Content

Title：	Regulations for Testing Body and Certification Body Management of Information and Communications Equipment Used by Critical Telecommunications Infrastructure Ch
Date：	2021.01.29
Legislative：	1.Promulgated on January 29,2021
Content：	Article 1 These Regulations are promulgated pursuant to Paragraph 2 and 3, Article 87 of the Telecommunications Management Act（hereinafter the “Act”）. Article 2 The terms adopted in these Regulations are defined as follows: 1. Information and communications equipment used by critical telecommunications infrastructure（hereinafter the “Equipment”）: The equipment regulated in Technical Specifications announced by the competent authority in accordance with the Paragraph 8, Article 42 of the Act. 2. Testing Body: The institution that performs testing of the Equipment in accordance with the Technical Specifications described in the preceding subparagraph. 3. Certification Body: The institution commissioned by the competent authority to perform certification of the Equipment. The inspection items for the Equipment mentioned in Subparagraph 3 of the previous paragraph shall be announced by the competent authority. Article 3 The Testing Body shall be accredited by the Taiwan Accreditation Foundation（hereinafter the “Accreditation Organization”）and shall be capable of undertaking the tests listed in Technical Specifications announced by the competent authority. The Testing Body shall comply with the following requirements: 1. Shall be a domestic legal entity or institution established by law. 2. Compliance with CNS 17025 or ISO/IEC 17025 standards. 3. Shall not be engaged in the input, design, manufacturing or trading of the Equipment to be tested. 4. Include at least three professional and full-time personnel, consisting of one testing supervisor and two testing engineers. The personnel mentioned in Subparagraph 4 of the previous paragraph shall comply with the following requirements: 1. The Testing Supervisor shall: （1）Possess a bachelor’s degree or above, majoring in information engineering, information management or relevant department from a domestic or foreign public or private college or university recognized by the Ministry of Education. （2）Have at least five years of practical experience in cybersecurity related management or testing evaluation and understanding of regulations and technical specifications. （3）Acquire CNS 17025 or ISO/IEC 17025 training certificate. 2. The Testing Engineer shall （1）Possess a bachelor’s degree or above, majoring in information engineering, information management or relevant department from a domestic or foreign public or private college or university recognized by the Ministry of Education. （2）Have at least two years of practical experience in cybersecurity related testing evaluation. （3）Acquire a certificate of attending ISO/IEC 15408 testing and evaluation training program at least 40 hours. （4）Acquire a valid cybersecurity related professional license of Certified Ethical Hacker（CEH）or CompTIA Security+. （5）Acquire one of the following valid professional licenses related to

cybersecurity:
i. (ISC) 2 Certified Information Systems Security Professional (CISSP) .
ii. EC-Council Certified Security Analyst (ECSA) .
iii. EC-Council Computer Hacking Forensic Investigator (CHFI) .
iv. GIAC Penetration Tester (GPEN) .
v. (ISC) 2 Systems Security Certified Practitioner (SSCP) .
vi. Offensive Security Certified Professional (OSCP) .
After confirming the Testing Body meeting the requirements mentioned in the previous three paragraphs and accrediting the Testing Body, the Accreditation Organization shall submit the accreditation certificate of the Testing Body to the competent authority for reference.
In order to enforce the Technical Specifications announced by the competent authority, the Testing Body shall put in place the necessary testing equipment to perform testing work.
The competent authority may examine and audit relevant documents from the Testing Body and may also dispatch staff to the Testing Body to perform an onsite appraisal. The Testing Body shall not evade, interfere with or refuse such verification without justification.
Article 4
In any of the following circumstances, the competent authority may order the Testing Body to undertake corrective action within a prescribed period and suspend its testing work. Testing work shall only be resumed after the completion of the corrective action has been confirmed by the competent authority:
1. Failure to comply with the requirements under Paragraph 2, Article 3.
2. Failure to perform testing work in accordance with the Technical Specifications applicable to the Equipment announced by the competent authority.
3. Refusal to provide relevant documents or refusal of on-site evaluation by the competent authority staff without justification.
4. Breach of CNS17025 or ISO/IEC 17025 standards as determined by the competent authority or Accreditation Organization.
The suspension period of testing work of the Testing Body in the previous paragraph shall be at least three months. The competent authority may also extend the period to one year depending on the gravity of the situation.
Article 5
An applicant to become qualified as a certification body (hereinafter the Applicant) shall be:
1. Domestic legal entity or institution established in accordance with laws.
2. Does not engage in the input, design, manufacturing or trading of the Equipment to be certified.
3. Compliance with CNS 17065 or ISO/IEC 17065 standards.
4. Include at least two full-time certification personnel.
The certification personnel mentioned in Subparagraph 4 of the previous paragraph shall comply with the following requirements:
1. Possess a bachelor’ s degree or above, majoring in information engineering, information management or relevant department from a domestic or foreign public or private college or university recognized by the Ministry of Education.
2. Have at least five years of practical experience in cybersecurity related management or testing evaluation and understanding of regulations and technical specifications.
3. Acquisition of CNS 17065 or ISO/IEC 17065 training certificate.
4. Acquire one of the following valid professional licenses related to cybersecurity:
(1) (ISC) 2 Certified Information Systems Security Professional (CISSP) .
(2) EC-Council Certified Security Analyst (ECSA) .
(3) EC-Council Computer Hacking Forensic Investigator (CHFI) .
(4) GIAC Penetration Tester (GPEN) .
(5) (ISC) 2 Systems Security Certified Practitioner (SSCP) .
(6) Offensive Security Certified Professional (OSCP) .
5. No personnel shall also serve as personnel under Subparagraph 4, Paragraph 2, Article 3.
Article 6
The Applicant shall submit the following documents with its application to

the competent authority:
1. Critical Telecommunications Infrastructure Information and Communications Equipment Certification Body Application Form (as Attachment 1).
2. Photocopy of corporate or business registration documents.
3. Photocopy of CNS 17065 or ISO/IEC 17065 certificate acquired by the Applicant.
4. Basic information of certification personnel showing compliance with the qualifications as prescribed in Paragraph 2 of the preceding Article.
5. Organization chart and function introduction of the certification department.
6. Quality manual of the certification department.
7. A list of quality documents of the certification department.
8. Inspection procedure for the Equipment to be certified.
9. Other materials designated by the competent authority.
Where the Applicant fails to provide all of above-mentioned documents or the content of provided document is incomplete, corrections shall be made within the period prescribed by the competent authority. If the submitted documents remain incomplete or insufficient, the application will be rejected.
The period as described in the preceding paragraph shall not be longer than one month.
Attachment 1 Critical Telecommunications Infrastructure Information and Communications Equipment Certification Body Application Form.pdf
Article 7
Where all documents submitted by the Applicant according to the preceding article are approved, the competent authority will conduct an on-site evaluation.
The said evaluation shall be conducted according to the following terms and conditions, and an evaluation report shall be provided accordingly:
1. CNS 17065 or ISO/IEC 17065 standards.
2. Technical Specifications applicable to the Equipment announced by the competent authority or national standards.
3. Other matters related to the on-site evaluation requested by the competent authority.
Where the on-site evaluation results indicate any non-conformity to the preceding paragraph, the competent authority shall list all of them and notify the Applicant to make corrections accordingly. The Applicant shall make corrections and submit an improvement report within the prescribed period. If not, the application will be rejected.
The period as prescribed in the preceding paragraph shall not exceed three months.
Article 8
The Applicant shall carry out Equipment inspection work only after it passes the evaluation, signs a commissioned inspection contract for the Equipment with the appraisal (hereinafter the “Commissioned Inspection Contract”) and after the acquires an accreditation certificate for Certification Body of Equipment (hereinafter the “Accreditation Certificate”, as shown in Attachment 2) issued by the competent authority.
Attachment 2 Accreditation Certificate for Certification Body of Information and Communications Equipment used by Critical Telecommunications Infrastructure.pdf
Article 9
The Certification Body shall not refuse or make discrimination on any of application for Equipment inspection (hereinafter an “Inspection Case”) without justification.
Certification Bodies and their certification personnel must not engage in any work related to assisting the manufacturer or adjusting the functions of the Equipment.
The Certification Body shall process Inspection Cases in the name of the Certification Body.
The testing reports for Inspection Cases under the previous paragraph shall be issued by a Testing Body that has been accredited by the Accreditation Organization.
Article 10
The Certification Body shall process the issuance, renewal, reissue,

revocation or annulment of of inspection certificates of the Equipment (hereinafter the “Inspection Certificates”), rejection of inspection application or approval for change of the appearance of the approved Equipment, etc., according to the Technical Specifications for Security Testing of Information and Communication Equipment for Critical Telecommunications Infrastructure.
All information of each Inspection Case shall be reported to the competent agency within 10 days after the completion of the said work for reference.
The competent agency shall instruct the Certification Body to sample the Equipment of installers of critical telecommunications infrastructure when necessary. The Certification Body shall report results of all sampling cases to the competent authority within two months after the sampling day.
The Equipment to be inspected under the previous paragraph shall be provided by the installer of critical telecommunications infrastructure.
Article 11
If the Certification Body submits an application to add an inspection item for certification of the Equipment, the application shall be submitted in accordance with Article 6 and the Accreditation Certificate shall be reissued. The validity of the new Accreditation Certificate shall be identical to the original certificate.
The competent authority may perform an on-site evaluation in accordance with Article 7 when it processes an application under the previous paragraph.
If there are any changes of the specifications in an Accreditation Certificate, other than adding item mentioned in the first paragraph, an application for reissue of the Accreditation Certificate shall be submitted to the competent authority within 15 days from the date of the change. The validity period of the new Accreditation Certificate shall be identical to the original certificate.
If any certification personnel of the Certification Body is absent or added, information about the personnel change shall be submitted to the competent authority for reference within 15 days from the date of change.
The competent authority may order the Certification Body to suspend relevant inspection work when the position of the certification personnel is vacant and leads to non-conformities as described in Subparagraph 4, Paragraph 1, Article 5. The Certification Body shall apply to the competent authority for resuming the conduction of certification by submitting the basic information of the certification personnel after above-mentioned vacancy has been filled.
Article 12
The competent agency may dispatch personnel to the certification body for irregular inspections and the Certification Body must not refuse it.
Article 13
The duration of Commissioned Inspection Contract shall be three years.
The Certification Body may apply for renewal within two months starting from three months prior to the expiry of the Commissioned Inspection Contract. The competent authority may undertake a review and evaluation as required in accordance with Articles 6 and 7.
The competent authority shall notify the Certification Body one month prior to the expiry of the Commissioned Inspection Contract that the Certification Body shall no longer accept Inspection Cases. The Certification Body shall complete all accepted Inspection Case within one month from the date of the notification.
Article 14
The competent authority may terminate the Commissioned Inspection Contract in any of the following circumstances and order the Certification Body to return and annul its accreditation certificate:
1. Failure to comply with terms and conditions of Paragraph 1, Article 5.
2. Violation of Paragraph 2 of Article 9, Article 10, Article 11 or Article 16.
3. Where the Certification Body performs inspection activities beyond the scope of authority as prescribed in the Commissioned Inspection Contract or shows tardiness to perform the said activities.
4. Where the Certification Body refuses irregular inspections conducted by competent authority without any justifiable reason.
5. Violation of any legislation such as the Act, Administrative Procedure

Act, Technical Specifications for Security Testing of Information and Communication Equipment for Critical Telecommunications Infrastructure or the Regulations.
6. Where the Certification Body rejects or makes discrimination on accepted Inspection Case without any justifiable reason.
7. Where the Inspection Certificate issued by the Certification Body contains false or incorrect information.
In the case of any event under Subparagraphs 1 to 4 of the previous paragraph, the competent authority may order the Certification Body to undertake corrective action within a prescribed period. Those who fail to make corrections within the prescribed deadline will be handled according to the preceding paragraph.
Article 15
When a Commissioned Inspection Contract is terminated in accordance with the previous article, the Certification Body shall forward uncompleted Inspection Cases to the Certification Body designated by the competent authority.
The Certification Body shall forward complete information related to all Inspection Cases within 7 days from the end of the Commissioned Inspection Contract.
Certification Body that has the Commissioned Inspection Contract terminated due to circumstances described in the previous article must not become a Certification Body within one year after the termination of the said Contract.
Article 16
The Certification Body shall establish an online application system within one year from the date of acquisition of the Accreditation Certificate described in Article 8 to accept applications of the inspection of Equipment.
Article 17
The Certification Body shall charge an inspection fee from the applicant according to charging standards set by the competent authority, and transfer the entire amount to national treasury the next day. The competent authority will pay the outsourcing fee to the Certification Body according to the Commissioned Inspection Contract.
Article 18
These Regulations shall take effect upon the date of promulgation.