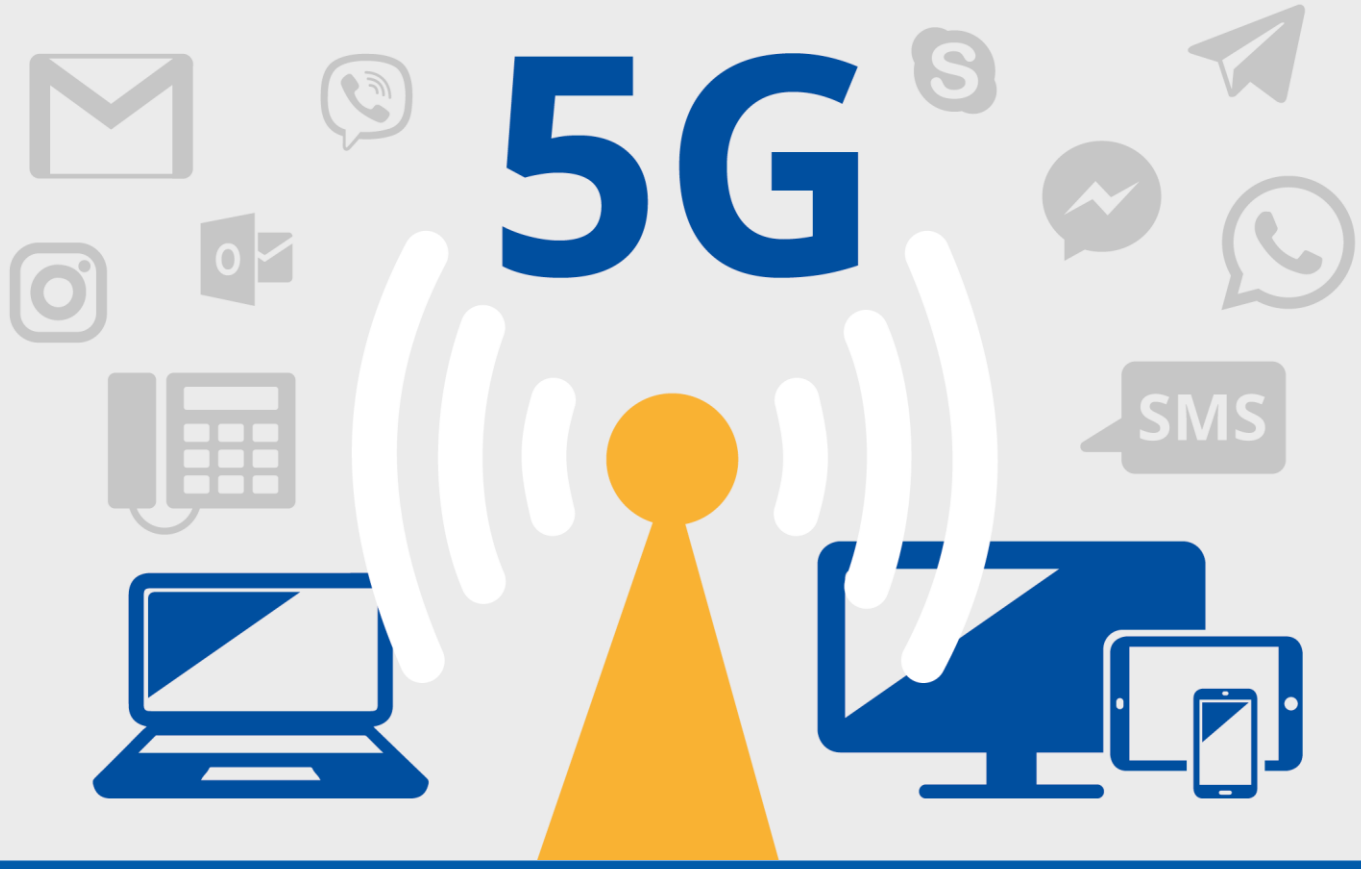
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



5G SUPPLEMENT

To the Guideline on Security Measures
under the EECC

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Goran Milenkovic and Dr. Marnix Dekker, European Union Agency for Cybersecurity

ACKNOWLEDGEMENTS

We are grateful for the review and valuable input received from the experts in the ECASEC Expert Group (formerly known as Article 13a Expert Group), which comprises national telecom regulatory authorities (NRAs) from all EU and EFTA countries, and from the experts from national authorities in the NIS Cooperation group, and particularly those experts contributing to the NIS CG work stream on 5G cybersecurity. In the preparation of the report we have conducted an analysis of publically available information on security in 5G specifications in collaboration with Plum Consulting, under the tender ENISA S-COD-20-T14.

LEGAL NOTICE

COPYRIGHT NOTICE

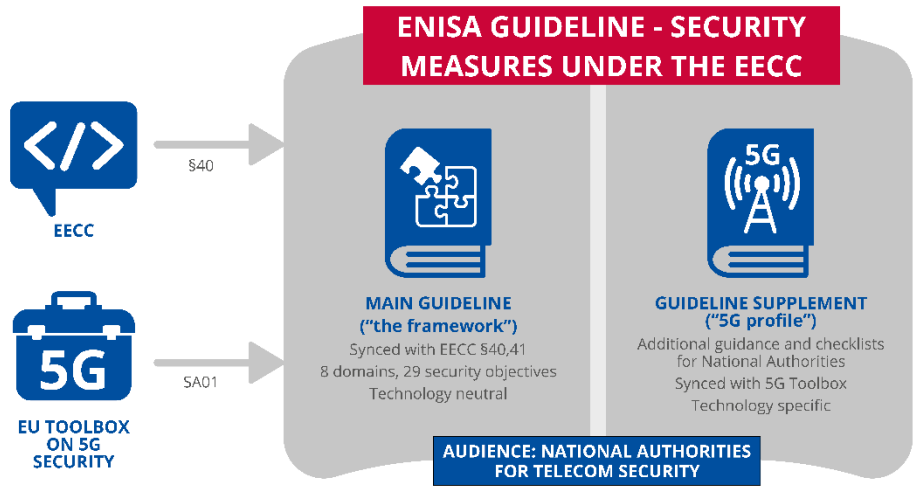
ISBN: 978-92-9204-456-5 - DOI: 10.2824/098554

TABLE OF CONTENTS

1. INTRODUCTION

This document contains a 5G technology profile which supplements the **Guideline on Security Measures under the EECC**[1], called **the Guideline** hereinafter. The 5G technology profile gives additional guidance to competent national authorities about how to ensure the security of 5G networks. This document was developed in close collaboration with experts from national telecom security authorities across the EU, i.e. the ECASEC Expert Group (formerly known as the Article 13a Expert Group), and with the members of the NIS CG work stream for 5G cybersecurity.

Figure 1: Structure of the ENISA Guideline on Security Measures under the EECC



Considering the dynamic nature of 5G technology and the related threat landscape, this document is meant to be updated as technology and risks evolve. ENISA may consider using an alternative electronic format for this supplementary guideline, to better support regular updates.

1.1 OBJECTIVES AND SCOPE

The objective of this document is to provide additional guidance for competent authorities on how to ensure that appropriate security measures are taken by providers of 5G networks and services. This supplement clarifies and refines the more generic security measures in the Guideline on Security Measures under the EECC specifically for 5G technology.

Considering the complexity of 5G technology and the variety of deployment and configuration options, both the risks and the necessary security measures will be very different for different deployments of 5G networks and services. This means that it is important to assess the setup and the security in depth, for each case, for example by performing audits[2] on MNOs.

[1] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc
[2] This scope of this supplement does not include full audit guidelines for 5G networks, but competent authorities may refer to the general guidance for auditing communication service providers given in the section 5.6 of the Guideline.

1.2 POLICY CONTEXT

The Guideline, and this supplement, is a guideline for national authorities with competence on Article 40 of the EECC.

The Guideline, and this supplement, also addresses Supporting action SA01 of the Union toolbox of mitigating measures for 5G. It also gives guidance to EU Member States about the technical security measures under the Toolbox, in particular TM01. References to other technical measures that may be fully or partially implemented through the implementation of the measures in the Guideline and this supplement are provided further in this supplement.

1.3 STRUCTURE OF THIS DOCUMENT

This document is structured as follows:

Section 2 contains the necessary background, i.e. a short introduction to cybersecurity of 5G networks, summarizing the outcomes of the coordinated EU approach for the cybersecurity of 5G networks, listing the critical assets, and key risks identified in the Union-wide risk assessment and summarizing what is in the EU toolbox on 5G cybersecurity.

Section 3 contains the 5G technology profile which provides supplementary guidance to national authorities on what are the appropriate security measures for 5G networks. The profile contains short general guidance and specific guidance for each of the 8 security domains in the Guideline.

Finally, in Section 4 we briefly discuss some specific technological aspects of 5G networks that are of particular interest from the cybersecurity point of view. For each of the key technologies we provide information or references to relevant industry standards and best practices that competent authorities may want to take in consideration.

2. BACKGROUND: 5G RISKS AND MEASURES

2.1 COORDINATED EU APPROACH TO CYBERSECURITY OF 5G

The European Commission's **Recommendation on the cybersecurity of 5G networks** (hereafter **'The Recommendation'**) published on 26 March, 2019, states that the cybersecurity of 5G networks is considered critical, to protect the EU's economy and society and to ensure the technological sovereignty of the Union. The recommendations called on Member States to complete national risk assessments and review national measures, to work together at EU level on a coordinated risk assessment and to prepare a toolbox of possible mitigating measures.

Based on the individual national risk assessments, the Commission and the Member States, with the support of ENISA, developed a single **EU Coordinated Risk Assessment on Cybersecurity in 5G Networks**[3] (hereafter **'Coordinated risk assessment'**). This coordinated risk assessment identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities and the main risks. For ease of reference, we re-iterate the main assets, in section 2.2 and the main risks, in section 2.3.

2.2 TERMINOLOGY AND DEFINITIONS

Terminology and definitions used in this document follows the terminology and definitions in the Coordinated risk assessment, paragraphs 1.12 and 1.24. For ease of reference, we list them here.

Table 2: Definitions

Term	Definition
5G Networks	5G networks means a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network
Mobile Network Operators - MNOs[4]	Entities providing mobile network services[5] to users, operating their own network [or] with the help of third parties[6].
Suppliers of MNOs	Entities providing services or infrastructure to MNOs in order to build and/or operate their networks. This category includes: - Telecom equipment manufacturers; - Other third-party suppliers, such as cloud infrastructure providers, systems integrators, security and maintenance contractors, transmission equipment manufacturer.
Manufacturers of connected devices and related service providers	Entities providing objects or services that will connect to the 5G networks (e.g. smartphones, connected vehicles, e-health) and related service components hosted in 5G control plane as defined in Service Based Architecture or Mobile Edge Computing

[3] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[4] In the context of EECC, MNOs are one type of providers of public electronic communications networks or of publicly available electronic communications services
[5] In this document mobile network services refer to 5G networks and hence the corresponding term MNOs is used to denote entities providing 5G mobile network services
[6] The original definition as given in the Coordinated risk assessment reads "entities providing mobile network services to users, operating their own network with the help of third parties". To avoid a possible confusion that MNOs always depend on third parties, an 'or' has been added to slightly amend the said definition.

2.3 5G ASSETS

Where references are made in this document to **critical or sensitive network component or functions**, the identification of these components or functions should be based on and consistent with the **high-level categorisation of asset sensitivity defined in the Coordinated risk assessment,** paragraph 2.21.

For ease of reference, we reproduce the table from the referenced paragraph 2.21 below.

Table 3: Assets (according to the Coordinated risk assessment)

Categories of elements and functions	Criticality	Examples of key elements
Core network functions	**CRITICAL**	User Equipment Authentication, roaming and Session Management Functions; User Equipment data transport functions; Access policy management; Registration and authorization of network services; Storage of end-user and network data; Link with third-party mobile networks; Exposure of core network functions to external applications; Attribution of end-user devices to network slices
NFV management and network orchestration (MANO)	**CRITICAL**	
Management systems and supporting services (other than MANO)	**MODERATE/HIGH**	Security management systems; Billing and other support systems such as network performance
Radio Access network	**HIGH**	Base stations
Transport and transmission functions	**MODERATE/HIGH**	Low-level network equipment (routers, switches, etc.); Filtering equipment (firewalls, IPS...)
Internetwork exchanges	**MODERATE/HIGH**	IP networks external to MNO premises; Network services provided by third parties

Further details about the listed asset categories is available in paragraphs 2.22 - 2.27 of the Coordinated risk assessment.

Remark: *The above list of assets is a generic, high-level list, looking at the overall elements of 5G architecture. When identifying specific assets, MNOs are expected to follow the recommended approach from the Guideline and to perform their own analysis, specific for their particular setting and to determine which specific assets are in scope (see section 4.1 of the Guideline). With transition to 5G network and services, such asset lists are expected to be updated in order consider new assets introduced (as also recommended further in section 3) and should ideally be aligned with the above list of assets, in particular in terms of estimated asset criticality.*

2.4 5G RISKS

Coordinated risk assessment identified several main risk categories illustrated by concrete risk scenarios, describing possible attacks paths that a threat actor can use to reach its target. For ease of reference, we list these risks in the table below, reproducing the text from the Coordinated risk assessment.

Table 4: Risks (according to the Coordinated risk assessment)

Risk group	Individual risks/risk scenarios
I - Risk scenarios related to insufficient security measures	**R1**: Misconfiguration of networks: Exploiting poorly configured systems and architecture, a State actor penetrates into the 5G network via its external interfaces, leading to the compromise of the network core functions, or exploits edge-computing nodes in order to compromise information confidentiality and disrupt distributed services. **R2:** Lack of access controls: A subcontractor with administrator's privileges on the network performs adverse action, leading to confidentiality/integrity and/or availability breach. The subcontractor's action may be due to a legal requirement imposed by a third country or rogue behaviour of the contractor's staff.
II – Risk scenarios related to 5G supply chain	**R3:** Low product quality: Espionage by state or state-backed actors using malware to abuse poor quality network components or unintentional vulnerabilities affecting sensitive elements in the core network, such as Network Virtualisation Functions. **R4:** Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis: A mobile network operator sources a large amount of its sensitive network components or services from a single supplier. The availability of equipment and/or updates from this supplier is subsequently drastically reduced, due to a failure by the supplier to supply (e.g. due to trade sanctions by a third State or to other commercial circumstances). In consequence, the quality of a supplier's equipment decreases due to priority given to guaranteeing supply over improvements in product security.
III - Risk scenarios related to modus operandi of main threat actors	**R5:** State interference through 5G supply chain: A hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities. **R6:** Exploitation of 5G networks by organised crime or Organised crime group targeting end-users: By taking control of a critical part of the 5G network architecture, an organized crime group disrupts various services to ransom businesses relying on those services, or the mobile network operator itself. Alternatively, using a similar attack path, an organised crime group may also target end-users, e.g. by injecting false messages to the users of the network as part of a large-scale "phishing" attack or online scam, or by using the compromised network to gain access to confidential data about users (e.g. second-factor authentication codes) for further profit.
IV - Risk scenarios related to interdependencies between 5G networks and other critical systems	**R7:** Significant disruption of critical infrastructures or services: Malicious hackers are able to compromise emergency services by gaining control of their dedicated network slice, thus compromising the availability of the service and the integrity of the information/data used for/within that service. **R8**: Massive failure of networks due to interruption of electricity supply or other support systems: Massive outage of power supply due to natural disasters or to attacks to the energy grid by a state, a state-backed actor or an organised crime group.
V - Risk scenarios related to end user devices	**R9:** IoT (Internet of Things) exploitation: A hacktivist group or state-backed actor takes control of low security devices like IoT (sensors, home appliances, etc.), in order to attack the network by overwhelming its signalling plane.

Remark: *The above list of risks identified in the Coordinated risk assessment may be seen as a generic, high-level list of risks that are believed to be relevant for MS across EU. In reality, MNOs are expected to follow the recommended approach from the Guideline and to perform their own risk assessment, specific for their particular setting and to determine which specific risks are relevant (see section 4.1 of the Guideline). With transition to 5G network and services, such risk assessment is expected to be updated in order consider specific 5G risks (as also recommended further in section 3) and should ideally be aligned with the above list of risks.*

We refer the reader to the ENISA 5G threat landscape[7] for a more detailed and more technical overview of threats for 5G networks.

[7] For information about the ENISA Threat Landscape for 5G networks, refer to section 4 and Table 15.

2.5 MITIGATING MEASURES IN THE 5G CYBERSECURITY TOOLBOX

On 29 January 2020, the NIS Cooperation Group published the **EU toolbox of risk mitigating measures[8] ('the Toolbox')** addressing the risks identified in the coordinated risk assessment. On the same date, the Commission adopted a **Communication (Secure 5G deployment in the EU - Implementing the EU Toolbox)[9],** in which it endorsed the Toolbox conclusions and underlined the importance of their effective and quick implementation and called on Member States to take concrete steps to implement them.

The Toolbox identifies two groups of measures MS can take: *strategic* and *technical* measures and it also identifies a number of supporting actions that may enable, assist in implementation or improve effectiveness of the strategic and technical measures.

Figure 2: Toolbox structure

We summarize the strategic and technical measures in the Toolbox in the tables below.

Table 5: List of strategic measures from the Toolbox

Strategic Measures	
SM01	Strengthening the role of national authorities
SM02	Performing audits on operators and requiring information
SM03	Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk
SM04	Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support
SM05	Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies
SM06	Strengthening the resilience at national level
SM07	Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU

[8] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
[9] Commission Communication COM (2020)50, Secure 5G deployment in the EU - Implementing the EU toolbox, 29 January 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481

Table 6: List of technical measures from the Toolbox

Technical Measures	
TM01	Ensuring the application of baseline security requirements (secure net. design and architecture)
TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards
TM03	Ensuring strict access controls
TM04	Increasing the security of virtualised network functions
TM05	Ensuring secure 5G network management, operation and monitoring
TM06	Reinforcing physical security
TM07	Reinforcing software integrity, update and patch management
TM08	Raising the security standards in suppliers' processes through robust procurement conditions
TM09	Using EU certification for 5G net. components, customer equipment and/or suppliers' processes
TM10	Using EU certification for other non 5G-specific ICT products and services[10]
TM11	Reinforcing resilience and continuity plans

Table 7: List of supporting actions from the Toolbox

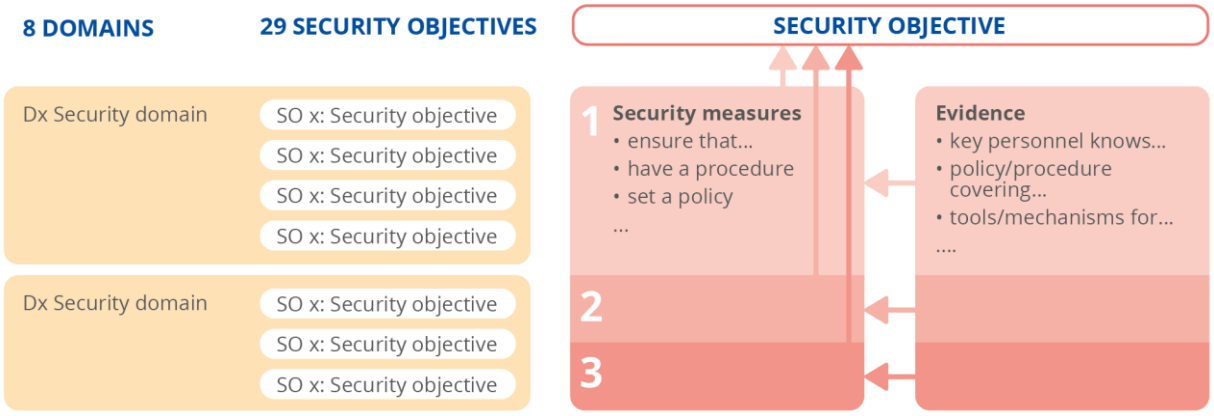
Supporting Actions	
SA01	Reviewing or developing guidelines and best practices on network security
SA02	Reinforcing testing and auditing capabilities at national and EU level
SA03	Supporting and shaping 5G standardisation
SA04	Developing guidance on the implementation of security measures in existing 5G standards
SA05	Ensuring the application of standard technical and organisational security measures through specific EU-wide certification scheme
SA06	Exchanging best practices on the implementation of strategic measures, in particular national frameworks for assessing the risk profile of suppliers
SA07	Improving coordination in incident response and crisis management
SA08	Conducting audits of interdependencies between 5G networks and other critical services
SA09	Enhancing cooperation, coordination and information sharing mechanisms
SA10	Ensuring 5G deployment projects supported with public funding take into account cybersecurity risks

[10] (connected devices, cloud services)

2.6 GUIDELINE ON SECURITY MEASURES UNDER THE EECC

The ENISA Guideline on Security Measures under the EECC[11], referred to as the Guideline, provides guidance to competent authorities about the technical details of implementing Articles 40 and 41 of the EECC. It gives guidance to authorities on how to ensure that providers assess risks and take appropriate security measures. It contains a list of 29 high-level security objectives, grouped in 8 domains. Per security objective it lists detailed security measures which could be taken by providers to reach the security objective. The measures are grouped in 3 levels of increasing sophistication. The overall structure of security objectives and security measures is depicted in the diagram below.

Figure 3: Overall structure of the security objectives and security measures



The Guideline is split in 8 security domains:

- D1: Governance and risk management
- D2: Human resources security
- D3: Security of systems and facilities
- D4: Operations management
- D5: Incident management
- D6: Business continuity management
- D7: Monitoring, auditing and testing
- D8: Threat awareness

The Guideline is technology neutral and the security measures are applicable to different types of networks and services and different types of electronic communication providers.

[11] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

3. 5G TECHNOLOGY PROFILE

This section, the 5G technology profile, supplements the Guideline, which is generic and technology-agnostic, with additional and more specific guidance on 5G by clarifying and refining the security measures for 5G networks and services.

When supervising MNOs offering 5G networks, competent authorities should ask a number of high-level, general questions:

1. Does the MNO already have the general security measures in place, such as the security measures contained in the Guideline on Security Measures under the EECC?
2. Has the MNO updated the risk assessments, asset lists and operational procedures and has it reinforced general security measures accordingly, as required for the 5G network deployment and operation?
3. Is the MNO implementing specific security measures from the relevant 5G standards such as 3GPP[12], including the security-relevant optional controls, and does the same principle also apply to products and equipment that MNO is using in the network?
4. Has the MNO considered the key new technologies of specific relevance for 5G networks (such as virtualization, slicing, edge computing etc.) in the overall risk assessment and has it deployed adequate controls for mitigating related risks?

In the rest of this section we provide detailed guidance for competent authorities for each of the 8 security domains, as follows:

- For each of the domains we first list all the underlying security objectives;
- We then highlight those objectives that may be considered of particular importance for 5G networks and services and we provide a brief rationale for their relevance;
- For each of these highlighted objectives we also include a checklist containing additional elements that competent authorities may consider;
- Finally, we include reference to directly related technical measures from the Toolbox[13].

Remark: *Taking into account the type of service provided and perceived overall level of risk, competent authorities may want to consider requesting the implementation of measure up to level 3, in particular for those security objectives identified (in the step #2 above) to be of particular importance. However, it is ultimately up to the competent authorities to choose the appropriate sophistication levels, taking in consideration also the guidance provided in section 4.2 of the Guideline (Remark on minimum security measures).*

[12] When assessing the implementation of security controls from the 3GPP standards, competent authorities may find useful to refer to the reference list provided in Annex II of this supplement.
[13] In addition, Annex III of this supplement includes a mapping table between the (supplemented) Guideline security domains and related technical measures form the Toolbox that are being addressed through the implementation of related measures and supplementary guidance

3.1 DOMAIN D1: GOVERNANCE AND RISK MANAGEMENT

Domain D1 (Governance and risk management) covers the following security objectives:

- SO 1: Information security policy
- SO 2: Governance and risk management
- SO 3: Security roles and responsibilities
- SO 4: Security of third party assets

This security domain is important to ensure that MNOs have appropriate measures and processes in place to manage information security risks continuously and adequately. It is of particular importance to ensure that the list of risks is reviewed and updated to consider key risks specific to 5G networks, especially those identified in the Coordinated risk assessment and that adequate technical measures are in place for mitigating supply-chain risks pertaining to 5G networks. Depending on the national approach in respect of assessment of high-risk supplier (as per the Toolbox measure SM03), this may also include requirements for MNOs to conduct an assessment of the risk profile of their key suppliers, say in relation to the last criteria mentioned in the Coordinated risk assessment: *The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices*. Some of the guidance listed further in this section includes examples of checks that could be considered in this regard[14].

Competent authorities should pay close attention to objectives **SO 2 (Governance and risk management)** and **SO 4 (Security of third party assets)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This addresses Toolbox measures **TM08** and, to some extent, **TM09** and **TM10**.

Table 8: Additional guidance checklist for domain D1

#	SO	Checks to consider	Ref.[15]
1	SO2	Is the list of identified risks aligned with the main risks for 5G networks identified in the Coordinated risk assessment?	[a,e] [i,vi]
2	SO2	Are threats related to the exposure to potentially high-risk suppliers or managed service providers, including those residing in other jurisdictions, taken in consideration?	[a,e] [i,vi]
3	SO2	Has a potential dependency on a single supplier of 5G equipment been considered when assessing the main risks for security of networks and services?	[a,e] [i,vi]
4	SO4	Does MNO have security requirements placed on third parties as part of contractual arrangements & is there a mechanism to monitor that suppliers are meeting said contractual arrangements?	[e] [vi]
5	SO4	Does MNO require suppliers to comply with relevant EU certification schemes for 5G network components, customer equipment and/or suppliers' processes or for other non 5G-specific ICT products and services, such as end-user devices and/or cloud services[16]?	[e] [vi]
6	SO4	Does MNO require suppliers to demonstrate quality level of internal information security processes, including having security by design, built in the product development process?	[e] [vi]
7	SO4	Does MNO require suppliers to adhere to best practices and industry standards throughout the lifetime of the product?	[e] [vi]

[14] In addition, competent authorities may also want to explore and make use, if appropriate, of a concept of supplier trustworthiness, as applied in some MS. For example, according to Annex 2 of Germany's security catalogue (https://ec.europa.eu/growth/tools-databases/tris/de/index.cfm/search/?trisaction=search.detail&year=2020&num=496&mLang=EN), public telecommunications network operators and providers of publicly accessible telecommunications services with increased criticality are required to, in particular, appropriately select manufacturers and sellers or suppliers of critical components before purchasing them. An appropriate selection also includes an appropriate examination of the supply source's trustworthiness. The obligated company must obtain a comprehensive declaration from the supply source to demonstrate its trustworthiness. The declaration must relate to all safety-relevant components and, if applicable, functionalities, as well as the supply source itself (the manufacturer, including the supplier, and, if applicable, the seller or supplier).

[15] Here, and further in this section, the reference in the last column of a checklist table refers to the corresponding measure(s) and related evidence(s) in the Guideline that are most relevant for the check suggested and is provided in the following format: *[measure id] [evidence id]*

[16] When an EU certification schemes are not available, other interim solutions, such as reliance on certification schemes based on industry standards, could be considered instead.

#	SO	Checks to consider	Ref.[15]
8	SO4	Does MNO require suppliers to provide support for periodic security and penetration testing of its products?	[e] [vi]
9	SO4	Does MNO require suppliers to guarantee there are no intentionally introduced vulnerabilities in their products and to disclose and patch any known vulnerabilities[17] in their products without undue delay?	[e] [vi]
10	SO4	Does MNO require suppliers to have implemented security requirements of relevant 5G technical specifications and industry standards by default[18]?	[e] [vi]
11	SO4	Does MNO require suppliers to guarantee adequate protection and non-disclosure of confidential information from or about its customers to third parties, in particular to foreign intelligence or security authorities?	[e] [vi]
12	SO4	Does MNO require suppliers to support MNO in investigating and remedying security incidents[19]?	[e] [vi]

When reviewing and refining requirements for MNOs related to procurement (in relation to the above highlighted security objective SO 4 - Security of third party assets), competent authorities may also find useful to explore to technical reports and best practices related to security requirements for ICT procurement, such as the two ENISA reports listed below.

Document	Year	Description	URL
Indispensable baseline security requirements for the procurement of secure ICT products and services	ENISA, 2016	Short, practical, technologically neutral document with clear, simple and sector-agnostic minimum necessary indispensable requirements for secure ICT products and services.	https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services
Security Guide for ICT Procurement for electronic communications service providers	ENISA, 2014	Practical tool for individual providers to better manage security risks when dealing with vendors of ICT products and outsourced services. The Guide maps security risks which could lead to a disruption of electronic communications services for users, to a full framework of security requirements, which can be applied to vendors of ICT products and outsourced services used for the core operations of electronic communications networks and services.	https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement

3.2 DOMAIN D2: HUMAN RESOURCES SECURITY

Domain D2 (Human resources security) covers the following security objectives:

- SO 5: Background checks
- SO 6: Security knowledge and training
- SO 7: Personnel changes
- SO 8: Handling violations

Many of the measures in this security domain refer to *personnel*, which, in this context, includes not only employees, but also *contractors* and *third-party users*. This could be of particular importance in the context of 5G networks, with increased reliance on sub-contractors, including those from third countries, for the purpose of managing critical network functions. Moreover, adequate knowledge of key personnel is relevant for addressing one of the important vulnerabilities identified in the coordinated EU risk assessment, which applies particularly to

[17] In the case of vulnerabilities disclosed by the suppliers, competent authorities may also want to ensure that MNOs disclose such vulnerabilities to them
[18] Including all 3GPP optional security features of direct relevance for 5G network security
[19] Security should ideally be a shared responsibility between MNOs and suppliers.

MNOs: *lack of specialised and trained personnel* to secure, monitor and maintain 5G networks and services.

Competent authorities should pay close attention to objectives **SO 5 (Background checks)** and **SO 6 (Security knowledge and training)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This addresses Toolbox measures **TM05** and **TM06**.

Table 9: Additional guidance checklist for domain D2

#	SO	Checks to consider	Ref.
1	SO5	Does the list of personnel for whom background checks/screening has been performed also include contractors and third-party suppliers?	[b] [ii]
2	SO5	Are personnel who will have access (either physically or through management systems) to critical or sensitive components of 5G networks security-vetted (as stipulated in the provisions of the Toolbox technical measure TM06)?	[b] [ii]
3	SO6	Has the training program been updated to include coverage of specialized 5G technical topics?	[d] [iv]
4	SO6	Is there an evidence that the key personnel who will be in charge of deploying and operating 5G networks have followed the updated training courses?	[d] [v]
5	SO6	Is there an evidence that personnel who will have access (either physically or through management systems) to critical or sensitive network components are trained and qualified (as stipulated in the provisions of the Toolbox technical measure TM06)?	[d] [v]

3.3 DOMAIN D3: SECURITY OF SYSTEMS AND FACILITIES

Domain D3 (Security of systems and facilities) covers the following security objectives:

- SO 9: Physical and environmental security
- SO 10: Security of supplies
- SO 11: Access control to network and information systems
- SO 12: Integrity of network and information systems
- SO 13: Use of encryption
- SO 14: Protection of security-critical data

These security objectives contain various controls for ensuring physical and logical security of networks and systems. For this reason the domain D3 plays perhaps a central role in ensuring technical protection of critical or sensitive network components or functions, since majority of technical risks identified in the Coordinated risk assessment and, subsequently, majority of related technical measures identified in the Toolbox, are related precisely to physical and logical security of 5G networks and related information systems and facilities.

Competent authorities should therefore pay close attention to objectives **SO 9 (Physical and environmental security)**, **SO 11 (Access control to network and information systems)**, **SO 12 (Integrity of network and information systems)**, **SO 13 (Use of encryption)** and **SO 14 (Protection of security-critical data under this domain)**, checking that measures under these objectives are implemented and considering some of the additional checks as suggested in the tables below. This addresses Toolbox measures **TM03**, **TM06** and **TM07**.

Table 10: Additional guidance checklist for domain D3

#	SO	Checks to consider	Ref.
1	SO9	Are there documented, additional, risk-based controls for physical security for MEC and base stations included in the policy for physical security measures?	[d] [ii,iv]
2	SO9	Are there documented additional, adequate physical infrastructure controls (for example perimeter security for infrastructure and administrative premises, alarms and CCTV for detecting and recording incidents), especially for equipment locations which are unmanned, in place?	[d] [ii,iv]
3	SO9	Are there any controls in place to allow failsafe remote shutdown (or data clearing) for stolen equipment and/or to require re-authentication or configuration after a physical attack or power failure at base stations?	[d] [ii,iv]
4	SO9	Is there an evidence that access controls are in place for individuals accessing premises, including assurance that they are security-vetted, trained and qualified and that any access, especially by third parties and contractors is strictly monitored?	[d] [ii,iv]
5	SO9	Do physical security controls included in the policy for physical security measures cover (multi-vendor) spare part management, at least for critical assets?	[b] [ii]
6	SO11	Are there any additional strict network access controls applied according to the updated risk assessment that particularly considers 5G network architecture elements?	[f] [vii]
7	SO11	Is there an evidence demonstrating how the principle of least privilege is applied (including the explanation on how various rights in the network, such as access rights between network functions, network administrators' rights and alike are minimized)?	[f] [vi]
8	SO11	Is there an evidence showing how the principle of segregation of duties is applied?	[f] [vi]
9	SO11	Is there an evidence that the access control policy has been reviewed and revised in the context of assessment of 5G risks?	[c,h] [iii,xi]
10	SO11	Does the (revised) access control policy include provisions for restricting and/or strict controlling of remote access by third parties, especially by suppliers or managed service providers considered to be high-risk or accessing the network from outside of EU?	[c,h] [iii,iv]
11	SO11	Do authentication mechanisms implemented follow general good practices and industry standards for strong authentication?	[d] [iii,iv,vii]
12	SO11	Are there controls in place to only allow temporary access to third parties and/or remote access and that no permanent credentials are granted (e.g. temporary or one-time passwords, usable only for designated tasks)?	[d] [iii,iv,vii]
13	SO11	Is there a centralised solution for Privileged Access Management (PAM) in place[20]?	[d] [vii]
14	SO12	Do software patching procedures follow industry standard best practices for ensuring that software products or components have not been altered (e.g. appropriate cryptographic methods for integrity and authenticity protection)?	[d] [vi,vii]
15	SO12	Are there documented and tested processes for delivery and implementation of security patches to vulnerable components?	[d] [iii]
16	SO12	Are there appropriate physical protection mechanisms in place to ensure that hardware product have not been tampered with (e.g. physical security protection for equipment transport)[21]?	[c,d] [iii]
17	SO12	Are there specific timeframes for applying security patches to vulnerable components, particularly in the case of high and critical vulnerabilities[22]?	[d] [iii]
18	SO13	Is encryption applied for the concealment and protection of customer security critical data, in particular the permanent user identifiers[23]?	[a] [i,ii]
19	SO13	Is encryption applied for protection of signalling traffic between operators[24]?	[a] [i,ii]
20	SO13	Is encryption applied for transport protection between network functions[25]?	[a] [i,ii]

[20] Such solution should secure physical or virtual network functions and resources by controlling, monitoring and auditing privileged access to all critical or sensitive network components or functions through a single pane of glass
[21] Note that this check may be seen as not being directly in the scope of SO 12, if this security objective is interpreted to pertain to software integrity only. If interpreted in its wider meaning, as pertaining to general integrity of network and information systems, then securing hardware devices that contain data or that ultimately will be running embedded software themselves, could be considered in the scope. Alternative mappings of this check could be considered, such as related it to SO 10 – Security of supplies (although supplies in this context pertain more to utilities such as power supply), to SO 4 – Security of third party assets (if the obligation is defined for suppliers) or even SO 9 – Physical security (if assets not yet deployed within the network are included in the scope).
[22] E.g. CVSS score 7.0 – 10.0
[23] SUPI concealment and de-concealment through SUCI and SIDF
[24] E.g. TLS 1.2 or 1.3 or PRINS
[25] SBA, using TLS 1.2 or 1.3

#	SO	Checks to consider	Ref.
21	SO13	Is encryption applied for protection of confidentiality of user and signalling data between user equipment and base stations?	[a] [i,ii]
22	SO14	Are there appropriate controls in place, according to best practices, for the protection of cryptographic key material in UICC (or eUICC)[26]?	[a,b] [ii]
23	SO14	Are appropriate controls in place, according to best practices, for the protection of cryptographic key material for encryption of subscriber permanent identifiers (SUPI)?	[a,b] [ii]
24	SO14	Are there appropriate controls in place, according to best practices, for the protection of any other cryptographic key material used to encrypt communication between network elements or between different networks[27]?	[a,b] [ii]
25	SO14	Are there appropriate controls in place for protection of VNF private keys to authenticate NF exchanges in the 5G core network?	[a] [ii]

3.4 DOMAIN D4: OPERATIONS MANAGEMENT

Domain D4 (Operations management) covers the following security objectives:

- SO 15: Operational procedures
- SO 16: Change management
- SO 17: Asset management

Considering the technical complexity and increased softwarization of key elements of 5G network infrastructure, it is of particular importance that MNOs have good and up-to-date operational procedures in place, in particular related to asset management, to understand the critical assets, and to have solid change management mechanisms in place.

Competent authorities should therefore pay close attention to objectives **SO 16 (Change management)** and **SO 17 (Asset management)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This address Toolbox measures **TM01** and **TM07**.

Table 11: Additional guidance checklist for domain D4

#	SO	Checks to consider	Ref.
1	SO16	Are there regular assessments of potential impact of an intended change prior to major system changes, especially when critical or sensitive network components are about to be updated?	[all] [ii,iv]
2	SO16	Is there a mechanism in place to ensure that any major actual change implemented, especially for critical or sensitive network components, is recorded and any irregularities encountered during the change process are investigated and, if incident reporting conditions are met, reported to competent authorities?	[all] [ii,iv]
3	SO16	Are changes to virtualised network environment (e.g. through patching of software defined network components) included in the change management policies and procedures?	[b,d] [ii,iv]
4	SO16	Has MNO given consideration to moving to software development lifecycle best practices such as Agile, Continuous Integration/Continuous Development (CI/CD), and DevSecOps, given 5G's shift to a software based network?	[b,d] [ii,iv]
5	SO17	Is asset criticality assessment aligned with the list of critical assets identified in the Coordinated risk assessment?	[b,c] [ii,v]
6	SO17	Has the MNO established relevant information repositories/registries containing details about deployed technologies and components and are such registries appropriately maintained (e.g. timely updates upon changes to the network)?	[b,c] [ii,v]
7	SO17	Are there mechanisms envisaged in the MNO policies/procedures for asset management for conducting regular assessments of their physical assets and for categorisation of their physical network assets (e.g. core network assets, transmission hubs, exchanges, base-stations, interconnection and transport links) based on a risk assessment and according to the assets sensitivity/criticality.	[b,c] [ii,v]

[26] Even when transferred from the UICC manufacturer to the MNO
[27] This may include (but Is not limited to) cryptographic key material for remote SIM provisioning, for operating the N32 interface and DIAMETER or for the operation of the SIP infrastructure

#	SO	Checks to consider	Ref.
8	SO17	Have policies/procedures for asset management been updated to reflect the fact that 5G networks will likely be virtualised, with VNFs being instantiated and decommissioned in an automated way and do such updates include sufficient provisions to ensure good understanding of the virtual network, including data flows, trust domains and the location and status of the physical hosts on which the virtual network resides?	[b,c] [ii,v]

3.5 DOMAIN D5: INCIDENT MANAGEMENT

Domain D5 (Incident management) covers the following security objectives:

- SO 18: Incident management procedures
- SO 19: Incident detection capability
- SO 20: Incident reporting and communication

Technological complexity of new generation mobile networks, potential dependency on suppliers and/or managed service providers that provide equipment and/or services, sometimes using remote connections from third countries and the overall complexity of the threat landscape require mature incident management capabilities, including state of the art incident detection capabilities. Moreover, comprehensive and reliable reporting on incidents that had a significant impact on operations of 5G networks and services to relevant competent authorities is equally important.

Competent authorities should therefore pay close attention to objectives **SO 19 (Incident detection capability)** and **SO 20 (Incident reporting and communication)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This addresses Toolbox measure **TM05**.

Table 12: Additional guidance checklist for domain D5

#	SO	Checks to consider	Ref.
1	SO19	Are relevant logs related to remote network access regularly reviewed according to predefined procedures?	[d] [v]
2	SO19	Are there capabilities for anomaly detection in place?	[b] [ii]
3	SO19	Is the monitoring infrastructure[28] implemented according to the recommendation from the Toolbox, including whether such monitoring infrastructure is established on premise, ideally inside the country or inside the EU[29]?	[c] [iii]
4	SO19	Does MNO have adequate resources available to monitor, understand and analyse security-related network activity?	[b] [ii]
5	SO20	Does MNO comply with relevant incident reporting provisions within a given legal framework?	[c] [iv]

3.6 DOMAIN D6: BUSINESS CONTINUITY MANAGEMENT

Domain D6 (Business continuity management) covers the following security objectives:

- SO 21: Service continuity strategy and contingency plans
- SO 22: Disaster recovery capabilities

Implementation of measures under this domain ensures robust network resilience and adequate disaster recovery and business continuity capabilities. And while this may already be essential part of MNO's operations, it is worth emphasizing its importance in the context of 5G networks,

[28] such as Network Operation Centres (NOC) and/or Security Operation Centres (SOC), that can serve for the purpose of timely detection of significant events or incidents
[29] This follows the general requirement as identified in the Toolbox technical measure TM05, implementation on MS level may vary

as indicated in both the Coordinated risk assessment and the Toolbox. In the Coordinated risk assessment, a massive failure of networks due to interruption of electricity supply or other support systems is explicitly highlighted as one of the 9 identified significant risks to 5G networks. Consequently, the Toolbox technical measure TM11 calls MNOs to further strengthen the corresponding resilience and continuity plans.

Competent authorities should pay close attention to objectives **SO 21 (Service continuity strategy and contingency plans)** and **SO 22 (Disaster recovery capabilities)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This addresses Toolbox technical measure **TM11**.

Table 13: Additional guidance checklist for domain D6

#	SO	Checks to consider	Ref.
1	SO21	Are there measures in place to ensure supply-chain resilience (e.g. by ensuring that contingency plans consider scenarios of removal of critical suppliers[30], understanding the related impact and having appropriate failback strategies in place)?	[b] [vii]
2	SO21	Are there any special provisions added to existing contingency plans to cover time-critical applications of 5G services, such as URLLC as to ensure higher network availability for such services?	[b] [vii]
3	SO21	Is there a map of critical dependencies that may directly or indirectly impact availability or continuity of 5G network service and if corresponding mitigation measures are defined and documented?	[d] [x]
4	SO21	Is there a map of critical sectors and services directly dependent on the continuity of network and service operations and if criticality of such systems is taken in consideration in contingency plans?	[d] [x]
5	SO22	Are there documented plans in place in case of a disaster affecting the ongoing operation of the MNO's network?	[b] [ii]

3.7 DOMAIN D7: MONITORING, AUDITING AND TESTING

Domain D7, Monitoring, auditing and testing, covers the following security objectives:

- SO 23: Monitoring and logging policies
- SO 24: Exercise contingency plans
- SO 25: Network and information system testing
- SO 26: Security assessments
- SO 27: Compliance monitoring

In addition to having robust incident detection and management capabilities in place, as discussed earlier, having sophisticated monitoring and logging capabilities is of significant importance for detecting and analysing security incidents. This may particularly be relevant for the environments where remote access to critical or sensitive network components or functions is expected and especially when such access is to be established from third countries and/or from suppliers or service providers considered to be high-risk. Coordinated risk assessment, in particular, identifies lack of adequate monitoring practices in MNOs as one of the key vulnerabilities. Consequently, the need for strict monitoring and logging is emphasized in Toolbox technical measure TM05 as well as in the technical measure TM03.

At the same time, considering the increased virtualization and softwarization, the importance of testing and security assessments may be higher in 5G networks. Although not explicitly mentioned in the Toolbox, this is implicitly related to some of the technical measures, in particular to the technical measure TM07[31].

[30] Say, due to trade sanctions, market conditions or similar
[31] The Toolbox implementation report, published in June 2019, implicitly confirms the importance of good security testing practices by referring to best practices in several MS who have highlighted the relevance of this security control. One of the sources to consider for general guidance on security testing best practices is the US NIST special publication SP-800-115,

Finally, having the appropriate compliance monitoring in place ensures continuous compliance with relevant standards and in the context of 5G this could also ensure compliance with relevant 5G standards, such as 3GPP, as requested by the Toolbox (technical measure TM02).

Competent authorities should therefore pay close attention to objectives **SO 23 (Monitoring and logging policies), SO25 (Network and information system testing), SO 26 (Security assessments)** and **SO 27 (Compliance monitoring)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the tables below. This addresses Toolbox measures **TM02**, **TM03**, **TM05** and **TM07**.

Table 14: Additional guidance checklist for domain D7

#	SO	Checks to consider	Ref.
1	SO23	Are there adequate monitoring capabilities in place in line with the recommendations form the Toolbox technical measure TM05, to ensure providing clear visibility and to implement effective network monitoring of at least the critical or sensitive network components or functions, to detect anomalies and to identify and avoid threats, including but not limited to threats to 5G core coming from compromised end-user devices?	[b,c] [iii,iv]
2	SO23	Does the monitoring and logging policy also include monitoring of VPN and remote access to 5G network from remote locations[32]?	[b,c] [ii]
3	SO23	Is there monitoring in place for roaming and interconnections (e.g. message monitoring and filtering capabilities to identify and block malformed, prohibited and unauthorised packets, confirm that interfaces are only accessible to the correct external applications and/or networks and enabling of audit logging and delivery of data to SIEM for analysis for relevant threat vectors)?	[b,c] [iii,iv]
4	SO25	Are all patches, especially those to critical or sensitive network components or functions, subjected to security testing in controlled environment prior to deployment?	[a,d] [i,iii]
5	SO26	Are security tests, vulnerability assessments/scans and penetration tests done on deployment and subsequently, on periodic basis, for newly deployed network components, in particular for products supplied by suppliers considered to be high-risk?	[a,d] [i,iii]
6	SO27	Is monitoring of compliance with relevant 5G standards (e.g. 3GPP, ETSI NFV[33]) included in the compliance monitoring policies and procedures?	[c,d] [iv,v]

3.8 DOMAIN D8: THREAT AWARENESS

Domain D8, Threat awareness, covers the following security objectives:

- SO 28: Threat intelligence
- SO 29: Informing users about the threats

In the complex and evolving 5G threat landscape, it is necessary to ensure that MNOs operating 5G networks are aware of the current and emerging threats and that they take them in consideration when (re)assessing security risks. At the same time, user awareness about known threats and vulnerabilities, as recommended in the security objective SO29, may increase the overall security of 5G services provided to end-users.

Competent authorities may want to focus in particular on objectives **SO 28 (Threat intelligence)** and **SO 29 (Informing users about the threats)**, checking that measures under these objectives are implemented and considering additional checks as suggested in the table below. This addresses Toolbox measure **TM05** and is related to the Toolbox supporting action SA09 and may contribute to the mitigation of the Risk 9 from the Coordinated risk assessment (listed in the Table 3 in this document).

Technical Guide to Information Security Testing and Assessment
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152164

[32] This may include installation of appropriate technical solutions for monitoring such as recording jump-boxes for remote connections

[33] References to related technical specs for 3GPP and ETSI NFV standards can be found in Annex II and Section 4 of this supplement, respectively

Table 15: Additional guidance checklist for domain D8

#	SO	Checks to consider	Ref.
1	SO28	Does threat monitoring and/or threat intelligence program include variety of threats of particular significance for 5G networks?	[a,b] [i,iii]
2	SO28	Are relevant and current sources and publications[34] and/or relevant CTI tools and platforms[35] consulted or used systematically?	[a,b] [i,iii]
3	SO29	Are there mechanisms in place to inform users about potentially vulnerable end user devices, including IoT devices and of related risks?	[b] [iv]
4	SO29	Has guidance been provided to consumers and enterprises on signalling threats in legacy network environments (associated with SS7[36], GTP[37] and Diameter[38] signalling protocols) such as location tracking, interception of data, call, e-mail and SMS messages, financial fraud and theft or digital identity theft and highlighting the risk of using SMS as a multi-factor authentication mechanism?	[b] [iv]

[34] For example, ENISA 5G threat landscape report, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, or other relevant reports from private and public organisations and bodies active in the CTI in the area of telecommunications and mobile networks
[35] In addition to commercial products and services, there are also open source solutions available that may be considered. Examples include MISP (https://www.misp-project.org/), OpenCTI (https://www.opencti.io/en/) and others.
[36] Signalling System 7 (SS7) is a set of signalling protocols developed in 1975, used primarily in 2G, 3G and fixed networks, to exchange information among different elements of the same network or between networks (call routing, roaming information, features available to subscriber etc.).
[37] GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry general packet radio service (GPRS) within GSM, UMTS and LTE networks
[38] Diameter Protocol provides authentication, authorization, and accounting (AAA) messaging services for network access and data mobility applications primarily in 3G, IP Multimedia Systems (IMS), and LTE/4G networks and may also be used in 5G networks

4. SECURITY OF SPECIFIC 5G TECHNOLOGIES

5G introduces or utilises several new technologies, in different places of the network, such as:

- Network virtualization
- Network slicing
- Edge computing

Number of security risks related to the utilisation of the above listed technologies in MNO's 5G networks can be addressed by deploying general network security and information security management controls, such as those related to access control (including robust authentication and authorization mechanisms), DDoS prevention, reinforced physical security (including at remote locations) or security incident and event monitoring. Therefore, it is important that competent authorities ensure implementation and audit of relevant measures from the corresponding Guideline security objectives, taking in consideration additional guidance provided in this supplement, where applicable.

However, there are some specific vulnerabilities related to these technologies, which MNOs would have to take in consideration when doing a risk assessment. Consequently, the identified risks need to be addressed adequately, which in some cases may require implementation of additional security controls.

In this section, we provide further high-level information about some of these underlying technologies and we highlight the most relevant security aspects. We also include reference lists with pointers to the relevant industry standards and best practices for each of these technologies.

A more detailed technical information about the listed technologies and their security aspects, including the *architecture*, *assets*, *security considerations* and *threats* can be found it the comprehensive **ENISA threat landscape for 5G Networks**[39] (hereinafter '**ETL5G**'). The new version of the report (currently in preparation) also brings analysis of *vulnerabilities* and identification of *related security controls*.

Table 16: ENISA Threat Landscape for 5G Networks

Document	Body	Description	URL
ENISA Threat Landscape for 5G networks 2019	ENISA	The **2019 report** drew an initial threat landscape and presented an overview of the challenges in the security of 5G networks. It included a comprehensive 5G architecture, asset diagram, threat taxonomy, threats – assets mapping and an initial assessment of threat agent motives.	https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks
ENISA Threat Landscape for 5G networks 2020	ENISA	The **2020 update** (in preparation) brings updates to 5G architecture and assets and includes 5G migration options, management processes, vulnerability analysis an map of security controls from 5G specs to key vulnerabilities.	Document in preparation, will be available on ENISA website: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/

[39] Reference provided in the Table 15

4.1 NETWORK VIRTUALISATION SECURITY

Network Function Virtualisation (NFV) technology is based on the virtualisation of network services traditionally run on proprietary dedicated equipment including routers, switches, access nodes, gateways and a variety of other hardware [40]. The main benefits of the NFV technology are scalability and better utilisation of network resources; reduced power consumption and improved efficiency of space usage; and reduced operational and capital expenditures.

The main elements of the NFV architecture are:

- Virtual Network Functions (VNFs);
- NFV Infrastructure (NFVI); and
- Management, Automation and Network Orchestration (MANO) layer.

The latter, MANO, is also identified as a critical asset in the EU coordinated risk assessment.

A more detailed technical information about the NFV architecture can be found in ETL5G. The same report also identifies the key virtualisation threats, being the following:

- Abuse on Data Centres Interconnect (DCI) protocol
- Abuse of cloud computational resources
- Network virtualisation bypassing
- Virtualised host abuse

The closely related technology is **Software Defined Networks (SDN)**. It allows dynamic management of network resources by separating the network control plane from the data plane. This enables a directly programmable network control and an abstracted underlying infrastructure for applications and network services. A logically centralised control plane allows a network wide view of data plane network elements. This can then be exposed to the application layer to achieve simplified network management and improved agility. ETL5G identifies and explains number of control plane, data plane and API related vulnerabilities in SDN.

Another related concept of relevance is **containerisation**. Containerisation is essentially a simplified form of virtualisation, whereby instead of running an entire operating system virtually only the user-space elements of the host OS are separated from each other and the hosting operating system. This gives all the advantages of full virtualisation but without the overhead of running the full guest OS, thus leading to greater efficiencies, although it does require that each container presents the same OS version to all applications (i.e. identical instances of the host OS). The efficiency and reliability gains greatly increase the portability of such containers and the ability to move entire application stacks within a virtualised environment has been made of great use for application development. The table 16 (below) includes references to documents that cover security aspects of containerisation in more detail.

In addition to ensuring the implementation of general security measures from the Guideline and taking in consideration additional guidance provided in the chapter 3 of this supplement, competent authorities may also want to check that relevant network virtualisation security risks are included in MNO's security assessment and that MNOs follow industry standards and best practices, in particular relevant ETSI NFV. We list the most relevant[41] ETSI technical specifications and additional relevant technical reports and documents, including two ENISA publications on SDN and virtualization security in the following table.

[40] https://searchnetworking.techtarget.com/definition/network-functions-virtualization-NFV
[41] The list of ETSI NFV-SEC specifications given in the table does not include all the specification document, but only selected ones, that are believed to be of most relevance in terms of identifying specific detailed technical controls that could be considered for securing NFV. The full list is available here: https://www.etsi.org/standards#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=0&published=1&historical=0&startDate=&endDate=&harmonized=0&keyword=&TB=799&stdType=&frequency=&mandate=&collection=&sort=1

Table 17: Virtualisation security reference list

Document	Body	Description	URL
Technical specifications/standards			
NFV-SEC 001	ETSI	Main security specification defining the NFV security and the problem statement, identifying several work areas associated with securing the NFV technology	https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf
NFV-SEC 003	ETSI	Describes the security and trust guidance for NFV development, architecture and operation	https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf
NFV-SEC 021	ETSI	The specification addresses security requirements for VNF onboarding and instantiation	https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/021/02.06.01_60/gs_NFV-SEC021v020601p.pdf
Technical reports and other documents			
TR 33.848	3GPP	Draft specification provides the progress to date on 3GPP study on security impacts of virtualization. It is work in progress. It includes twenty-four key security issues with respect to the virtualisation of 3GPP functions and architecture. Some of these key issues refer to ETSI NFV SEC specification	https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=3574
Threat Landscape and Good Practice Guide for SDN	ENISA	The study reviews threats and potential compromises related to the security of SDN networks and includes related technical, policy and organizational recommendations.	https://www.enisa.europa.eu/publications/sdn-threat-landscape
Security aspects of virtualization	ENISA	Analysis of the status of virtualization security, including current efforts, emerging best practices, known security gaps, challenges and limits of virtualized systems.	https://www.enisa.europa.eu/publications/security-aspects-of-virtualization
SP 800-125	NIST	Guide to Security for Full Virtualisation Technologies. The purpose of the guide is to discuss the security concerns associated with full virtualization technologies for server and desktop virtualization, and to provide recommendations for addressing these concerns.	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf
SP 800-125B	NIST	Secure Virtual Network Configuration for VM Protection. The purpose of this NIST Special Publication (SP) is to provide an analysis of various virtual network configuration options for protection of virtual machines (VMs) and present recommendations based on the analysis.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf
SP 800-190	NIST	Application Container Security Guide. This publication explains security concerns associated with the use of containers and gives recommendations and best practices for addressing these concerns.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf
Best practices for mitigating risks in virtualized environments	CSA	This paper by Cloud Security Alliance provides guidance on security risks and best practices specific to virtualization technologies that run on server hardware.	https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf

4.2 NETWORK SLICING SECURITY

Network slicing enables MNOs to allocate portions of their networks for specific users (to ensure isolation on a neutral host environment) and use cases, e.g. industry automation, connected cars or enterprise networks. The objective is to provide a set of optimised resources and network topology to satisfy the needs of use cases (for example, connectivity, speed, latency and capacity) and conform to a specific service level agreement. As NFV, MEC and SDN, the network slicing concept is also built on virtual networking architecture where multiple virtual networks are established using shared physical infrastructure. Using common network resources (e.g. storage and processors), network slices can be created to establish a logical and self-contained network configured and connected end-to-end.

A detailed technical information about the network slicing architecture can be found in ETL5G. The same report also identifies the key areas network slicing **vulnerabilities**[42] (Security-as-a-Service, Resource isolation, Secure Management and Orchestration and Trust Model) and provides further explanations related to these vulnerabilities.

In addition to ensuring the implementation of general security measures from the Guideline and taking in consideration additional guidance provided in the section 3 of this supplement, competent authorities also may want to check that relevant network slicing security risks are included in MNO's security assessment and that MNOs follow industry standards and best practices for securing network slicing. We list some of the relevant technical documents in the table below.

Table 18: Slicing security reference list

Document	Body	Description	URL
Technical reports and other documents			
TR 33.811	3GPP	Technical Report (TR) 33.811 (Release 15, June 2018) presents a study on the threats, potential security requirements and solutions for the 5G network slicing management and includes identification of key security issues and recommended mitigation measures.	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3358
TR 33.813	3GPP	Technical Report (TR) 33.813 (Release 16, July 2020) is currently being developed mainly to address network slicing security issues not addressed in Release 15. The contents of the technical report are work-in-progress and include several key issues and proposed solutions.	https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541

4.3 EDGE COMPUTING SECURITY

Edge computing refers to a cloud-based IT service environment located at the edge of a network. Multi-access Edge Computing (MEC) is a technology aiming to satisfy the requirements of high-bandwidth and low-latency applications which operate at the edge of the network[43]. MEC is based on the convergence of IT and telecommunications networking. Key benefits are reduced network congestion and improved performance for low latency applications. The ability of storing, processing and delivering content locally without requiring backhauling and centralised core network is the main feature of the technology.

Deployment of MEC technology as part of an NFV environment is envisaged. Therefore, security requirements of MEC enabled applications are expected to be addressed within the

[42] Vulnerability analysis is include in the ETL5G only in the 2020 report version (currently in preparation)
[43] Based on: https://www.sdxcentral.com/edge/definitions/what-multi-access-edge-computing-mec/

NFV security framework. Security fundamentals including data encryption, network visibility, automated monitoring and access control based on the principle of least privilege and supported by intrusion prevention and detection are all applicable to the MEC platform. Threats include infrastructure attacks related to wireless technology vulnerabilities (e.g. denial of service attacks to consume the bandwidth and computing resources at the edge or man in the middle attacks to inject or eavesdrop traffic from the edge), virtualisation attacks (e.g. denial of service and man in the middle attacks by rogue virtual machines) and privacy leakage (e.g. unauthorised access to information storage in the edge cloud).

A more detailed technical information about the MEC architecture can be found it ETL5G. The same report also identifies and described the key MEC **threats** (e.g. a false or rogue MEC gateway, edge node overload and abuse of edge open APIs) as well as the key areas of **vulnerabilities**[44] (vulnerabilities related to virtualization and containerization, physical security, APIs and regulatory issues) and provides further explanations related to these vulnerabilities.

In addition to ensuring the implementation of general security measures from the Guideline and taking in consideration additional guidance provided in the chapter 3 of this supplement, competent authorities may want to check that relevant edge computing security risks are included in MNO's security assessment and that MNOs follow industry standards and best practices, in particular relevant technical specifications and reports from ETSI, as a leading organization in standardization of MEC technology[45]. We list some of the most relevant technical specifications and additional relevant technical reports and documents in the table below.

Table 19: MEC security reference list

Document	Body	Description	URL
Technical specifications/standards			
GS MEC 002	ETSI	Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/02.01.01_60/gs_MEC002v020101p.pdf
GS MEC 003	ETSI	Multi-access Edge Computing (MEC); Framework and Reference Architecture	https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_MEC003v020101p.pdf
Technical reports and other documents			
ETSI white paper #20	ETSI	Developing Software for Multi-Access Edge Computing	https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf
ETSI white paper #36	ETSI	Harmonizing standards for edge computing - A synergized architecture leveraging ETSI ISG MEC and 3GPP specification	https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_wp36_Harmonizing-standards-for-edge-computing.pdf

[44] Vulnerability analysis is included in the ETL5G only in the 2020 report version (currently in preparation)
[45] https://www.etsi.org/technologies/multi-access-edge-computing/mec

Additionally, competent authorities may also find useful to take note of the following additional security aspects related to MEC[46]:

- MEC device clusters may be more susceptible to physical theft and infiltration as they are likely to be located in physically less secure locations. Similarly, software tampering of the MEC platform should be prevented. To achieve this, platform security, platform management security, data storage and transmission security need to be enhanced as well as introducing trusted computing technologies.
- An increased number of entry points in the MEC environment (e.g. IoT use case) implies challenging attack surface and complex certificate management as the absence or weakness of security measures in MEC devices can be exploited and create vulnerabilities for the whole network. Ensuring real-time network visibility is one of the key considerations.
- Robust authentication and authorisation procedures need to be in place for the MEC platform which is located much closer to access network than the core network. The key issue is how to establish a uniform level of security policies for all MEC elements to minimise the risks.
- In terms of network resilience, the introduction of the MEC platform should not affect network availability. This means that MEC solution vendors should offer the level of resilience to meet high-availability requirements of network operators. An appropriate failsafe mechanism should be in place to prevent the MEC platform failure from adversely affecting the normal operation of the network.

[46] Based on: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20ed2_MEC_SoftwareDevelopment.pdf, https://www.sdxcentral.com/edge/definitions/mec-security/ , https://www.gsma.com/futurenetworks/wp-content/uploads/2020/02/6_Smart-Port-MEC-Security-Application-Based-on-5G-SA_GSMA.pdf, https://innovationatwork.ieee.org/edge-computing-security-issues-and-trends-to-watch-in-2020/ . Remark: The last URL referenced is valid at the time of document writing (October 2020). Please note, however, that given that GSMA is a closed group organisation the document may not be publicly available in the future to non-members.

ANNEX I: LIST OF ACRONYMS

Acronym	Meaning
5GC	5G Core Network
5G-RAN	5G Radio Access Network
API	Application Programming Interface
CCTV	Closed-circuit television
CTI	Cyber threat intelligence
DDoS	Distributed Denial of Service (attack)
ETSI	European Telecommunications Standards Institute
eNB	Evolved Node B
eUICC	Embedded Universal Integrated Circuit Card
gNB	NR Node B
GPS	Global Positioning by Satellite
GSMA	Global System for Mobile Communications Association
GTP	GPRS Tunnelling Protocol
LTE	Long-Term Evolution
MANO	NFV management and network orchestration
MEC	Multi-access Edge Computing
NFV	Network Function Virtualisation
NOC	Network Operation Center
NSA	Non stand alone
PAM	Privilege Access Management
PRINS	PRotocol for N32 INterconnect Security
PKI	Public key infrastructure
SBA	Service Based Architecture
SDN	Software Defined Networking
SIDF	Subscription Identifier De-concealing Function
SIEM	Security Information and Event Management
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
UE	User Equipment
UMTS	Universal Mobile Telecommunications Service
UICC	Universal Integrated Circuit Card
URLLC	Ultra-Reliable Low-Latency Communication
VPN	Virtual Private Network

ANNEX II: 3GPP SECURITY REFERENCE LIST

The reference list in the table below contains references to 3GPP technical specification TS 33.501, which defines the 5G security architecture, as well as to a series of technical specification documents from the SCAS (Security Assurance Specifications) that contain relevant test cases for assessment of compliance with security requirements.

In addition, the table contains an additional list of 3GPP specs of relevance for NSA (non-standalone) 5G deployments options. Further technical details about different implementation options/migration paths can be found in ETL5G[47]. This includes the description of the main elements of a NSA architecture, as well as identification and analysis of specific risks (such as those related to legacy technologies, roaming risks or a failure to meet general security assurance requirements).

Table 20: 3GPP Security Specifications Reference List

Standard / specs/ doc	Body	Description	URL
Technical specifications – 5G security requirements			
TS 33.501	3GPP	Security architecture and procedures for 5G System	https://www.3gpp.org/DynaReport/33501.htm
Technical specification – 5G assurance			
TS 33.511	3GPP	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class	https://www.3gpp.org/DynaReport/33511.htm
TS 33.512	3GPP	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)	https://www.3gpp.org/DynaReport/33512.htm
TS 33.513	3GPP	5G Security Assurance Specification (SCAS); User Plane Function (UPF)	https://www.3gpp.org/DynaReport/33513.htm
TS 33.514	3GPP	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class	https://www.3gpp.org/DynaReport/33514.htm
TS 33.515	3GPP	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class	https://www.3gpp.org/DynaReport/33515.htm
TS 33.516	3GPP	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class	https://www.3gpp.org/DynaReport/33516.htm
TS 33.517	3GPP	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class	https://www.3gpp.org/DynaReport/33517.htm
TS 33.518	3GPP	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class	https://www.3gpp.org/DynaReport/33518.htm
TS 33.519	3GPP	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class	https://www.3gpp.org/DynaReport/33519.htm
TS 33.520	3GPP	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)	https://www.3gpp.org/DynaReport/33520.htm
TS 33.521	3GPP	5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)	https://www.3gpp.org/DynaReport/33521.htm
TS 33.522	3GPP	5G Security Assurance Specification (SCAS); Service Communication Proxy (SECOP)	https://www.3gpp.org/DynaReport/33522.htm

[47] Coverage of implementation options/migration paths is included in the ETL5G only in the 2020 report version (currently in preparation)

Technical specifications of relevance for 5G NSA (non-standalone)			
TS 33.401	3GPP	3GPP System Architecture Evolution (SAE); Security architecture	https://www.3gpp.org/DynaReport/33401.htm
TS 33.402	3GPP	3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses	https://www.3gpp.org/DynaReport/33402.htm
TS 33.116	3GPP	Security Assurance Specification (SCAS) for the MME network product class	https://www.3gpp.org/DynaReport/33116.htm
TS 33.117	3GPP	Catalogue of general security assurance requirements	https://www.3gpp.org/DynaReport/33117.htm
TS 33.216	3GPP	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class	https://www.3gpp.org/DynaReport/33216.htm
TS 33.250	3GPP	Security assurance specification for the PGW network product class	https://www.3gpp.org/DynaReport/33250.htm

ANNEX III: TOOLBOX MAPPING

The table below shows a mapping between the (supplemented) Guideline security domains and related technical measures form the Toolbox that are being addressed through the implementation of related measures and supplementary guidance.

Table 21: Toolbox Mapping

	D1: Governance and risk mgt.	D2: Human resources security	D3: Security of systems and facilities	D4: Operations management	D5: Incident management	D6: Business continuity management	D7: Monitoring, auditing, testing	D8: Threat awareness
TM01	■	■	■	■	■	■	■	■
TM02			■				■	
TM03			■				■	
TM04			■				■	
TM05		■			■		■	■
TM06		■	■					
TM07			■	■			■	
TM08	■							
TM09	■							
TM10	■							
TM11						■		

■ Directly addressed
■ Indirectly/partly addressed

TP-01-20-759-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-456-5
DOI: 10.2824/098554