THE EU CYBERSECURITY AGENCY

ENISA – 5G SECURITY

Main projects implementing 5G Toolbox

Sławomir Bryska, ENISA

20 October 2022

AGENDA

EU 5G security policy context

Main ENISA publications (Dec 2020 – present)

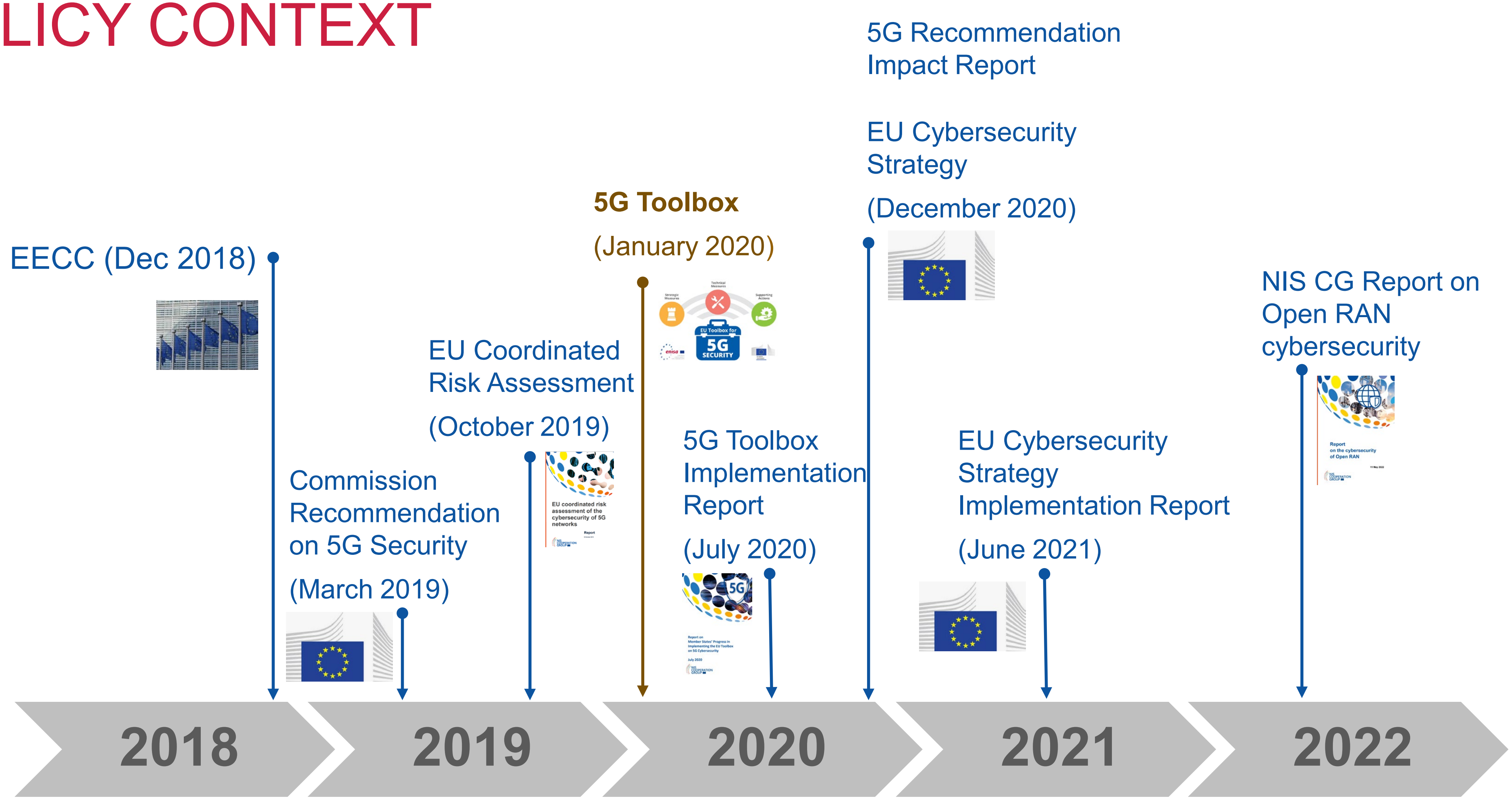
Report by NIS CG on cybersecurity of Open RAN

5G security certification scheme

5G Matrix

EU 5G SECURITY POLICY CONTEXT

POLICY CONTEXT



EECC (Dec 2018)

Commission Recommendation on 5G Security

(March 2019)

EU Coordinated Risk Assessment

(October 2019)

5G Toolbox

(January 2020)

5G Toolbox Implementation Report

(July 2020)

5G Recommendation Impact Report

EU Cybersecurity Strategy

(December 2020)

EU Cybersecurity Strategy Implementation Report

(June 2021)

NIS CG Report on Open RAN cybersecurity

2018
2019
2020
2021
2022
EU coordinated risk assessment of the cybersecurity of 5G networks
Report
NIS COOPERATION GROUP
Strategic Measures
Technical Measures
Supporting Actions
EU Toolbox for 5G SECURITY
enisa
5G
Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity
July 2020
NIS COOPERATION GROUP
Report on the cybersecurity of Open RAN
11 May 2022
NIS COOPERATION GROUP

MAIN ENISA PUBLICATIONS
DEC 2020 – PRESENT

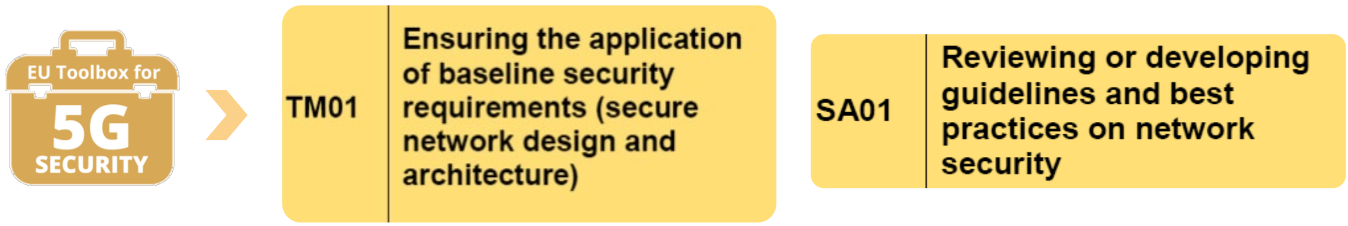
ENISA EECC GUIDELINE

Published in December 2020 and revised in July 2021, this is a general technology-neutral guideline, rather than 5G-specific.

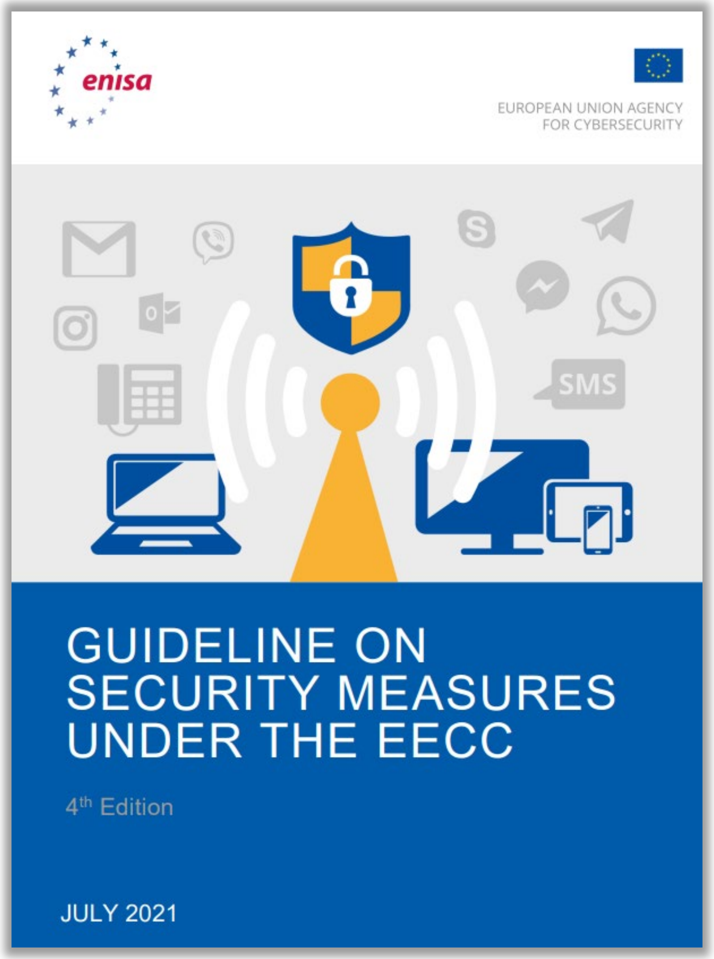
It is an evolution of a prior Article 13a Technical Guideline, first published in December 2011.

29 security objectives grouped into 8 domains

144 high-level general controls and corresponding 171 pieces of evidence, grouped into three sophistication levels.



TM01	Ensuring the application of baseline security requirements (secure network design and architecture)
SA01	Reviewing or developing guidelines and best practices on network security


enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

GUIDELINE ON SECURITY MEASURES UNDER THE EECC

4th Edition

JULY 2021

5G SUPPLEMENT TO THE EECC GUIDELINE

Published in December 2020 alongside the EECC Guideline (also revised in July 2021), it adds an additional 5G checklist.

70 5G ‘checks’. For example:

- Has a potential dependency on a single supplier of 5G equipment been considered in the risk assessment?
- Do authentication mechanisms implemented follow general good practices and industry standards?
- Is encryption applied for protection of signalling traffic between operators?

EU Toolbox for 5G SECURITY

TM01	Ensuring the application of baseline security requirements (secure network design and architecture)
SA01	Reviewing or developing guidelines and best practices on network security

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

5G SUPPLEMENT

To the Guideline on Security Measures under the EECC

2nd Edition

JULY 2021

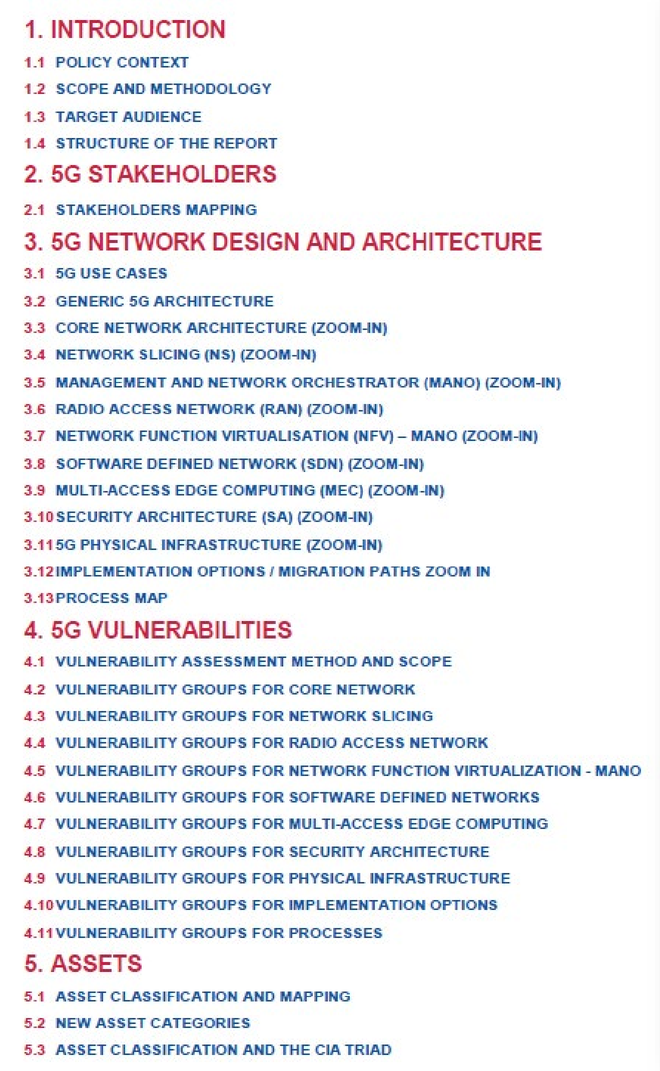
5G THREAT LANDSCAPE

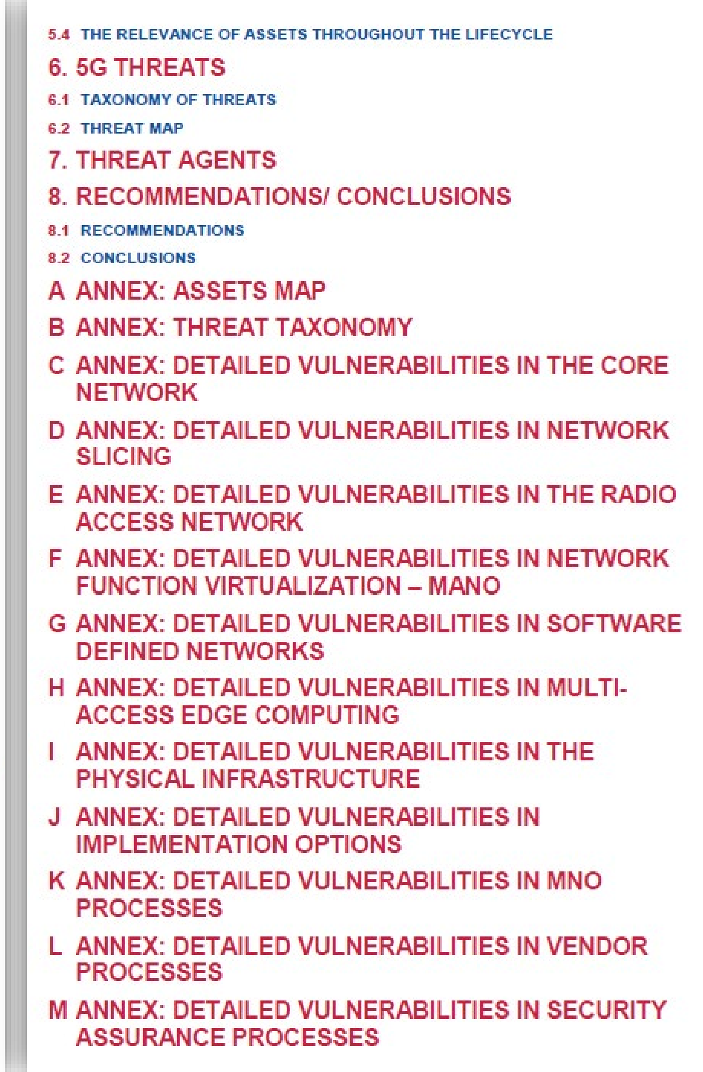
Published in November 2019 and revised in December 2020.

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020





EU Toolbox for 5G SECURITY

SA09 Enhancing cooperation, coordination and information sharing mechanisms

STUDY ON SECURITY CONTROLS IN 5G SPECS

Published in February 2021, this study discusses 3GPP security specifications relevant to 5G.

- Overview of security-related 3GPP TS and TR
- Overview of key 3GPP security features, such as protection of gNB setup and configuration, or protection of RAN interfaces
- Section-by-section description of TS 33.501 in Annex A

Security standards and specifications

Product development

Network design

Network configuration and deployment

Network operation and management

EU Toolbox for 5G SECURITY

TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards

SA04	Developing guidance on implementation of security measures in existing 5G standards

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

SECURITY IN 5G SPECIFICATIONS

Controls in 3GPP Security Specifications (5G SA)

FEBRUARY 2021

TECHNICAL DEEP DIVE INTO 5G NFV SECURITY

Published in February 2022.

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

NFV SECURITY IN 5G

Challenges and Best Practices

FEBRUARY 2022

Technical best practices			
BP-T1 Security monitoring and filtering	BP-T2 VNF Image validation and protection	BP-T3 Tracking VNF version changes	BP-T4 VNF deployment
BP-T5 VNF deletion or relocation	BP-T6 Cryptography	BP-T7 Hypervisor protection	BP-T8 Security Management and orchestration
BP-T9 Remote attestation	BP-T10 Software compliance and integrity preservation	BP-T11 Security segmentation and isolation between network functions	BP-T12 Secure boot integrity
BP-T13 Data protection and privacy	BP-T14 Encrypting VNF Volume/swap Areas	BP-T15 Trusted computing technologies	BP-T16 Hardware security
BP-T17 Centralized log auditing	BP-T18 Use and ownership of 'root' administration credentials	BP-T19 VNF protection	BP-T20 Local or removal Blade Storage – SAN protection
BP-T21 Network security	BP-T22 SDN security management	BP-T23 MANO access control and management	BP-T24 VIM connectivity to hypervisor
BP-T25 Recovery and reinstallation	BP-T26 Deploying VMs of differing trust levels	BP-T27 Orchestration platform security management	BP-T28 Trusted time source
BP-T29 Secure 3rd party hosting environments	BP-T30 Redundancy and backup	BP-T31 Specific container security controls	BP-T32 OSS/BSS protection
BP-T33 LI capabilities	BP-T34 User plane security	BP-T35 MEC security	

Policy best practices			
BP-P1 Zero Trust	BP-P2 Security Assessment of new or changes to existing VNF Service Templates	BP-P3 Vulnerability handling & patch management	BP-P4 Security testing and assurance
BP-P5 Incident management	BP-P6 Secure Update Management	BP-P7 Restriction on installing applications	BP-P8 Defense in depth
BP-P9 Strong password policy	BP-P10 Secure supply chain	BP-P11 Resources inventory management system and database	BP-P12 Apply hardening policies
BP-P13 Multi-vendors segregation and trust	BP-P14 Security by design	BP-P15 Life cycle management	BP-P16 Software Bill Of Materials (SBOM
Organisational best practices			
BP-O1 Secure Physical Environment and Geographical location	BP-O2 Training and awareness	BP-O3 Trust model	BP-O4 SLAs establishment

EU Toolbox for 5G SECURITY

SA01	**Reviewing or developing guidelines and best practices on network security**
TM04	**Increasing the security of virtualised network functions**

REPORT ON 5G CYBERSECURITY STANDARDS

Published in March 2022, this report:

- Collects cybersecurity standards *relevant* to 5G.
- Identifies gaps in standardisation and, accordingly, provides recommendations.

EU Toolbox for 5G SECURITY

TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards
SA04	Developing guidance on implementation of security measures in existing 5G standards

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

5G CYBERSECURITY STANDARDS

Analysis of standardisation requirements in support of cybersecurity policy

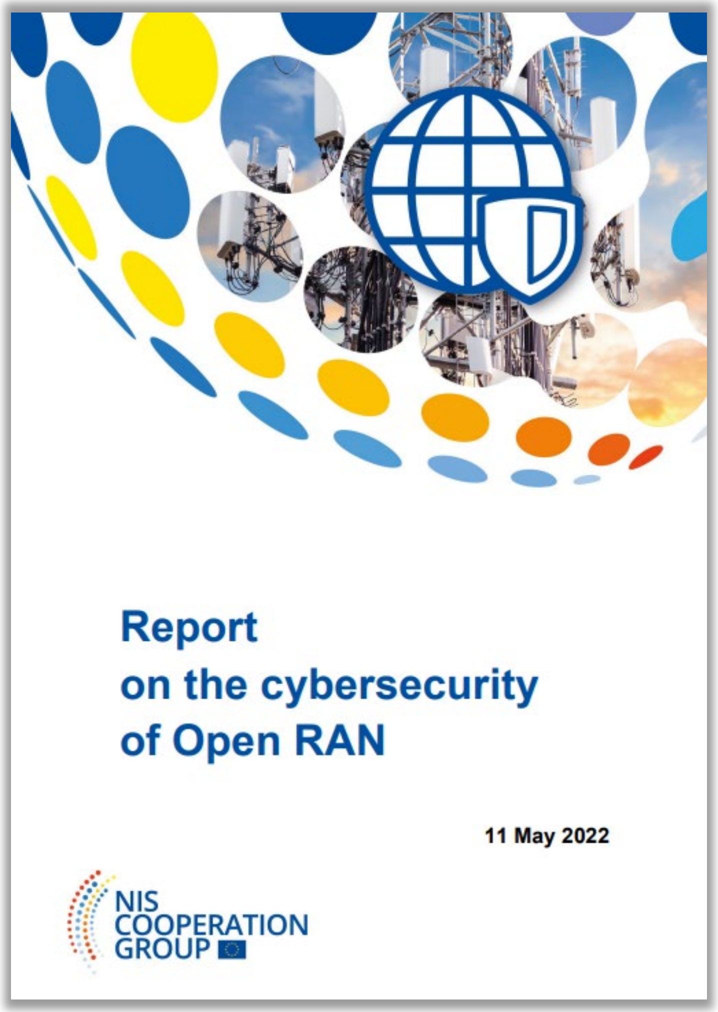
MARCH 2022

NIS CG REPORT:
CYBERSECURITY OF OPEN RAN

NIS COOPERATION GROUP

OPEN RAN REPORT

1. Assesses Open RAN **risks** through the framework of the NIS CG Coordinated Risk Assessment (October 2019):
   - Impact on existing CRA risks
   - New ‘Open RAN-specific’ risks
2. Assess OPEN RAN **opportunities** and the enabling factors.
3. Builds on the EU 5G Toolbox to provide **guidance** for Open RAN deployments.



Report on the cybersecurity of Open RAN

11 May 2022

NIS COOPERATION GROUP

5G SECURITY CERTIFICATION SCHEME

5G CYBERSECURITY CERTIFICATION SCHEME

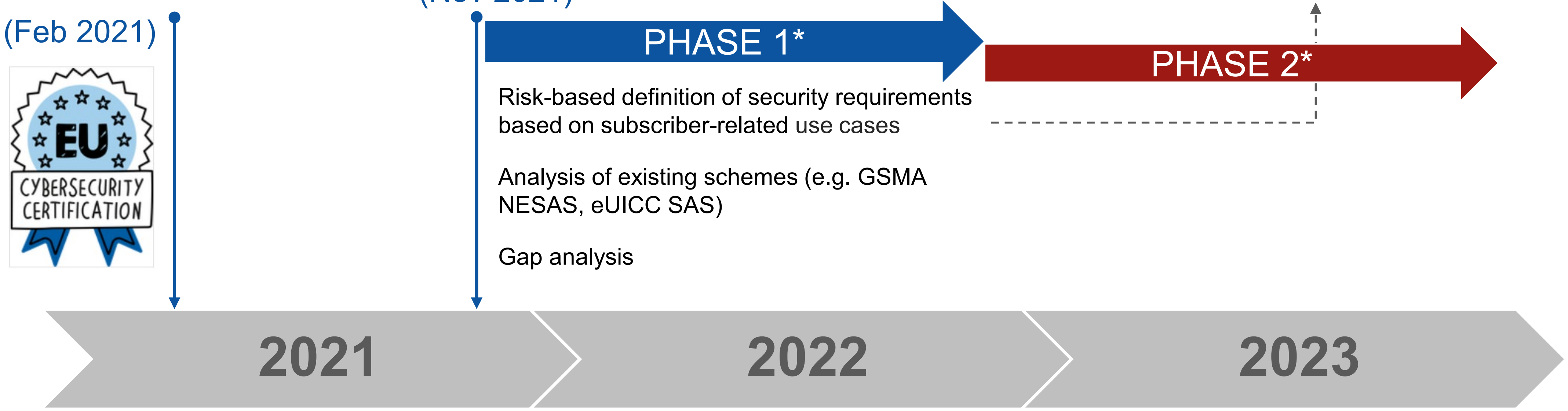
Following a request by the European Commission, on 29 November 2021, ENISA launched an ad hoc working group on EU 5G certification scheme.

https://www.enisa.europa.eu/news/enisa-news/going-full-throttle-on-cybersecurity-certification-and-market

1. The supply and deployment of identified 5G network equipment
2. Management of subscriber identities
3. Remote SIM provisioning
4. 5G authentication (incl. roaming)
5. Subscriber connectivity services

Launch of the AHWG (Nov 2021)

Commission's request (Feb 2021)



Risk-based definition of security requirements based on subscriber-related use cases

Analysis of existing schemes (e.g. GSMA NESAS, eUICC SAS)

Gap analysis

*Indicative – for presentational purposes

5G SECURITY CONTROLS MATRIX

WHAT IS THE (5G) MATRIX?

Consolidating various 5G security controls in a single repository

Numerous sources of information relevant to 5G security

3GPP

ISO

ETSI

IETF

ITU

Benefit to NRAs, telecom companies and others stakeholders

5G Security Controls Matrix

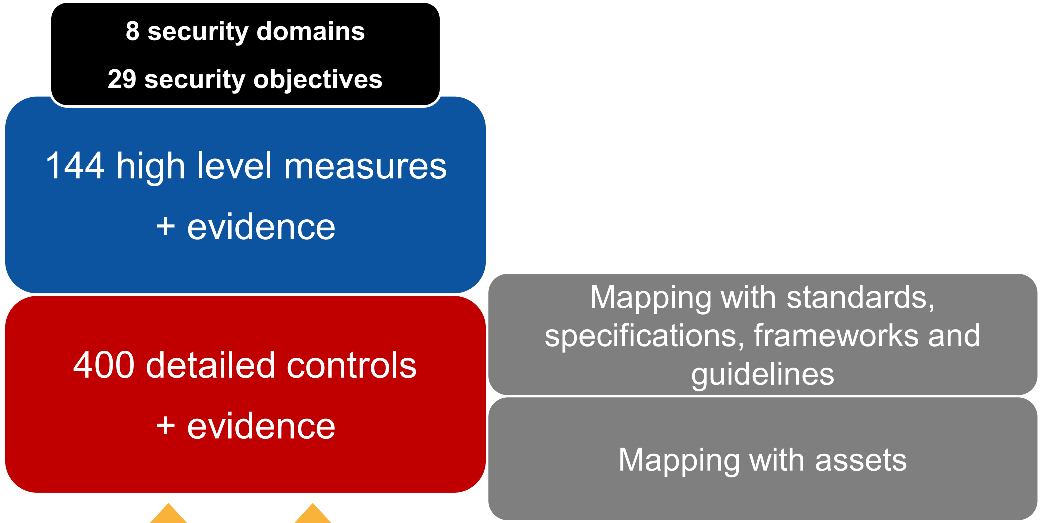
powered by ENISA

ALL CONTENTS SO FAR

GUIDELINE ON SECURITY MEASURES UNDER THE EECC

3rd Edition

DECEMBER 2020


8 security domains

29 security objectives

144 high level measures + evidence

400 detailed controls + evidence

Mapping with standards, specifications, frameworks and guidelines

Mapping with assets

NFV SECURITY IN 5G

Challenges and Best Practices

FEBRUARY 2022

5G SUPPLEMENT

To the Guideline on Security Measures under the EECC

DECEMBER 2020

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020

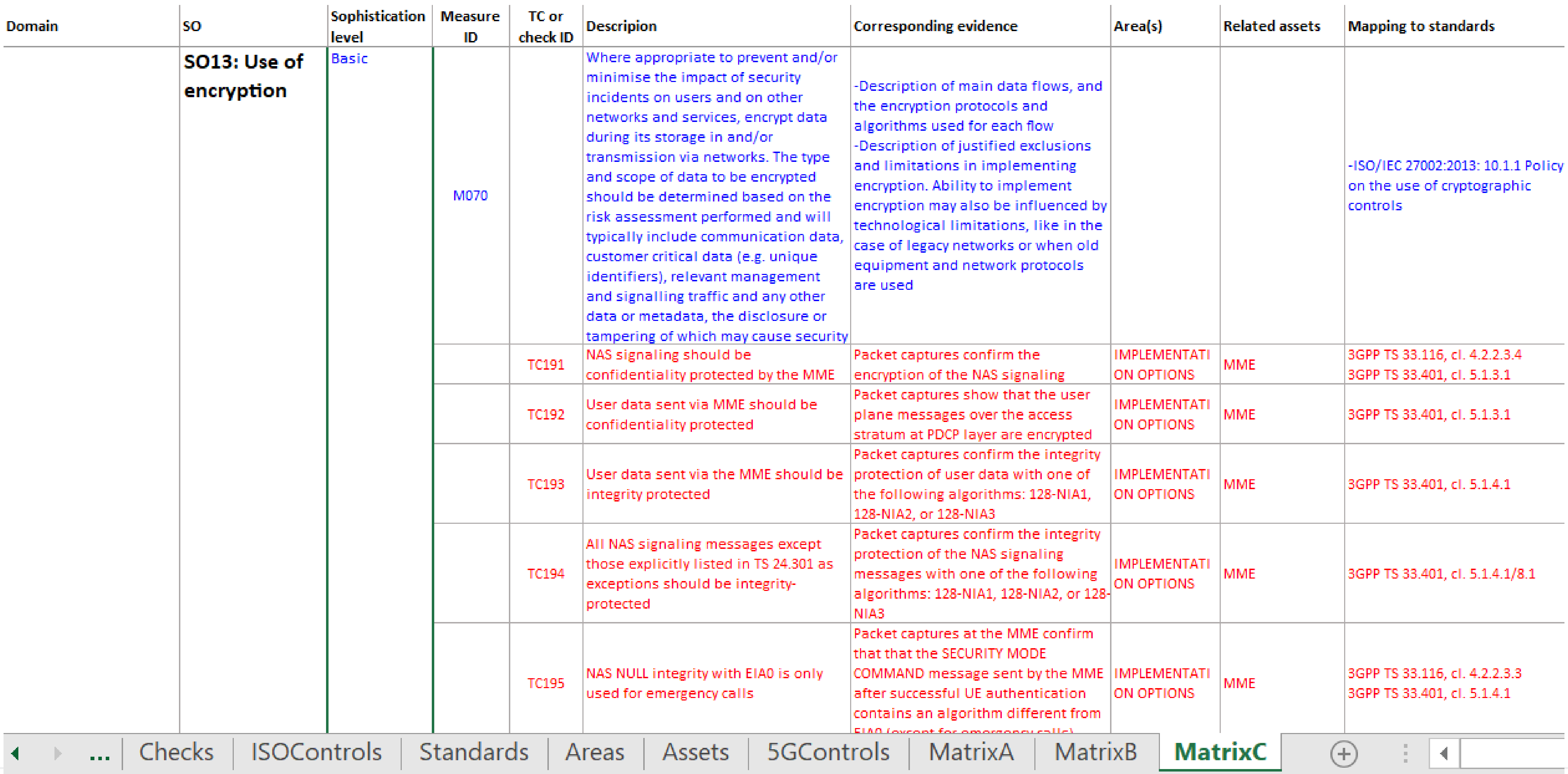
SECURITY IN 5G SPECIFICATIONS

Controls in 3GPP Security Specifications (5G SA)

FEBRUARY 2021

Additional specs not captured in the documents to the left

5G SECURITY CONTROLS MATRIX - CONTENT

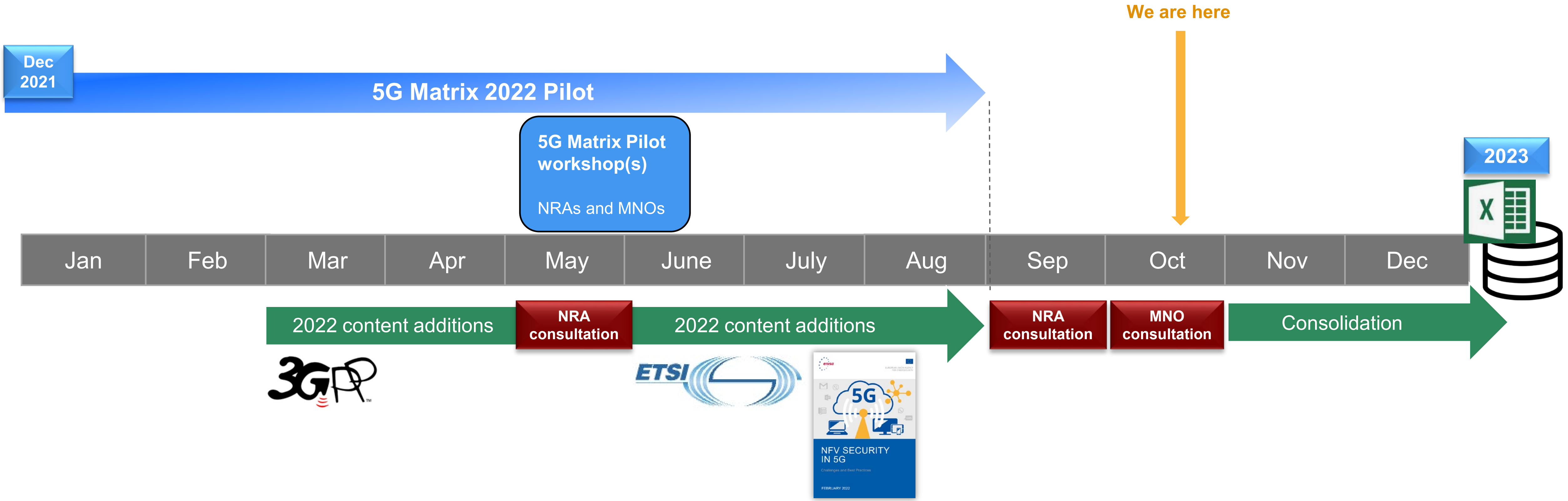


Domain	SO	Sophistication level	Measure ID	TC or check ID	Descripion	Corresponding evidence	Area(s)	Related assets	Mapping to standards
	SO13: Use of encryption	Basic	M070		Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security	-Description of main data flows, and the encryption protocols and algorithms used for each flow -Description of justified exclusions and limitations in implementing encryption. Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used			-ISO/IEC 27002:2013: 10.1.1 Policy on the use of cryptographic controls
				TC191	NAS signaling should be confidentiality protected by the MME	Packet captures confirm the encryption of the NAS signaling	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.116, cl. 4.2.2.3.4 3GPP TS 33.401, cl. 5.1.3.1
				TC192	User data sent via MME should be confidentiality protected	Packet captures show that the user plane messages over the access stratum at PDCP layer are encrypted	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.3.1
				TC193	User data sent via the MME should be integrity protected	Packet captures confirm the integrity protection of user data with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.4.1
				TC194	All NAS signaling messages except those explicitly listed in TS 24.301 as exceptions should be integrity-protected	Packet captures confirm the integrity protection of the NAS signaling messages with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.4.1/8.1
				TC195	NAS NULL integrity with EIA0 is only used for emergency calls	Packet captures at the MME confirm that that the SECURITY MODE COMMAND message sent by the MME after successful UE authentication contains an algorithm different from EIA0 (except for emergency calls)	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.116, cl. 4.2.2.3.3 3GPP TS 33.401, cl. 5.1.4.1

Sample extract

2022 TIMELINE

5G Security Controls Matrix
powered by ENISA



We are here

Dec 2021

5G Matrix 2022 Pilot

5G Matrix Pilot workshop(s)

NRAs and MNOs

2023

Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec

2022 content additions

NRA consultation

2022 content additions

NRA consultation

MNO consultation

Consolidation

THANK YOU

ALL FEEDBACK, ADVICE, IDEAS, SUGGESTIONS WELCOME

☎ +30 693 651 3974

✉ slawomir.bryska@enisa.europa.eu

🌐 www.enisa.europe.eu