Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-11

Peer review of the National Cybersecurity Certification Authority

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 the peer review procedures of the National Certification Authority **(NCCA)** in accordance with the provisions of **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification** (**CSA**) **[CSA**] and **Commission Implementing Regulation (EU) 2025/2540, of 9 December 2025 laying down detailed rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of a plan for reviews [REV].** It applies both to cases where the **NCCA** is subject to peer review and where it participates in the peer review of other **NCCAs**.

2. PEER REVIEW PROCEDURES

2.1 SUBJECT OF PEER REVIEW

2. The **NCCA** shall undergo a peer review at least once every five years. **ENISA** publishes the review schedule; the head of the **NCCA** unit **(JAN)** supervises the review cycle and, upon receipt of the notification, appoints a peer review coordinator from among the **NCCA** (**TA**) technical staff. A work order will be issued in which the **TA** will be assigned responsibilities for self-assessment, documentation collection and interview coordination.

3. At least 21 days before the on-site review, the **TA** shall submit:

   a) the completed self-assessment template;

   b) the most recent summary report in accordance with the '*ANCC-PO-01 Annual Report*';

   c) documentation on separation of duties, supervision of **CABs**, complaints handling and internal control.

4. All documentation will be submitted in English.

5. The **TA** will prepare the logistics of the on-site review (maximum three working days), coordinate access to systems and facilities and ensure that process managers are available for interviews. Interview scripts will be prepared, and all exchanges will be recorded in the Information System of the National Cybersecurity Certification Authority **(SGA)**.

6. **JAN** shall ensure that **NCCA** responds to requests from reviewers within a maximum of seven working days. At the end of the review, a closing meeting will be held with the reviewers. The **TA** shall prepare, within fourteen days, a draft response to any deviations identified in the preliminary peer review report, which shall be approved by the **JAN**. The final reports and summaries will be archived and their follow-up recorded.

7. Once the conclusions of the peer review have been received, the **JAN** will convene a review committee to analyze the recommendations and develop a plan of corrective actions to address the potential deviations identified in the review.

8. Corrective actions will be allocated to the relevant managers, recorded in a centralized register of actions such as the **SGA** and monitored quarterly. Progress will be included in the annual report for the following year. Updates to internal procedures and staff training will be triggered where appropriate.

2.2 PARTICIPATION AS PEER REVIEWER

9. The **NCCA** shall act as reviewer in at least two peer reviews per five-year cycle. Upon receiving an invitation, the **JAN** will designate, from among the qualified **TAs** based on the requirements set out by **[REV]** (with a minimum of two years of experience in the

NCCA or having participated in two peer reviews, at least as an observer, or in two reviews or Voluntary Periodic Assessments (**VPA)**), designate one or more representatives. Those representatives designated by other **NCCAs,** shall form the review team, ensuring that the review team has the necessary competences to carry out the review. Candidates shall declare the absence of conflicts of interest. The **NCCAs** under review may object to the designation.

10. The confirmed reviewers will analyze the self-assessment and the submitted documentation, coordinate their actions with the Commission, define areas of focus, conduct interviews and analyses on-site (or in hybrid mode), and document their findings. They will also contribute to the drafting of the report and ensure internal peer validation prior to its submission.

11. The reviewers will issue their report, which may be reviewed by **JAN** prior to submission. A copy of the final report and associated documentation deemed necessary and authorized by the reviewed **NCCA** shall be stored in the **SGA**. **JAN** will ensure that lessons learned are documented and, where appropriate, considered for the improvement of internal processes.

2.3 INTEGRATION OF LESSONS LEARNED AND GOOD PRACTICES

12. The **NCCA** may designate **TA** to attend peer reviews as observers, subject to the approval of the parties concerned. Observers will be able to attend interviews and review documentation, but will not make findings or conclusions. Their observations shall be recorded internally in the **SGA**.

13. The **TA** will consolidate lessons learned and recommendations derived from all reviews (own or observed). The **JAN** shall evaluate such proposals and adopt, where appropriate, relevant practices through internal instructions or procedural updates. Common guidelines or tools developed by **ENISA** or the European Cybersecurity Certification Group (**ECCG)** will be reviewed, at least quarterly, for possible adoption.

2.4 CONFIDENTIALITY, RECORDS AND REPORT

14. All documentation relating to peer reviews shall be cataloged and stored securely in the **SGA** with appropriate access controls. The **TA** shall ensure the use of secure communication channels and the deletion of draft documents after the review is completed.

15. The sanitised reports intended for publication will be reviewed by the **JAN** to verify their accuracy and the adequate level of anonymization and editing. Sanitised reports shall be archived and linked to the relevant annual report. Any personal data or sensitive information will be anonymized before dissemination.

3. 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)
REV	Commission Implementing Regulation (EU) 2025/2540 of 9 December 2025 laying down detailed rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of a plan for peer reviews (http://data.europa.eu/eli/reg_impl/2025/2540/oj)

4. 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