to address them. The Authority also proposes a minimum set of mitigation measures that should be implemented for a provider to be considered as having met the requirements of this regulation.

3.2 Security Audits

Regulation 30(2) of the ECNSR empowers the Authority to request providers of publicly available Electronic Communication Networks and Services to submit to an audit. In this context the Authority proposes that providers should carry out audits on a periodic basis. In addition, to ensure that the audit meets the objective set out in the law, the Authority is proposing a regulatory measure to ensure that the audit meets the objectives of the regulation, while further reserving the right for the Authority to maintain control of key aspects of the audit.

3.3 Incident Reporting

Regulation 28(2) of the ECNSR requires that if incidents have a significant impact on the security of electronic communication networks or services, the providers are required to notify the Authority of such incidents without undue delay and in doing so prepare an incident report providing details of the cause of the incident, and actions to be taken to prevent similar occurrences. In this consultation, the Authority will (a) provide a clear meaning to the term “significant impact on the operation of networks or services” and (b) define appropriate reporting procedures together with the information required in such reports.

Noting that the Authority published incident reporting guidelines in 2013, and that the proposals on incident reporting are far reaching, the Authority proposes that the guidelines

currently in place shall be eventually repealed and replaced by the proposed Framework upon publication of the final Decision following this consultation process.

3.4 CSIRTS

Knowledge collected through broader collaboration with other industry players, is a source of valuable information which feeds into the security cycle. Such sources of information include fellow network providers and suppliers that are typically connected through CSIRT networks. These function by relaying intelligence information harvested from a broader scope of bodies within the industry and sharing it with all participants within the network. Members of CSIRTS benefit from the collective knowledge gathered from multiple incidents and analysis of various threat vectors that the provider did not necessarily experience.

In its consultation paper on establishing the Minimum Security Measures, the Authority proposes that providers of ECNS that operate Category A Assets⁴ should ensure that the Chief Information Security Officer (CISO) is continuously accessible on a 24/7 basis both for the providers of locally-based Electronic Communication Networks and Services, and when necessary with national competent authorities and the Malta CSIRT for information exchange and collaborative mitigation action that may be necessary to curb network threats. This measure is presented as an interim measure where the main objective is to achieve a situation where ECNS providers have in place a CSIRT function that collaborates with its peers by sharing and gathering information.

⁴ Refer to definitions section for further detail and Category A and Category B assets.

4 The Legal Basis

Articles 40 and 41 of the EECC are transposed into national law in Part VII of ECNSR. Regulation 28 of ECNSR imparts obligations on the publicly available electronic communication network and service providers, while regulation 30 of ECNSR provides the Authority with the necessary regulatory tools to supervise the security aspects of the sector.

The following are the main principles of the security provisions as listed in Part VII of the ECNSR that are relevant to the proposal of this Framework:

1. Providers are obliged to take the necessary technical and organisational measures to appropriately manage the risks posed to the security of their networks and services. Providers are further expected to adequately manage their risks while considering the state of the art of technology.
2. Providers are obliged to report those security incidents which significantly disrupt electronic communication networks and services to the Authority.
3. The Authority may request from the providers any documentation necessary to assess the security of their networks and services. The proposals in this framework discuss the documentation to be maintained by the providers, primarily regarding risk assessments and policies, procedures and maintenance of relevant evidence.
4. The Authority may require providers to submit to a security audit. The proposals in this framework detail how the requirement of such audits are achieved and assessed.

The security provisions in Part VII of the ECNSR are supported by definitions listed either in the same regulations or in the Electronic Communications and Networks (Regulation) Act (cap. 399). The following definitions are of relevance:

Security of Networks and Services - refers to the ability of electronic communication networks and services to resist, at a given level of confidence, any action that compromises the integrity, authenticity and confidentiality of both (a) the networks and services themselves, but also of (b) the data that is stored within the network and flowing through the networks and services.⁵

Security Incident refers to an instance where the security of the networks and services has been actually compromised.⁶

⁵ See definition of “security of networks and services” as per article 2 of Cap. 399.

⁶ See definition of “security incident” as per reg. 2 of SI 399.48.

Reference to the definitions of electronic communication networks and electronic communication services are also an operative part of the definitions of security and security incident as these address which elements of the ECS and ECN lie within the scope of the proposed framework.

The definition of an electronic communications network includes what can be termed as traditional networks capable of carrying signals through wired, optical or wireless means. Under the EECC, the definition of the network includes its components, both active and passive. This is important within the context of security as the provisions of security and integrity also extend to all the elements encompassed within this definition.

Following the transposition of the EECC under Maltese law, the term “electronic communication services” has been extended to include those services that are provided (either directly or ultimately) over an electronic communication network. By way of example, a voice service could be delivered directly over a network capable of transmitting voice communications – e.g. mobile network. In addition, voice services may also be delivered as a service running over a broadband access service, which in turn requires a physical network able to deliver the broadband access service. The EECC provides a very granular hierarchy of these services. However, this is of little relevance to the discussion on security since the security provisions are applicable uniformly across the board.

5 Schedule of rolling out the Framework

The provisions of the Framework, along with the implementation timelines proposed for the different elements of this Framework, shall apply to all providers of publicly available electronic communication networks and services.

However, in managing the implementation of this Framework, the Authority is proposing that its detailed supervision will be staggered in two phases. Considering that operators of Category A Assets⁷ have the largest subscriber base and therefore pose a bigger risk of disruption on the national scale, it is proposed that initial focus will be set on operators that have at least one Category A Asset during the initial phase.

The Authority shall reserve the right to initiate an ad-hoc supervision process on any provider subject to this Framework if the Authority considers that a provider is deemed subject to significant security risk and/or suffers from a security incident of a significant scale.

The timelines for detailed supervision of the remaining ECNS providers shall be deferred to a later date when the MCA deems it appropriate.

⁷ Refer to section 6.1 for details about the term

6 Key Definitions

For the purposes of this Framework, unless the context suggests otherwise, the definitions that are listed in the Electronic Communications (Regulation) Act and the ECNSR shall prevail.

Additional definitions referring to assets are discussed in the next section.

6.1 Definition of Critical Assets

In this Framework, all the components required to set up the electronic communications network and service, both active and passive, are referred to as 'assets'. Assets are classified as either 'critical' or 'non-critical'. 'Critical assets' are further classified in two, with the criteria used to classify the assets shall be determined on the basis of the influence that the asset has on delivering the network and/or service measured by the number of subscribers and the geographical reach.

The remaining assets which do not fall within any of the aforementioned categories shall be considered as 'Non-Critical Assets'.

Category A Assets are those assets operated and managed by or for an operator of an electronic communications network and/or service which:

- a) When degraded, disrupted, or rendered entirely inoperable, will cause disruption or loss of service to a significant number of subscribers or a significant geographical area as follows:

- (i) A significant number of subscribers refers to at least 25% of the national subscribers of a service. The impacted subscribers shall include those directly serviced by the provider suffering the disruption and by third parties who service their customers using the disrupted infrastructure:

Provided further that in those cases where the estimate of the impacted subscribers is not easily calculated, then the use of geographic estimates is to be used. In such circumstances where the disruption of service can reach at least 20% of a contiguous area in Malta and Gozo, then such an asset is considered to be Category A.

- (ii) The term significant geographical area refers to a contiguous area in Malta and Gozo of similar characteristics. Individually, Malta and Gozo form two such distinct areas based on their natural boundaries. Other characteristics may include the economic importance of some specific

areas, e.g. regions of high value to the tourism industry, industrial regions or of special economic or administrative value, amongst others. The Authority may issue further guidelines on the classification of these areas and their identification.

- b) Provide international connectivity to Malta and Gozo. Such assets will include both the submarine infrastructure connecting Malta to foreign territories and related land-based infrastructure, including but not limited to landing sites and backhaul, land-based equipment connecting the landing site to the operations centre of the provider.
- c) Designated as critical by the Authority, as a result of the implementation of such designation arising from the classification exercise of assets carried out at a European level introduced either directly through EU legislation, by recommendations by the European Commission or by EU expert bodies such as ENISA.

Category B Assets are those assets which, when degraded, disrupted, or rendered entirely inoperable, will disrupt a significant portion of the subscriber base of the network and service provider, such that the level of disruption shall be classified as Level 3 in the Incident Classification Category as proposed in the Incident Reporting section of this Consultation. However, such disruption does not have significance on a national scale.

Consultation Questions

O 1	What are your views on the proposed classification of critical assets?
------------	--

7 Invitation to Comments

In accordance with its obligations under Article 4A of the Malta Communications Authority Act [Cap. 418], the Authority invites written submissions from interested stakeholders during the consultation period, which shall run from the 6th January 2023 to the 3rd March 2023.

The Authority appreciates that respondents may provide confidential information in their feedback to this consultation document. This information is to be included in a separate annex and should be clearly marked as confidential. Respondents are also requested to state the reasons why the information should be treated as confidential.

For the sake of transparency, the Authority reserves the right to publish a list of all respondents to this consultation. The Authority will take the necessary steps to protect the confidentiality of all such material submitted in accordance with the Authority's confidentiality guidelines and procedures. Respondents are however, encouraged to avoid confidential markings wherever possible.

All responses should be submitted electronically to the Authority on consultations@mca.org.mt, and addressed to the Chief Executive Officer.

Extensions to the consultation deadline will only be permitted in exceptional circumstances and only where the Authority deems fit. The Authority reserves the right to grant or refuse any such request at its sole discretion. Requests for extensions are to be made in writing within the first ten (10) working days of the consultation period. Any other requests shall not be considered.



MALTA COMMUNICATIONS AUTHORITY

-  (+356) 2133 6840
-  info@mca.org.mt
-  www.mca.org.mt
-  Valletta Waterfront, Pinto Wharf,
Floriana FRN1913, Malta