

# ENISA 5G SECURITY CONTROLS MATRIX

## 1. INTRODUCTION

The ENISA 5G Security Controls Matrix is a tool for national authorities. It was delivered in response to the EU Cybersecurity Strategy and as part of ENISA's broader support for the implementation of the EU Toolbox for 5G Cybersecurity. The matrix is currently available as a spreadsheet at the following URL:

<https://www.enisa.europa.eu/publications/5g-security-controls-matrix>.

This document is a short paper to accompany the publication of the ENISA 5G Controls Matrix. It explains the background of the matrix, its goal, its contents, and how the matrix can be used in practice by national telecom authorities and even telecom operators.

## 2. BACKGROUND

In 2019 the Commission made a recommendation that requested EU Member States to take steps to secure the roll out of 5G networks. In response, the NIS Cooperation group, with the support of ENISA, delivered a [Union Coordinated Risk Assessment of 5G Networks](#), and subsequently developed an [EU Toolbox for 5G Cybersecurity](#) containing strategic measures (SM01 - SM08), technical measures (TM01 - TM11) and supporting actions (SA01 – SA10). ENISA has been supporting the Commission and EU Member States with the implementation of the strategic and the technical measures, creating several deliverables with 5G security measures and controls (see next section).

The [EU Cybersecurity Strategy](#), published at the end of 2020, directs ENISA to support the implementation of the EU's 5G toolbox by developing *a comprehensive and dynamic matrix of security controls and best practices for 5G security*<sup>1</sup>.

In 2021 ENISA started developing a 5G controls matrix in consultation and collaboration with the NIS Cooperation Group's 5G workstream and the national telecom authorities in the ENISA ECASEC expert group. Early versions of the matrix were shared with national authorities from the end of 2021 for comments and as part of the piloting phase in the first half of 2021. In the second half of 2022 we entered consultations with industry, collecting feedback on the matrix from experts working at telecom operators in the EU. We are grateful for the support and feedback received from various groups of stakeholders.

---

<sup>1</sup> See Appendix Next Steps on cybersecurity of 5G - Key objective 1.

## 3. 5G SECURITY CONTROLS MATRIX

### 3.1 GOAL

The goal of the ENISA 5G Security Controls Matrix is to support national authorities in the EU with the supervision of 5G networks in their country by developing a *single repository of technical security controls for 5G networks*, to support implementation of the technical measures in the 5G Toolbox, drawing on measures in ENISA technical papers and, where relevant, other standards and specifications (see below).

### 3.2 CONTENT

The ENISA 5G Security Controls Matrix contains **144 high level security measures from EECG Guideline with 171 high level descriptions of evidence, 399 detailed security controls with detailed descriptions of evidence, 110 asset types, two 5G architectures (with 5G and 4G core), and three cloud deployment models as well as a mapping to standards.**

The ENISA 5G Security Controls Matrix consolidates and is based on the following four technical ENISA documents:

- **ENISA 5G Threat Landscape** – First published in 2019 (as input for a Union-wide risk assessment on 5G and the 5G Cybersecurity Toolbox) and revised in 2020, the [ENISA 5G Threat Landscape](#) provides a technical overview of relevant threats for 5G networks and lists potential counter measures.
- **ENISA Guideline on Security Measures under the EECG** – ENISA maintains a telecom security framework to support national telecom authorities with the supervision of security measures taken by telecom operators. The revision of the framework, the [ENISA Guideline on Security Measures under the EECG](#), addresses the new requirements of the European Electronic Communication Code (EECC), which had come into force in December 2021.
- **5G Supplement** – The [5G Supplement](#) extends the above mentioned ENISA Guideline on Security Measures under the EECG, with more detailed additional guidance for national authorities on how to ensure mobile network operators take appropriate measures to secure their 5G networks. The 5G Supplement, together with the EECG guideline, supports Member States with implementing the 5G Toolbox technical measure TM01 and addresses the 5G Toolbox supporting action SA01.
- **Security Controls in 5G Specifications** – This ENISA paper lists different (optional and mandatory) [Security Controls in 5G Technical Specifications](#) (of 3GPP), and aims to support authorities in understanding the controls and why they are important. This ENISA paper supports Member States with implementing the 5G Toolbox technical measure TM02 and addresses the 5G Toolbox supporting action SA04.

In addition, the 5G Matrix also includes technical controls from several different standards, industry good practices and technical specifications, including 3GPP specifications, such as 3GPP 33.501, ETSI standards for component technologies, such as network function virtualisation (NFV), ISO standards on information security, such as ISO27001, good practices from GSMA, OWASP, eTom, NTIA, IEEE, NIST, ONF, CISA, OpenStack and ENISA papers on 5G.

### 3.3 USE CASES FOR THE MATRIX

We conducted a pilot study to understand better how national authorities will be using the 5G Matrix. In summary, we identified the following three use cases:

**Use case 1: NRAs use the 5G Matrix to review and update national regulation and frameworks**, for example to understand what high level security objectives to include.

**Use case 2: NRAs use the 5G Matrix to develop high-level or more technical questionnaires for operators**, for example, to follow up on an incident ex-post, or to carry out supervision ex-ante, to understand how operators work in more detail and to provide guidance to mobile network operators at the national level.

**Use case 3: NRAs use the Matrix to develop detailed technical guidance for telecom operators**, for example on a specific topic that supports operators with deploying 5G networks securely.

Additionally, several telecom operators said they would be using the 5G Matrix as input to their 5G security controls and overall architecture.

## 4. NEXT STEPS

In 2023, ENISA is taking the following next steps with regards to the 5G Security Controls Matrix:

- We are developing a webtool to improve the usability of the matrix. The plan is to deliver the webtool by the end of 2023.
- We are also extending the 5G Matrix with non-technical controls regarding, amongst others, risk management, human resources security, supplier risk management, access control policies, incident and business continuity management, based on standards such as ISO/IEC 27002, ISO/IEC 27005, ISO 22301 and NIST SP 800-53.

The 5G Controls Matrix has been set up to become a dynamic and comprehensive repository. This means that, although the bulk of the technical controls is now in place, we aim to keep the matrix up-to-date in the coming years and to extend it with controls from relevant standards and specifications where needed. The 5G Controls Matrix should therefore not be seen as a one-off delivery but rather a long-term initiative to support national authorities with their supervision of 5G networks, providing a one-stop shop for 5G security controls.

Finally, we should mention that ENISA has been developing in parallel an EU certification scheme for 5G network products, following a certification request issued by the European Commission. This request asks ENISA to develop a candidate certification scheme based on two existing industry good practices, for network equipment (GSMA NESAS) and for mobile network electronic SIMs (GSMA EUICC). In the future, when this candidate scheme is ready and adopted, the 5G Controls Matrix will be aligned with and mapped to the relevant controls in the EU 5G Certification Scheme.