Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-08

Monitoring of cybersecurity certification developments

March 2026
Version 1

MINISTERIO DE DEFENSA

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be found related. In no event can the National Cryptologic Center be held liable for direct, indirect, incidental or extraordinary damages arising from the use of the information and software indicated even when it is warned of such possibility.

LEGAL NOTICE

It is strictly prohibited, without the written authorization of the National Cryptologic Center, under the sanctions established by law, the partial or total reproduction of this document by any means or procedure, including reprography and computer processing, and the distribution of copies thereof by public rent or loan.

COURTESY TRANSLATION NOTICE

This document is provided solely as a courtesy translation. This translation has been generated using automated tools with minimal human supervision. In the event of any discrepancy, ambiguity, or conflict between this translation and the original Spanish version, the original Spanish version text shall prevail and shall be deemed the only official, authoritative, and legally binding version.

VERSION CONTROL

Version	Comments
1.0	Initial version

INDEX

1. INTRODUCTION

1. This document defines:

   a) The process by which the National Certification Authority (**NCCA**) monitors and assesses relevant developments in the field of cybersecurity certification.

   b) The dissemination of the results of this process, in the form of an annual report, aimed at contributing to the improvement of its own technical competence and capabilities of the **NCCA** and the schemes established under **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 concerning ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies** (hereinafter: **CSA**) **[CSA]** and its stakeholders.

2. CONTENT AND SCOPE OF THE FOLLOW-UP REPORT

2. The **NCCA** monitors developments in various areas to fulfil its mandate under the **[CSA]** and reflects them in an **internal annual monitoring report**. This internal report, intended to continuously improve the functioning of the Authority, is structured to include at least the following sections:

a) **Legislative and regulatory updates** — Summary of new and/or amended laws, regulations or policies at Union level (including updates or new regulations adopted under the **[CSA]**) and internationally relevant to cybersecurity certification, together with an analysis of their potential impact on the national certification framework.

b) **Developments in standards and technical criteria** — Relevant developments in standardization bodies or updates of technical criteria related to cybersecurity certification. This section covers new standards or revised standards and guidelines (e.g. assessment methodologies or security requirements) and assesses how they can influence certification practices or certificate recognition.

c) **Activities in other NCCAs —** Information on significant initiatives, procedural changes or good practices reported by **NCCAs** of other Member States. These developments are normally collected through exchanges in the European Cybersecurity Certification Group **(ECCG)** or bilateral communications, and their relevance to the Authority's own procedures or to possible harmonization efforts is examined.

d) **Results of conferences and workshops** — key conclusions of conferences, workshops or working group meetings on cybersecurity certification (e.g. international Common Criteria conferences or events organized by **ENISA**). This section includes emerging trends, recommendations or actions agreed in these forums that may affect certification schemes or evaluation techniques.

e) **Security research and alerts** — relevant findings from academic research, industry reports, or technical notices (e.g. on new vulnerabilities, threat landscape, or security technologies) that may affect certification criteria or the assurance of certified products. The report discusses how this information may require updating certification schemes or evaluation processes; in each section, the internal report not only reports on developments but also comments on their importance and, where appropriate, makes recommendations for action (e.g. updating guidelines, training needs for **NCCA** technical staff (**TA**) or adjustments to supervisory practices). In addition, a refined public version of this report is prepared, in which any sensitive or strictly internal analysis is omitted, keeping essential information on developments for communication to external stakeholders.

3. PREPARATION AND REVIEW PROCESS

3. The monitoring of developments in cybersecurity certification is a continuous activity throughout the year, which is formalized through an annual internal report. The process of collecting information and preparing the internal report includes the following steps:

a) **Continuous Information Collection** — **TA** regularly tracks defined sources of information throughout the year. It monitors official publications for legislative and regulatory changes, participates in or reviews the results of standardization committees, follows communications from other **NCCAs** (often through the **ECCG** network) and attends or reviews relevant conference documentation. It also focuses specifically on developments related to European cybersecurity certification schemes (such as updates or guidelines relating to **Implementing Regulation (EU) 2024/482 (EUCC**) or other schemes under the **CSA**) and in the relevant **ENISA** publications or **ECCG** notices.

b) **Start of the preparation of the report** — Towards the end of each year, the head of the **NCCA** unit **(JAN)** begins the preparation of the annual monitoring report. **JAN** directs the **NCCA** technical staff to consolidate all significant developments identified during the year. A timetable (usually at the beginning of the following year) is established for the drafting of the report, ensuring the inclusion of end-of-year developments. At this stage, the **JAN** may also identify areas of interest or concern to be addressed in the report.

c) **Report writing** — **TA** prepares a draft of the internal development monitoring report. The draft is structured according to the predefined sections (legislation, standards, other **NCCA** activities, events, research, etc.), collecting the information obtained. For each development or set of developments, **TA** describes the finding and analyzes its implications for the activity of the Authority (e.g., the need to update policies, possible changes in the demand for certification, or adjustments to supervisory processes). The initial draft should be completed during the beginning of the new year.

d) **Review and refinement** — The **JAN** reviews the draft report in detail, verifying the accuracy and completeness of the information and assessing the robustness of the analysis and recommendations. The draft may be forwarded to other managers or internal experts for comments on specific sections. **JAN** makes comments and requests clarifications or additions from **TA**. This iterative review process takes place over several weeks (usually in January and February), until the report reaches the required level of quality and completeness.

e) **Approval and Completion** — Once all revisions are incorporated, the **JAN** grants formal approval to the internal report. The Assistant Director-General of the **CCN** (**SGCCN**) shall be informed of the finalization of the report, providing him with a copy for strategic knowledge purposes. The final internal report will be recorded in the Information System of the National Cybersecurity Certification Authority **(SGA)** for conservation and future references.

4. COMPLETION AND DISTRIBUTION

4. Following internal approval, a public version of the follow-up report will be prepared for external dissemination. Under the direction of the **JAN**, **TA** shall remove any confidential or internal information from the approved report, ensuring that the external document focuses on factual developments and general comments. **SED** will be informed of the refined version, which is shared with the relevant external parties. In particular, the **NCCA** transmits the public report to **ENISA** and to the members of the **ECCG** (e.g. through the national representative in the **ECCG** or through an official secure channel) in accordance with Article 62(4)(f) of the **[CSA]**, in order to facilitate the exchange of information and good practices.

5. The public report may also be made available on the website of the National Cybersecurity Certification Authority **(WNCCA)** for transparency purposes, when deemed appropriate. Where possible, confirmation of receipt will be requested from external recipients and copies of the public version will be retained in the **SGA** together with the internal report. In this way, the Authority contributes to joint awareness and harmonization efforts among Member States, ensuring that results relating to developments in cybersecurity certification are shared and examined at European level.

5. REFERENCES

ACCCB	Accreditation of certification bodies for EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Accreditation of ITSEF for EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Authorisation of certification bodies and ITSEF for the EUCC scheme (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	Implementing Regulation (EU) 2024/482 of the 31 January 2024 Commission laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European criteria-based cybersecurity certification scheme common (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 laying down the circumstances, formats and procedures for notification in accordance with Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Guidelines on Vulnerability Management and Disclosure (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

6. ACRONYMS

NCCA	National Cybersecurity Certification Authority
CCN	National Cryptologic Center
EC	European Commission
CSIRT	Computer Security Incident Response Teams
ENAC	National Accreditation Body
ENISA	European Union Agency for Cybersecurity
EUCC	European cybersecurity certification scheme based on common criteria
ECCG	European Cybersecurity Certification Group
ITSEF	Information Technology Security Evaluation Facility
JAN	Head of the NCCA unit
CB	Certification Body
CAB	Conformity assessment body
CSA	Cybersecurity Regulations
SED	Secretary of State Director of the CCN
SGA	Information System of the National Cybersecurity Certification Authority
TA	Technical staff attached to the NCCA
ICT	Information and Communication Technologies
EU	European Union
VPA	Voluntary periodic audits
WNCCA	Website of the National Cybersecurity Certification Authority