SEMI E187 Cybersecurity Specification for Fab Equipment Certification Scheme

V1.0

2026/03/23

Table of Contents

Document Revision History

Establishment/Revision Date	Revised Pages	Summary of Changes	Revised Version
2026.03.23	N/A	Initial Release	1.0

1. Overview of the Certification Scheme

1.1 Purpose

SEMI E187 Cybersecurity Specification for Fab Equipment Certification Scheme (hereinafter referred to as "the Scheme")

The Scheme is jointly owned by the Administration for Digital Industries, Ministry of Digital Affairs, and SEMI (hereinafter collectively referred to as "the Scheme Owner"). It aims to establish a consistent and credible certification scheme as a core foundation for promoting cybersecurity management of semiconductor equipment in Taiwan. Through the Scheme, we seek to strengthen overall supply chain security and enhance the international competitiveness of the domestic industry.

1.2 Scope of Application

The Scheme applies to equipment products within the semiconductor equipment supply chain and governs certification-related activities involving Certification bodies, Laboratories, and Applicant. Accreditation Bodies participate in the Scheme in accordance with their respective roles and responsibilities.

1.3 Applicable Standards

A testing requirements developed based on the "SEMI E187 – Specification for Cybersecurity of Fab Equipment.

1.4 Principle of Impartiality and Non-Discrimination

The implementation of the Scheme shall follow the principles of impartiality and non-discrimination. Applicant shall not be treated differently based on their size, affiliation, financial status, social standing, or other factors unrelated to cybersecurity capability. Certification Body and Laboratories shall ensure consistency and objectivity throughout the acceptance, assessment, testing, review, and certification processes, in order to maintain the credibility of the Scheme.

2. Definitions

2.1 Accreditation

Refers to the formal qualification assessment procedure conducted by an Accreditation Body on a Certification Body or Laboratory to demonstrate its competence to perform certification activities.

2.2 Certification

Refers to the procedure in which a Certification Body, in accordance with the Scheme, conducts conformity assessment, review, and certification decision on equipment, and issues the Certificate of Conformity accordingly.

2.3 Semiconductor Equipment

Refers to electromechanical integrated systems that directly participate in semiconductor manufacturing processes and possess control, processing, measurement, or handling functions, including their embedded control systems and network communication modules. The detailed definition and applicable scope shall be based on the content of the SEMI E187 Standard for Cybersecurity of Semiconductor Manufacturing Equipment.

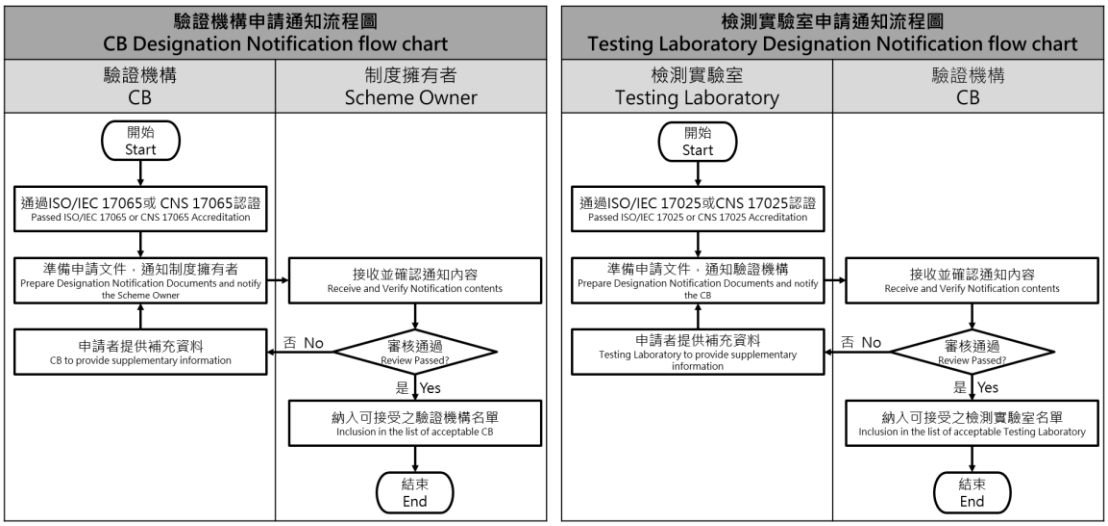
2.4 Application

Refers to (1) the testing application submitted by an equipment manufacturer or equipment supplier to a Laboratory in compliance with the Scheme, serving as a prerequisite process for verification activities, and (2) the certification application submitted to the Certification Body after obtaining the test report issued by the Laboratory.

2.5 Designation Notification

Refers to the process in which a Certification Body or a Laboratory, after obtaining accreditation from the Accreditation Body in accordance with ISO/IEC 17065 or ISO/IEC 17025, or their corresponding national standards (CNS 17065 or CNS 17025), submits its accreditation certificate and basic information to notify the Scheme Owner or the Certification Body for inclusion in the list of accepted Certification Bodies or Laboratories. The Scheme Owner or the Certification Body shall rely solely

on the accreditation results issued by the Accreditation Body when publishing such lists and shall not conduct any qualification or competence assessment of the Certification Bodies or Laboratories. The relevant notification process is described below.



2.6 Suspension

A decision to temporarily suspend, for a specified period, all or part of the scope of certification that Applicant has obtained under the Scheme.

2.7 Termination

A formal decision, under certain conditions, to end a valid relationship, certification contract, or qualification. From the date of termination, the rights and obligations of both parties shall cease.

2.8 Revocation

A decision made when a party violates the certification requirements under the Scheme, resulting in the loss—retroactive to its origin—of the certification previously granted.

3. Management of the Scheme

3.1 Roles and Responsibilities in the Scheme

3.1.1 Scheme Owner

The Scheme is jointly maintained and managed by the Administration for Digital Industries, Ministry of Digital Affairs, and SEMI. Both parties jointly retain the rights to revise, update, and provide the final interpretation of the Scheme, however, they shall not intervene in or influence the certification decisions made by the Certification Body.

The Scheme Owner may, as needed, invite representatives from Accreditation Body, Certification bodies, Laboratories, and industry experts to establish a Scheme Management Committee to perform management activities related to the Scheme. The organizational charter of the Scheme Management Committee shall be established and maintained as a separate document.

3.1.2 Accreditation Body

In the Scheme, the Accreditation Body refers to the Taiwan Accreditation Foundation (TAF), which is responsible for accrediting Certification Bodies and Laboratories to ensure their competence in performing assessments and testing in accordance with the SEMI E187 standard.

3.1.3 Certification Body

An organization accredited by the Accreditation Body to carry out certification activities. The body shall maintain impartiality in its operations and may issue Certificate of Conformity.

Responsibilities are as follows:

(1). Manage the overall conformity assessment process;

(2). Receive the application submitted by the Applicant;

(3). Where applicable, engage accredited laboratories certified under ISO/IEC 17025 or CNS 17025 to perform testing;

(4). Assessment and review test reports and make certification decisions;

(5). Issue Certificates of Conformity;

(6). Conduct necessary technical performance monitoring of Laboratories' testing activities to ensure continued conformity with the requirements of the Scheme.

3.1.4 Laboratory

A unit that accepts applications from equipment manufacturers or equipment suppliers and provides cybersecurity testing services to Applicant.

Responsibilities are as follows:

(1). Conduct equipment cybersecurity testing and inspection in accordance with the requirements of the SEMI E187 standard.

(2). Provide a test report based on the test results.

(3). May provide administrative assistance to the Applicant during the preparation of certification application materials, but shall not submit the application on behalf of the Applicant, and shall not affect the independence and impartiality between the Laboratory and the Certification Body.

3.1.5 Applicant

Refers to an equipment manufacturer or supplier who provides technical documents and samples, and is required to apply for certification from a Certification Body. Upon approval, a Certificate of Conformity will be granted.

3.2 Establishment or Revision of the Scheme

3.2.1 Scheme Owners reserves the rights to revise, update, and provide the final interpretation of the Scheme.

3.2.2 The period from the approval of the draft for establishment or revision to its implementation shall be considered a grace period. The Certification Body shall use this period to address changes and assess and adjust the affected areas accordingly.

3.2.3 The duration of the grace period shall depend on the scope and nature of the changes and shall be no less than six months. The Certification Body shall, within 20 working days following the announcement of any revisions or updates, proactively notify its designated Laboratories of the latest requirements of the Scheme.

3.3 Qualifications of Certification Body

3.3.1 A legitimate entity with certification and the following professional competency requirements:

(1). Accredited by the Accreditation Body based on ISO/IEC 17065 or CNS 17065 standards.

(2). At least one certification of semiconductor equipment cybersecurity functional specification verification.

3.3.2 Certification Body shall complete the Designation Notification under the Scheme and comply with the management requirements of the Scheme.

3.4 Qualifications of Laboratory

3.4.1 Laboratories established by a legal entity or organization in Taiwan, after being accredited under ISO/IEC 17025 or CNS 17025, shall submit the Designation Notification to the Certification Body and obtain legal authorization to use the SEMI E187 standard under the Scheme. And the Laboratories shall cooperate with the Certification Body in the necessary technical performance monitoring of its testing activities to ensure continual conformity with the requirements of the Scheme.

Such technical performance monitoring is unrelated to the Laboratory’s accreditation status, which shall be determined solely by the Accreditation Body in accordance with ISO/IEC 17025 or CNS 17025.

3.4.2 If the Laboratory's accreditation is suspended or revoked as a result of technical competence assessment conducted by the Accreditation Body, or if the Certification Body determines through technical performance monitoring that the Laboratory's testing activities no longer conform to the Scheme requirements and cooperation must be discontinued, the Laboratory shall comply with the relevant actions and any required public announcements. The Certification Body shall inform the Scheme Owner and the Accreditation Body of the relevant follow-up arrangements and outcomes for governance and coordination purposes.

3.4.3 If any disposition results occur during the Laboratory's surveillance or assessment period conduct by the Accreditation Body, the Laboratory shall proactively notify the Certification Body and cooperate with the related actions.

3.5 Management of Certification Body

3.5.1 The Certification Body shall establish the necessary management procedures to ensure that certification decisions are not influenced by the Scheme Owner or other interested parties, and shall report annually to the Scheme Owner and the Accreditation Body on the number of certifications, surveillance activities, and any issues affecting impartiality.

3.5.2 The Certification Body shall independently conduct certification activities in accordance with the requirements of the Scheme, including performing assessment, review, and post-market surveillance, and shall make independent decisions on granting, maintaining, extending, suspending, or withdrawing certificates.

3.5.3 The Certification Body may implement certification programs outside the scope of the Scheme, but shall ensure clear distinction between different certification programs and avoid any conflicts of interest or ambiguity in scope.

3.5.4 The Certification Body shall cooperate with periodic surveillance assessments conducted by the Accreditation Body. In the event of suspension, termination, or revocation, the Certification Body shall

immediately notify the Scheme Owner.

3.5.5 The Certification Body shall maintain documented records, resources, and capabilities that comply with the Scheme and the requirements of surveillance assessments by the Accreditation Body, and personnel qualified under the Scheme shall be designated to communicate and coordinate with Scheme Owners.

3.5.6 Certification Body shall conduct certification activities in accordance with the Scheme. For special or disputed cases, the Certification Body may invite a technical team to participate in the review and provide professional recommendations, ensuring impartiality and consistency of certification process, provided such personnel do not participate in certification decisions.

3.5.7 Complaints, appeals, and dispute resolution processes arising from certification activities shall be documented, and such records shall be provided upon request by Scheme Owners.

3.5.8 The reports and process records generated during certification activities are considered confidential documents. They shall be used solely by the Applicant, Laboratory, Certification Body, Accreditation Body, within the scope and purpose of activities under the Scheme, or may be provided to other parties only with the prior written consent of the aforementioned entities. They may be provided to Scheme Owners only in aggregated or non-confidential form, or with Applicant consent.

3.5.9 Upon obtaining the approval of the Scheme Owner, the Certification Body shall, at least once every three (3) years, be audited by the Scheme Owner or the Scheme Management Committee to assess the Scheme implementation by the CB (not the technical competence of the CB). This audit is an ongoing process beyond the accreditation by the Accreditation Body with the focus on the Scheme implementation as opposed to the technical competence of the Certification Body.

If the Certification Body is found unable to fulfill the requirements of the Scheme, the Scheme Owner or the Scheme Management Committee may, after deliberation, take necessary actions and suspend

cooperation with the Certification Body, and shall notify the Accreditation Body of the actions taken. The actions to be taken by the Scheme Owner may include termination, suspension, or revocation.

3.5.10 The Certification Body shall establish a clear and transparent appeals mechanism with defined timelines for acceptance and response, ensuring that all appeals are handled in a fair, objective, and procedurally proper manner. The relevant appeals procedure shall also be made publicly available.

3.6 Human Resources of Certification Bodies

3.6.1 Certification Body shall have sufficient personnel and resources to support certification activities. Its organizational structure shall include assessors, reviewers, and certification decision-makers.

3.6.2 Personnel responsible for assessing test reports shall hold at least a bachelor's degree, have completed 6 hours of cybersecurity-related courses, possess more than 1 year of relevant cybersecurity work experience, and have participated in at least 1 assessment case in the field.

3.6.3 Personnel responsible for reviewing assessment reports and making certification decisions shall hold at least a bachelor's degree, have completed at least 9 hours of cybersecurity-related courses, possess more than 3 years of relevant cybersecurity work experience, and have participated in at least 1 review case in the field.

3.6.4 The Certification Body shall maintain and regularly update a list of personnel performing activities under the Scheme, and retain all records related to their participation.

3.6.5 The Certification Body shall ensure that the initial qualification training for personnel performing assessment, review, and certification decision activities is delivered by instructors or institutions with practical experience in related cybersecurity field. Subsequent periodic training may be conducted internally by the body. The total duration of annual training shall be no less than 6 hours.

3.6.6 The Certification Body shall establish personnel training and performance evaluation procedures. The promotion of new assessors to formal assessors shall include a review process involving participation in actual assessment cases.

3.6.7 Before becoming a formal assessor, new assessors shall be assisted and guided by formal assessors of The Certification Body, fully participate in the execution of assessments during certification activities, and maintain training records.

4. Equipment Certification Process

4.1 General Provisions

4.1.1 The Scheme defines the overarching operational framework. Detailed procedures for application, modification, maintenance, extension, termination, and revocation shall be governed by the official procedural documents issued by the Certification Body.

4.1.2 The Certificate of Conformity shall remain valid for three years and the Certification Body shall conduct post-market surveillance at least ***once*** every three years to ensure its continued validity.

4.1.3 The Certification Body shall, in accordance with the Scheme, assign qualified personnel to perform assessment, review, and certification decision activities.

4.1.4 It is prohibited for any applicant to submit equipment certification, modification, or extension applications on behalf of another company without proper authorization.

4.1.5 Personnel making certification decisions for any equipment, including initial application, modification, maintenance, extension, suspension, termination, or revocation, shall not, within one year, have been involved in the testing of the same equipment.

4.2 Initial Application

4.2.1 For equipment applying for SEMI E187 certification, the Applicant shall ensure that the application documents are prepared and submitted to the Certification Body. Upon successful review and approval, the Certification Body shall issue a Certificate of Conformity.

4.2.2 When necessary, the review process may include on-site inspections at the Laboratory issuing the test report or at the Applicant’s premises.

4.3 Change Application

4.3.1 When any modification occurs to the equipment that has been granted a Certificate of Conformity, regardless of the nature of the change, the

Applicant shall ensure that a change application is submitted to the Certification Body, which will determine if a formal change application is required.

4.3.2 If the proposed change to the equipment does not involve cybersecurity functions, and the Certification Body verifies that the change is appropriate, the Certificate of Conformity may be updated accordingly.

4.3.3 If the proposed change to the equipment involves cybersecurity functions, the Certification Body shall assess its impact on the original certification decision. In cases where the impact is significant (e.g., changes to technical methods implementing cybersecurity functions), supplementary testing by the Laboratory shall be conducted before the Certificate of Conformity can be updated.

4.3.4 If the equipment undergoes major changes to its core functionality or security module design, it shall be regarded as a new application rather than a change request.

4.4 Extension Application

4.4.1 Applicants requesting an extension shall prepare the application documents and submit them to the Certification Body.

4.4.2 The Applicant shall submit the extension application for the Certificate of Conformity to the Certification Body within the period specified by the Certification Body. If the extension is not applied for before the expiry of the validity period, the Certificate of Conformity shall no longer remain in use, and the equipment shall undergo a new certification process.

4.4.3 Equipment applying for extension shall not include changes that materially affect cybersecurity functions or the basis of the original certification. The Certification Body shall verify and determine the impact on the certification results. When necessary, the Certification Body may conduct an on-site inspection or request the Applicant to provide samples, and the Applicant shall not refuse.

4.4.4 Upon approval of the extension application, the Certification Body

may extend the validity of the original certificate once and revise the Certificate of Conformity accordingly. Any subsequent extension applications shall be regarded as new applications.

4.5 Termination, Suspension, and Revocation

4.5.1 When the prerequisites for certification have changed, or new evidence emerges that may affect the accuracy of the original certification decision, the Certification Body shall review and, if necessary, adjust, amend, or revoke the previously issued Certificate of Conformity.

4.5.2 If an Applicant is found to have obtained certification through illegal or improper means, the Certification Body, upon verification of the facts, shall impose suspension, termination, or revocation of the certification.

4.5.3 If, after obtaining the Certificate of Conformity, the Applicant's improper use causes or is likely to cause damage to the rights, interests, or reputation of the Scheme Owner or other stakeholders, the case shall be reported to the Certification Body. The Certification Body shall make an independent decision based on severity, ensuring impartiality.

5. Management of Post-Market Surveillance

5.1 The Certification Body shall conduct post-market surveillance at least once every three years for equipment holding a valid Certificate of Conformity, in accordance with the risk level and technical requirements of this Scheme. The Applicant shall not evade, obstruct, or refuse such surveillance without justified reason.

5.2 The purpose of post-market surveillance is to ensure that the equipment continues to conform to the SEMI E187 standard throughout the validity period of the Certificate of Conformity.

5.3 Post-market surveillance may include, but is not limited to, the following activities and is not restricted to the methods used during initial certification:

(1) Review of documents and records;

(2) Sample-based verification of laboratory testing;

(3) On-site inspections;

(4) Partial or supplemental testing based on risk;

(5) Review of updated risk assessments and risk management measures.

5.4 To maintain the validity of the Scheme, if any nonconformities are found during the post-market surveillance, the Certification Body may, depending on the severity of the nonconformity, increase surveillance frequency, apply restrictions on certificate use, or suspend or revoke the Certificate of Conformity.

5.5 The review and certification decisions related to post-market surveillance shall be carried out by qualified personnel in accordance with ISO/IEC 17065 or CNS 17065, and all assessment and decision records shall be maintained to ensure the continued validity of the Certificate of Conformity.

5.6 Detailed requirements and procedures for post-market surveillance shall be defined and maintained in the official operational documents issued by the Certification Body.

6. Supplementary Provisions

6.1 Any matters not specified in the Scheme shall be handled in accordance with the relevant ISO/IEC international standards.

6.2 For the initial issuance of the Scheme, the grace period shall be determined separately by the issuing authority and shall not be subject to the provisions of Clause 3.2.3.