THE SECURITY OF NETWORKS AND INFORMATION SYSTEMS LAW OF 2020

———————

Decision under sections 17(r), 17(s), 17(v), 17(w), 17(ee), 20(1)(c) and (4), 40, 43 and 46

Preamble.
89(I)/2020

In exercise of the powers vested in it by sections 17(r), 17(s), 17(v), 17(w), 17(ee), 20(1)(c), 40, 43 and 46 of the Security of Networks and Information Systems Law , 2020, the Digital Security Authority (hereinafter "the Authority"), decided to issue this Decision which prescribes the framework of digital security measures for networks and information systems in the field of Fifth Generation Networks and Communications (5G) in Cyprus.

The Authority issues this Decision after taking into account, inter alia:

Official Journal of the E.U.: L194,19.7.2016, p.1.

(a) the provisions of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems throughout the Union,

Official Journal of the E.U.: L321, 17.12.2018, p.36.

(b) the provisions of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code,

(c) the provisions of the Security of Networks and Information Systems Law, 2020 (L.89(I)/2020),

Official Gazette, Suppl.III (I): 1.07.2011.

(d) the Security of Networks and Information Order ,2011 (P.I. 253/2011),

Official Gazette, Suppl.III(I): 25.10.2013.

(e) the Notification of Security Breaches or Loss of Integrity of Networks and/or Services Order of 2013 (P.I. 371/2013),

(f) the Decision of the Council of Ministers no. 86.094 and dated 01/11/2018,

Official Gazette, Suppl.III(I): 28.06.2019.

(g) the Security of Networks and Information Systems (Notification of Incidents) Decision, 2019 (P.I. 218/2019),

Official Gazette, ,Suppl.III (I): 21.08.2020.

(h) the Security of Information Systems (Security Measures of Operators of Essential Services and Operators of Critical Information Infrastructure) Decision,2020 (P.I. 389/2020),

(i) the National Strategy for the security of networks and information systems and cybersecurity;

(j) the Cybersecurity of Fifth Generation Networks and Communications (5G) - EU toolbox for risk mitigation measures, NIS Cooperation Group, dated. January 2020. The Decision does not include the provisions of the European Toolkit for imposing restrictions and/or exclusions on the basis of political criteria (see strategic measure SM03 and relevant reference to paragraph 2.37 of the EU-coordinated risk assessment where various risk factors are identified to assess the risk profile of suppliers),

(k) the Communication from the Commission dated 29 January 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Secure deployment of 5G networks in the EU - Implementing the EU toolbox, and

(l) the 5G Threat Scope of the European Union Agency for Cybersecurity (ENISA), November 2019.

PART I

Introductory Provisions

Short title.

1.This Decision may be cited as the Security of Networks and Information Systems (Fifth Generation Networks and Communications 5G) Decision , 2020.

Interpretation.

2. (1) In this Decision, unless the context otherwise requires;

P.I. 218/2019.

"Incident Notification Decision of 2019" means the Security of Networks and Information Systems (Notification of Incidents) Decision, 2019 and includes any decision amending or substituted for the same;

P.I..389/2020.

"Security Measures Decision of 2020" means the Security of Networks and Information Systems (Security Measures of Operators of Essential Services and Operators of Critical Information Infrastructure) Decision,2020 and includes any decision amending or substituted for the same;

"core 5G network assets" means critical and sensitive 5G network assets and includes at least core network functions, network orchestration and management functions and 5G access network functions responsible for resource allocation, access management, communications as well as Security of Networks (integrity, confidentiality, authenticity and availability) as set out in Annex III;

Annex III.

P.I. 253/2011.

"Security of Networks Order" means the Security of Networks and Information Order of 2011 and includes any decision amending or substituted for the same;

"5G network" means a fifth generation (5^{th} Generation) mobile communications network;

"guidelines" means the Decisions issued by the Authority pursuant to section 46 of the Law and which aim to clarify and regulate the procedures, methods and timelines of this Decision;

89(I)/2020.

"Law" means the Network and Information Systems Security Law, 2020 and includes any law amending or substituted for the same;

"Directive (EU) 2016/1148" means Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union;

"Directive (EU) 2018/1972" means Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code;

"Managed Service Providers" means service providers entrusted with monitoring networks, managing security incidents, managing resources and changes, as well as user accounts and services. These services are provided under service agreements between the electronic communications providers and the providers of managed services;

"electronic communications providers" or "providers" means providers of electronic communications networks and providers of electronic communications services;

"supplier" means the manufacturer of telecommunications equipment and includes third party suppliers such as cloud service providers and security and maintenance subcontractors.

"affiliated companies" means any two or more companies of a group of companies.

"group of companies" means a group of companies which consists of the parent and subsidiary or subsidiaries.

(2) Terms used in this Decision and not otherwise defined shall have the meaning assigned to them by the Law or Directive (EU) 2016/1148 or Directive (EU) 2018/1972.

Purpose.

3. (1) The purpose of this Decision is to introduce minimum security requirements capable of mitigating the main risks related to the security of Fifth Generation (5G) Electronic Communications Networks and Services.

(2) Without prejudice to the measures set out in the Security Measures Decision of 2020 (P.I. 389/2020) and the Order of 2011 (P.I. 253/2011) with regard to fifth generation (5G) electronic communications networks and services, this Decision sets out additional specific measures.

PART II

Powers of the Authority and Obligations of Providers

Powers of the Authority.

4. (1) For the purposes of this Decision, the Authority shall exercise the powers conferred on it by sections 17(r), 17(s), 17(v), 17(w), 17(ee), 20(1)(c) and (4), 40, 43 and 46 of the Law, the Security of Networks Order, the Incident Notification Decision of 2019 and the Security Measures Decision of 2020.

(2) Without prejudice to the provisions of sub-paragraph (1) above and subject to the provisions of subsection (3) of section 15 and section 18 of the Law and the general policy framework in relation to digital security that is issued by the Deputy Minister under section 16 of the Law, the Authority may:

(a) require electronic communications providers to provide technical, financial and other information and documents regarding the security and operation of fifth generation 5G networks and communications;

Provision of information to the Authority.

(b) impose restrictions, prohibitions, enhanced security provisions and specific requirements on electronic communications providers with respect to their suppliers, including high-risk suppliers and providers of managed services, in accordance with the provisions of Part VI of this Decision;

(c) carry out investigations and audits on electronic communications providers to ensure that they maintain the necessary security controls in the supply chain of mobile communications networks;

(d) impose additional measures as well as to carry out checks on the information security policies and basic and specific measures for the security of mobile communications networks implemented by electronic communications providers;

(e) impose administrative fines on electronic communications providers for violation of the provisions of this Decision, in accordance with the provisions of the Law;

(f) oblige providers of electronic communications, subject to the provisions of sections 2(2), 2(3), 17 and 19 of the Law and if the Authority deems appropriate at the request of the Police, to make information available to the Police, for the purposes of the Public Order and the National Security of the Republic.

(3) For the purpose of implementing this Decision, the Authority may require electronic communications providers to:

(a) notify to the Authority for review in writing the information security policy and the basic security measures in compliance with the guidelines issued by the Authority;

(b) provide written documentation and transmit information and documents to the Authority in electronic form in order to assess the security of their networks and services and regarding the security measures taken and documented by them in accordance with subparagraph (a) as well as their information security policy;

(c) apply all the obligations relating to the provision of information set out in detail in paragraphs 10 and 12 of this Decision;

(d) provide the required information regarding the supply measures, the policy of outsourcing and using third-line providers of managed services and support as well as the multi-supplier strategy as set out in detail in article 13 of this Decision, and

(e) submit documents and information regarding the notification of incidents and the assessment of the security of their networks and information systems, following a reasoned request by the Authority.

PART III

Basic Measures for the Digital Security of Networks and Information Systems

Adherence to basic digital security measures and information security policy.

5. (1) In order to ensure an appropriate level of security of mobile communications networks and for the purpose of avoiding incidents of security breach, electronic communications providers shall design, adopt and substantiate basic security measures and an information security policy. The basic security measures and the information security policy must be in line with the Orders and Decisions issued and/or applied under the Law and must cover the areas described in articles 5 to 22 of the Security Measures Decision, 2020 and articles 5 to 19 inclusive of the Security of Networks Order.

(2) Electronic communications providers shall, as a minimum:

(a) notify the information security policy and key security measures in writing to the Authority for review in compliance with the guidelines issued by the Authority;

(b) provide written documentation and transmit information and documents to the Authority in electronic form in order to assess the security of their networks and services and on the security measures taken and substantiated by them in accordance with subparagraph 1 as well as their information security policy;

(c) record and explain to the Authority the manner of implementation of the basic technical security measures they maintain for their network;

(d) implement the minimum requirements and obligations related to the security of networks and information systems, in accordance with the

provisions of the Security of Networks Order and the Security Measures Decision,2020;

(e) maintain an up-to-date record of the general security policy, of the incident management policies and of the applicable procedures for core network and information systems.

PART IV

Special Security Measures for 5G Networks

Adherence to security measures through compliance with safety standards.

Annex I.

6. (1) In order to ensure an adequate level of security for 5G networks, electronic communications providers shall comply with the standards set out in Part A of Annex I and shall take into account the other documents set out in Annex I, as well as submit a declaration of compliance with the standards to the Authority, for the first time and in relation to the current situation, no later than 30 June 2021 and periodically thereafter at intervals not exceeding two years or as determined from time to time by the Authority.

(2) Electronic communications providers must submit the declaration of compliance with the standards set out in Annex I following a self-assessment of the network design and architecture that is followed for the 5G infrastructure.

Ensuring strict access controls to the 5G network.

7.(1) Providers of electronic communications must implement strict technical security measures relating to the restriction of access to 5G networks. The technical security measures related to the restriction of access to 5G networks must ensure at least the following:

(a) the application of the principle of minimum privilege, which ensures that various rights on the network are minimised, including access rights between network functions, rights of network administrators and virtualisation configuration;

(b) the implementation of the separation of functions;

(c) the implementation of procedures to ensure that such access control measures are continuously implemented and evolving in parallel with the deployment of the 5G network, and

(d) the control of accesses and privileges for all users and roles in all applications and locations of the internal network of providers at regular intervals at least once a year in order to ensure the authorized access to applications, systems and information.

(2) When determining access control measures, particular care should be taken by electronic communications providers in order to ensure that remote access by third parties, including suppliers and in particular suppliers considered to be high-risk, is minimised and/or avoided whenever possible. Where remote access is necessary, for instance in order to deal with service interruptions, the provider should implement appropriate procedures of authentication, authorisation, logging and control in order to have a clear overview of access to the data and configuration changes or modifications of the network.

(3) Access to providers' 5G networks should be limited to specialised personnel who has undergone a security screening, in accordance with the provisions of the Security Measures Decision, 2020 on the security of human resources. Technical security measures apply to all accesses, including privileged access, and should cover all systems within the provider, including network operations and virtualisation configuration.

Ensuring the security of the management of operation and the monitoring of the 5G network and the enhancement of integrity.

8. (1) Electronic communications providers must comply with at least the following additional requirements:

(a) operation of the Network Operation Centre (NOC) and the Security Operations Centre (SOC) at the premises of the provider or that of an associated company, under the control of the provider or of the group of companies in which the provider forms part, and within the Republic or the European Union;

(b) effective monitoring of all critical network elements and sensitive parts of 5G networks by the NOC/SOC in order to detect anomalies/irregularities and detect and prevent threats;

(c) conducting tests and security tests at security operations centres in order to ensure the necessary coverage for the monitoring of resources as well as to record the ability to detect threats at the time;

(d) protection of the management of networks or communication services with a view to preventing unauthorised changes to network elements or services;

(e) physical protection of critical network elements and sensitive parts of 5G networks with a risk-based approach for base stations and other network access points, including multi-access edge computing;

(f) use of appropriate tools and procedures in order to ensure the integrity of software updates and reliable identification, traceability and change management and the status of update of the code and application of security fixes;

(g) implementation of best practices with regards to security for the virtualisation of network operations in accordance with the standards referred to in Annex I (D and F);

Annex I.

(h) implementation of security measures and practices contained in existing legislation, in relation to the areas referred to in article 5, in cloud computing networks and virtualisation systems/networks, and

(i) audits and revisions regarding the configuration reviews of cloud systems and infrastructure at regular intervals (at least once a quarter) as well as following any significant change that may affect the architecture of systems, networks or data.

(2) Subject to the provisions of subsection (3) of section 15 and section 18 of the Law and the general policy framework in relation to digital security which is issued by the Deputy Minister under section 16 of the Law, the Authority has the right by reasoned decision to impose restrictions,

including possible exclusions or enhanced security provisions as well as to carry out audits and consultations with electronic communications providers regarding the adoption and application of the security measures referred to in this Part.

(3) Where the 5G operation is adopted in a non-standalone device as referred to in section 11(3)(c), every possible measure should be implemented, at least as set out in Parts III and IV of this Decision, in order to ensure an adequate level of security for the 5G network.

Standards.

9. Any reference to standards in this Decision and its Annexes includes any standard amending or substituted for the time being:

Provided that in the cases referred to in this article, the declaration of conformity referred to in article 6(1) shall be made in the subsequent periodic declaration to be submitted to the Authority.

PART V

Business Continuity and Emergency Response

Measures to ensure the operation of the network and business continuity and emergency response policy.

10.(1) In order to ensure an appropriate level of security and for the purpose of ensuring integrity and business continuity, electronic communications providers shall design, adopt and document key measures in order to ensure the operation of the network and a business continuity and contingency policy. The basic measures for ensuring the safe operation of the network and the business continuity and contingency policy should be drawn up, approved and implemented by the provider in accordance with the provisions of the Law, Orders and Decisions issued and/or implemented under the Law and shall cover at least the areas described in articles 5 to 22 of the Security Measures Decision of 2020 and articles 5 to 19 inclusive of the Security of Networks Order.

(2) Providers of electronic communications must at least:

(a) notify to the Authority for audit purposes, the basic measures for ensuring network operation as well as the business continuity and contingency policy, taking into account the guidelines that may be issued by the Authority;

(b) provide written documentation and transmit information and documents to the Authority in electronic form on the security measures taken and documented by them in accordance with subsection (1) as well as the business continuity and contingency policy;

(c) keep a record of communications with the Authority which will be available for inspection and copies of which can be obtained by the Authority;

(d) comply with the notification obligations and other obligations provided by the Law and the Notification of Security Breaches or Loss of Network Integrity and/or Services Order of 2013, including any Decision amending or substituted for the same , and

(e) check and review the scope of business continuity plans in order to ensure that all necessary resources and in particular those related to 5G networks, as well as the appropriate measures for each one of the resources, are included.

(3) Subject to the provisions of subsection (3) of section 15 and section 18 of the Law and the general policy framework in relation to digital security issued by the Deputy Minister under section 16 of the Law, the Authority has the right to impose restrictions by reasoned decision, including possible exclusions or enhanced security provisions, as well as to carry out audits and consultations with electronic communications providers regarding the adoption and implementation of the security measures referred to in this Part.

PART VI

Supplier Management

Key security of supply measures and policy on the procurement of equipment and the participation of suppliers.

11. (1) In order to ensure an appropriate level of security of supply, electronic communications providers must:

(a) design, adopt and document basic and specific security of supply measures and a policy for the procurement of equipment and the participation of suppliers. Basic and specific measures for the security of supply and the policy for the procurement of equipment and the participation of suppliers must be in accordance with the Law, the Orders, the Decisions and this Decision,

(b) design and adopt a policy for the assignment and use of managed service providers and third line support, which sets limits on the types of activity and conditions under which electronic communications providers may outsource specific functions to managed service providers, both for the physical and virtual infrastructure of mobile networks; and

(c) design, adopt and document a multi-vendor strategy in order to avoid or reduce any significant reliance on a single supplier (or suppliers with a high risk profile). The multi-vendor strategy will take into account technical limitations and interoperability requirements between the different parts of a 5G network.

(2) In designing, adopting and documenting the measures for the security of supply, the outsourcing policy and the use of managed service providers and third line support and the multi-vendor strategy referred to in paragraph (1) of this article, electronic communications providers shall take into account the outcome of the risk assessment in accordance with the provisions of article 12 and justify their decisions in accordance with the provisions of article 13, taking into account any restrictions imposed by the Authority on sensitive elements of the infrastructure and/or geographical restrictions at points of increased security importance as set out in article14 and Annex III.

Annex III.

(3) The multi-vendor strategy referred to in sections 11(1)(c) and 13(1)(c) must be submitted by the providers to the Authority within four (4) months

from the date that they are authorised to use 5G radio spectrum. Exceptionally, in specific cases, after a reasoned request from the provider, the Authority may accept an extension of four (4) months.

The multi-vendor strategy shall be valid for five (5) years from the date of its submission to the Authority. Exceptionally, in specific cases and for reasons that could not have been foreseen in advance, upon the reasoned request of the provider, the Authority may accept a period of validity of the strategy beyond five (5) years.

The multi-vendor strategy must include at least the following:

(a) a description of the overall strategy, the expected benefits of its implementation, the risks identified and the measures and actions to mitigate them;

(b) a description of the provider's approach to the deployment of the 5G access radio network (RAN);

(c) a description of the provider's approach to the operation of 5G in a non-standalone configuration, namely with a 5G access radio network and a non-5G core network, and how it will work with the existing core;

(d) a description of the provider's approach to switching to a 5G core (full standalone 5G network);

(e) a detailed description of the provider's choices and how they will be implemented in practice, regarding the use of equipment and software by a combination of suppliers in the individual components of the infrastructure, as set out in Annex III;

Annex III.

(f) a description of the necessary changes or replacements that will need to be made to existing equipment and network elements in order to comply with the relevant restrictions that may be imposed on high-risk suppliers pursuant to section 15(3).

Supplier risk assessment.

12. (1) Electronic communications providers must:

Annex II.

(a) carry out, on the basis of strict criteria established by guidelines issued by the Authority described in Annex II and by tools (questionnaires) to be

provided by the Authority, risk assessments of the suppliers with which they intend to cooperate and must communicate to the Authority the outcome of the assessment of the risk profile of suppliers, before concluding new or amending contracts with suppliers, in order for the Authority to examine the outcome, in accordance with the provisions of article15, and to identify high-risk suppliers by taking into account information from competent state bodies;

(b) maintain and provide the Authority with a list of suppliers providing the equipment for 5G networks and/or providing services related to 5G networks;

(c) implement adequate controls and procedures and communicate to the Authority security measures for managing residual risks, such as regular supply chain audits and risk assessments, robust risk management and specific requirements for suppliers based on their risk profile.

Documentation of actions of an electronic communications provider. Security of supply measures.

13. (1) In order to document the actions and decisions that providers take in accordance with the provisions of section 11, providers must:

(a) as regards security of supply measures:

(i) notify the Authority for review, the basic security of supply measures and the policy for the procurement of equipment and the participation of suppliers in compliance with the guidelines;

Assignment and use of managed service providers and third-line support.

(ii) notify the Authority for review, the contracts for the supply of equipment and the participation of suppliers, that providers agree with their suppliers, so that the Authority can have access only to those parts of the contracts that document the security measures, the terms and obligations referred to in article 13(1)(a)(i);

(iii) notify the Authority for review and as additional documentation of the multi-vendor strategy referred to in article 13(1)(c), detailed and up-to-date information concerning their plans for the procurement of 5G network equipment and for the involvement of suppliers, and

(iv) provide written documentation and transmit information and documents to the Authority in electronic form for the assessment of security of supply

as well as on the security measures taken and documented by them in accordance with this section;

(b) with regard to the policy for the assignment and use of managed service providers and third-line support, providers must:

(i) notify the Authority for review, the policy for the assignment and use of managed service providers and third-line support in compliance with the guidelines that may be issued by the Authority;

(ii) notify the Authority for review the contracts for the assignment and use of managed service providers and third-line support in compliance with any guidelines that may be issued by the Authority;

(iii) provide written documentation and transmit information and documents to the Authority in electronic form on the measures for implementing the policy for the assignment and use of managed service providers and third-line support received and documented by them in accordance with this section;

(iv) carry out, on the basis of strict criteria, risk assessments of the managed service providers with which they intend to cooperate, identify high-risk managed service providers and communicate to the Authority the outcome of the assessment of the risk profile of the managed service providers , in compliance with any guidelines that may be issued by the Authority; and

(v) adopt and enforce enhanced security provisions with respect to the access granted to service providers to perform functions;

Multi-vendor strategy and strengthening resilience.

(c) With regard to the multi-supplier strategy, providers must:

(i) notify the multi-supplier strategy for review and approval by the Authority, in compliance with the guidelines set out in section 11(3);

(ii) provide written documentation and transmit information and documents to the Authority in electronic form for the evaluation of the multi-vendor strategy;

(iii) ensure an appropriate balance of suppliers and/or an appropriate safety framework to ensure resilience in the event of an incident with a supplier, by taking into account variations in the geographical characteristics and the population of the Republic, and

(iv) consult on the content of the strategy with the Authority in order to take appropriate technical and organisational measures to ensure that the strategy is acceptable to the Authority, and to enable the Authority to assess the situation at national level.

Sensitive infrastructure elements and geographical restrictions.

14. (1) In order to justify their adequacy in security matters as defined in this Decision, electronic communications providers shall:

(a) take into account any restrictions set by the Authority in relation to the use of equipment by high-risk suppliers;

(b) not to install and operate equipment that is supplied by a high-risk supplier as defined by the assessment referred to in section 15(1):

Annex III.

(i) in sensitive areas of the infrastructure as defined in Annex III, and

(ii) at geographical points designated by the Authority, in the vicinity of specific critical information infrastructure and facilities of increased security importance for the Republic;

unless, following an assessment by the Authority, electronic communications providers can justify adequate digital security measures in order to address the risks identified in the supplier's assessment.

Provided that subject to the provisions of sections 2(2) and 2(3) of the Law, the operation of the equipment by a high-risk supplier does not affect the measures that the Republic may take for the national security of the Republic and the maintenance of law and order in the Republic.

Provided further that the Authority, regardless of its actions under this article, it must comply with and apply the provisions of sections 15 (3) and 16 of the Law.

(c) provide the Authority for review with a list of functionalities and manufacturers of security-related network elements used to operate the 5G network, as set out in Annex III, and, where applicable, other components used by them, every six months, starting from 30 June 2021 and whenever required upon a reasoned request from the Authority.

Annex III.

Competences of Authority.

15. (1) Subject to the provisions of subsection (3) of section 15 and section 18 of the Law and the general policy framework in relation to digital security that is issued by the Deputy Minister under section 16 of the Law, the Authority shall carry out a risk assessment for suppliers and determine the high-risk suppliers. The Authority shall complete the risk assessment for suppliers within two months of receipt of all relevant information from the providers and the Competent Authorities of the Republic, by taking into account the respective assessments of providers which are carried out in accordance with the provisions of article 12, the assessments of the Competent Authorities of the Republic and any guidelines issued by the competent bodies of the European Union.

(2) Subject to the provisions of subsection (3) of section 15 and section 18 of the Law and the general policy framework in relation to digital security that is issued by the Deputy Minister under section 16 of the Law, the Authority shall assess, check and approve the documents submitted by the providers in accordance with the provisions of Part VI of this Decision.

(3) Subject to the provisions of Part VI of this Decision, the multi-supplier strategy submitted by providers in accordance with article 13(1)(c) shall be evaluated by the Authority within two months of the submission of a fully completed strategy and may be accepted by the Authority on the basis of

adequate justification and an appropriate safety framework for addressing the risks arising from the assessment referred to in article 12.

Restrictions on high-risk suppliers for core 5G network assets, on the avoidance of significant reliance on a single supplier, and on the outsourcing of activities.

(4) Subject to the provisions of subsection (3) of section 15 and section 18 of the Law, the general policy framework in relation to digital security issued by the Deputy Minister under section 16 of the Law and by taking into account the documents submitted by the providers in accordance with sections 12 and 13, the restrictions set by the Authority pursuant to article 14 and the assessment of the risk profile of suppliers referred to in paragraph one (1) of this article, the Authority may approve, amend or reject the recommendations made by the providers and/or impose additional restrictions, by reasoned decision at any point in time, including exclusions, or enhanced security provisions to mitigate the existence of risk:

(a) in the procurement of equipment and the participation of high-risk suppliers in core 5G network assets;

(b) on the assignment of specific functions in sensitive parts of 5G networks to providers of managed services, and

(c) in order to avoid or reduce any significant reliance on a single supplier.

(5) The Authority ,shall, in taking its decisions, pursuant to the provisions of Part VI of this Decision, take into account, information from competent authorities of the Republic in relation to:

(a) state aid, grants or other incentives to providers and suppliers;

173(I)of 2011
73(I)of2016.

(b) public procurement procedures;

(c) the protection of competition;

(d) the interests of consumers and any impact on the buying or selling prices or other trading conditions of the electronic communications services provided.

PART VII

Notification of Incidents, Obtaining Information and Audits

Incident notification procedure and content.

16. Subject to the provisions of sections 35, 37 and 40 of the Law, the provisions of the Decision ,2019 shall apply to the procedure and content of a notification that electronic communications providers must submit for any incident which has a serious impact on the services they provide.

Conduct of audits and investigations by the Authority on electronic communications providers.

17. (1) Subject to the provisions of the Law, the Authority may:

(a) by reasoned request require electronic communications providers to submit documents and information regarding the notification of incidents and the assessment of the security of their networks and information systems;

(b) check and investigate ex officio the activities, the functions and the proper performance of the obligations of providers arising from this Decision and the relevant annexes.

(2) For exercising the powers, audits and investigations provided by paragraph (1) above, the Authority shall exercise the powers afforded to it and shall comply with the procedures provided by sections 15, 16, 17, 18, 19, 20, 23, 36, 38 and 40 of the Law.

(3) Where the audit or investigation referred to in paragraph (1) which is carried out by the Authority requires a contract for the provision of services by technical advisers or other persons, the Authority shall take reasonable steps to ensure their independence and to maintain their confidentiality and impartiality.

PART VIII

Compliance – sanctions

Administrative fine.

18. Subject to the provisions of sections 43 and 54 of the Law and without prejudice to the other penalties provided therein, the Authority may impose an administrative fine not exceeding two hundred thousand euros (€ 200,000) in case it ascertains that a provider or other person does an act or makes an omission in contravention of the provisions of this Decision.

Criminal offenses.

19. Sections 22, 44 and 54 of the Law shall be applied to the sanctions and liability of a legal person in case of the commission of a criminal offence for the contravention of the provisions of this Decision.

PART IX

Final Provisions

Date of commencement.

20. This Decision shall come into effect on the date of its publication in the Official Gazette of the Republic.

Amendments.

21. Subject to the provisions of the Law, the Authority may, by decision amend, replace or repeal this Decision or its Annexes.

ANNEX I

STANDARDS AND GUIDELINES

A. 3GPP standards:

• 3GPP TS 33.116 V15.0.0 (2018-06), Security Assurance Specification (SCAS) for the MME network product class

• 3GPP TS 33.117 V16.3.0 (2019-12), Catalogue of general security assurance requirements

• 3GPP TS 33.216 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

• 3GPP TS 33.250 V15.1.0 (2019-09), Security assurance specification for the PGW network product class

• 3GPP TS 33.401 V16.1.0 (2019-12), 3GPP System Architecture Evolution (SAE); Security architecture

• 3GPP TS 33.402 V15.1.0 (2018-06), 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses

• 3GPP TS 33.501 V16.1.0 (2019-12), Security architecture and procedures for 5G System

• 3GPP TS 33.511 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

• 3GPP TS 33.512 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF)

• 3GPP TS 33.513 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

• 3GPP TS 33.514 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

• 3GPP TS 33.515 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

• 3GPP TS 33.516 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

• 3GPP TS 33.517 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

• 3GPP TS 33.518 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

• 3GPP TS 33.519 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

B. ETSI standards:

• ETSI GS NFV-SEC001 V1.1.1 (2014-10), Network Functions Virtualisation (NFV); NFV Security; Problem Statement

• ETSI GS NFV-SEC 002 V1.1.1 (2015-08), Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software

• ETSI GS NFV-SEC 003 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance

• ETSI GS NFV-SEC 004 V1.1.1 (2015-09), Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications

• ETSI GS NFV-SEC 006 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns

• ETSI GS NFV-SEC009 V1.1.1 (2015-12), Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration

• ETSI GS NFV-SEC 010 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements

• ETSI GS NFV-SEC 012 V3.1.1 (2017-01), Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components

• ETSI GS NFV-SEC 013 V3.1.1 (2017-02), Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification

• ETSI GS NFV-SEC 014 V3.1.1 (2018-04), Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points

• ETSI GS NFV-SEC 021 V2.6.1 (2019-06), Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification

• ETSI GS NFV-SEC 022 V2.7.1 (2020-01), Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access

• ETSI TS 103 487 Baseline security requirements regarding sensitive functions for NFV and related platforms

• ETSI TR 103 308 Security baseline regarding LI and RD for NFV and related platforms

• ETSI TS 103 307 Security Aspects for LI and RD Interfaces

C. GSMA documents:

• GSMA FF.02 Fraud Management Systems - Guidelines for Mobile Operators

• GSMA FF.15 Advice on Internal Fraud Risks

• GSMA FF.19 NRTRDE Commercial Implementation Handbook

• GSMA FF.21 Fraud Manual

• GSMA FS.01 Use of SIM Boxes to bypass interconnect communications

• GSMA FS.07 SS7 and SIGTRAN Security of Networks

• GSMA FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines

• GSMA FS.13-16 NESAS

• GSMA FS.19 Diameter Interconnect Security

• GSMA FS.20 GTP Security

• GSMA FS.21 Interconnect Signalling Security Recommendations

• GSMA FS.22 VoLTE Security Analysis and Recommendations

• GSMA FS.24 CAMEL Roaming Fraud Management Handbook

• GSMA FS.26 Guidelines for Independent Remote Interconnect Security Testing

• GSMA FS.30 Security Manual

• GSMA FS.31 Baseline Security Controls

• GSMA FS.33 NFV Threats Analysis

• GSMA FS.34 Key Management for 4G and 5G inter-PLMN security

• GSMA FS.35 Security Algorithm Implementation Roadmap

• GSMA FS.36 5G Interconnect Security

• GSMA FS.37 GTP-U Security

• GSMA FS.38 SIP Security of Networks

• GSMA FS.40 5G Security

• GSMA IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers

• GSMA IR.88 LTE and EPC roaming guidelines (5G NSA uses LTE roaming)

• GSMA SGP.21 - RSP Architecture

• GSMA SGP.22 - Technical Specification

• GSMA TS.26 - NFC Handset Requirements

• GMSA TS.27 - NFC Handset Test Book

• GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile

• GSMA SGP.05 - Embedded UICC Protection Profile (for m2m-devices)

• BSI-CC-PP-0104-2019 - CC-PP Cryptographic Service Provider

• GSMA FS.27 Security Guidelines for UICC profiles

• GSMA FS.28 Security Guidelines for UICC credential protection

D. ENISA documents:

• ENISA Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services, Version 1.0, December 2016.

• Technical Guideline on Security Measures in section 13a, Version 2.0 October 2014.

• ENISA Security aspects of virtualization, February 2017

E. Certification Schemes

• ISO/IEC 27001

• ISO/IEC 22301

• NESAS (Network Equipment Security Assurance Scheme) under governance by EU-COM (CSA)

• SOGIS Common Criteria

F: NIST Guidelines

• SP 800-125 - Guide to Security for Full Virtualization Technologies

• SP 800-125A Rev. 1 - Security Recommendations for Server-based Hypervisor Platforms

• SP 800-125B - Secure Virtual Network Configuration for Virtual Machine (VM) Protection

ANNEX II

SUPPLIER RISK ASSESSMENT CRITERIA

Supplier Risk Assessment Criteria

Electronic communications providers shall carry out a risk assessment for suppliers in addition to integrating security requirements into the procurement process which relate to the components of the 5G network. Further tools in the form of questionnaires will be provided by the DSA in order to facilitate the assessment. The material will be provided in English due to the technical terms.

The procedure for the conclusion of contracts for components or services related to the 5G network must comply with the recommendations set out in the ENISA document 'Indispensable baseline security requirements for the procurement of secure ICT products and services' which is in line with the EU requirement for compliance with specific security standards in the procurement process for ICT components and services.

A. Product development lifecycle

The risk assessment shall take into account the life cycle of the parts/services provided by the supplier in the development of the product. In detail, the following are evaluated:

- The quality and transparency of the technical practices of the supplier and cybersecurity audits
- Quality control is performed to find accidental or intentional security vulnerability in the components provided by the supplier and in the software. This shall include at least:
  - Security/quality gateways for the development of software and hardware
  - Threat modelling built into the design phase
  - Secure Development of Software
  - Training on the Lifecycle for all employees involved
  - Static & Dynamic Analysis of the Security of the Code during development

- Automated testing for the production code during development
- Security testing, including penetration testing for products/software before development

- Measures taken to ensure safety by design and pre-selection with clear safety requirements.
- Management of dependency in order to ensure interoperability, including third-party libraries or components.
- Maintenance of an account of materials for third-party libraries and including those assets in the supplier's vulnerability management program.

B. Governance/Risk Management

Suppliers must be able to demonstrate the alignment of their security practices with the provider's security objectives. The risk assessment should therefore take into account:

- Compliance with international standards & Regulations such as ISO27001, ISO22301, ISO9001, PCI-DSS & GPDR as appropriate.
- The supplier's information security program, including risk management which is in place.
- The supplier should have an information security policy that ensures the security and resilience of its products and services and is in line with the provider's high-level security objectives.
- The supplier should be able to comply with the legal requirements of the provider which are imposed by law.
- The supplier must be able to comply with the Law as well as with the Decisions and Regulations issued thereunder.

C. Business Continuity & Resilience

The supplier has available a BPP/DRP in order to ensure the continuity of its services in addition to KPIs for monitoring performance. The risk assessment should include at least:

- The ability to provide spare parts for the network and to maintain SLAs.
- The business continuity plans which ensure continuous operation and the provision of services / support.
- The resilience of the supplier both from a technical point of view and in terms of the continuity of the service offer provided to electronic communications providers of Cyprus.

D. Interoperability

Ensuring the resilience of 5G networks is a major priority for Cyprus. Therefore, the risk profile of the supplier also depends on the following interoperability factors:

- Products or services acquired by the supplier must follow important standards such as 3GPP .
- The products or services acquired by the supplier must meet the interoperability requirements of the electronic communications provider concerned, allowing for the implementation of a multi-vendor strategy.
- Products or services acquired by the supplier shall ensure business continuity in multi-vendor environments in cases where vulnerable/problematic components need to be removed/replaced from the 5G network.

E. Data security/privacy

The supplier should comply with any legal or regulatory requirements regarding data privacy laws, such as the GDPR, as applicable. Therefore, the risk assessment shall include at least the following:

- Data location and whether data is stored outside the EU.
- The supplier has an adequate data privacy policy.
- Whether the supplier will have access to confidential or private data related to end-user data within the mobile network, or business data, such as network configurations and privileged access credentials.

- Whether the supplier will have access to a large volume of records.
- Data classification policy in conjunction with the handling and marking of all media.

F. Human Resources Security

As part of the procurement process, electronic communications providers shall assess the information security procedures applied to the suppliers' human resources. At least the following should be ensured:

- The supplier carries out a check on all employees before employment, except for periodic displays to identify anyone who could tamper with the equipment (as part of hacking, organized crime, government pressure, or espionage).
- The supplier provides adequate training to employees on cybersecurity.
- The supplier must incorporate a relevant non-disclosure clause in all employee contracts.
- The supplier includes a thorough exit process to end the employment of employees.

G. Internal Security Reviews

Suppliers are required to implement internal security procedures to ensure the security of their customers' products, services, and data. Therefore, the following reviews shall be included in the risk assessment:

- The supplier shall implement a vulnerability management plan that includes:
  - Patching management for all internal systems and components.
  - Vulnerability assessments across systems.
- The supplier shall have monitoring and tracing mechanisms in place to ensure that security threats or incidents are detected.
- The supplier has an incident management policy, with the relevant procedures to be followed and manuals, which allows immediate response to security incidents.
- The supplier performs network splitting/partitioning.

- Suppliers shall implement access control mechanisms and procedures, including access management to system administrators, to ensure that the principle of minimum privileges and the need-to-know principle are respected.
- The supplier has physical security and information measures in place to protect unauthorized access to its intellectual property and procedures.
- The supplier shall have backup policies in place, and the data shall establish processes that are documented and clearly linked to roles and responsibilities. Backups are encrypted and stored securely.
- The supplier shall carry out regular security testing, including penetration tests in its network infrastructure and applications for existing and new systems.

H. Strategic Factors

- The likelihood of the supplier having access to confidential or private data. Percentage and types of services assigned/provided to suppliers by third parties.
- Whether suppliers follow security best practices in managing third parties (their own suppliers). Ensure that the services provided to suppliers do not include third parties who have access to data or parts of the providers' network/infrastructure.
- Suppliers perform testing/verification/checking on code developed by third parties.
- The criticality of the component in the 5G network that the supplier must provide.

ANNEX III

LIST OF BASIC NETWORK ASSETS 5G

- Access and Mobility management Function (AMF)
- Authentication Server Function (AUSF)
- Network Exposure Function (NEF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- Policy Control Function (PCF)
- Security Edge Protection Proxy (SEPP)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- User Plane Function (UPF)
- New Radio Base Station (gNodeB) [At sensitive points such as base stations operating with multi-access edge computing or in geographically sensitive areas as defined in accordance with section 14 (1) (b) (ii)].