CCC SP-151-1



Cybersecurity Labelling Scheme for IoT
Publication No. 1

Overview of the Scheme

April 2025
Version 1.4

FOREWORD

The Cybersecurity Labelling Scheme for IoT [CLS(IoT)] is part of Cyber Security Agency's (CSA) efforts to better secure Singapore's cyberspace and to raise cyber hygiene levels. It aims to improve security awareness by making security provisions more transparent to consumers and empowers consumers to make informed purchasing decisions for products with better security using the information on the cybersecurity label.

Under the CLS(IoT), the cybersecurity label provides an indication of the level of security in the network-connected smart devices.

The CLS(IoT) seeks to incentivise manufacturers to develop and provide products with enhanced cybersecurity provisions. The labels also serve to differentiate smart devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS(IoT) with the objective of eliminating duplicated assessments across national boundaries.

The CLS(IoT) is an initiative under the Safer Cyberspace Masterplan, to create a safer cyberspace and protect the public and enterprises against cyber threats, as Singapore moves towards a Digital Economy and Smart Nation.

The CLS(IoT) is owned and managed by the Cybersecurity Certification Centre (CCC), under the ambit of the Cyber Security Agency of Singapore (CSA).

AMENDMENT RECORD

Version	Date	Author	Changes
1.0	October 2020	Cyber Security Agency of Singapore	Release
1.1	April 2021	Cyber Security Agency of Singapore	Included assurance continuity requirements
1.2	October 2022	Cyber Security Agency of Singapore	Revised framework
1.3	September 2023	Cyber Security Agency of Singapore	Revised process
1.4	April 2025	Cyber Security Agency of Singapore	Revised process

CONTENTS

1 INTRODUCTION 5

2 BACKGROUND 6
2.1 Impetus for CLS(IoT) 6
2.2 Baseline Security in Consumer Products 6

3 ORGANISATION AND MANAGEMENT OF CLS(IOT) 8

4 OVERVIEW OF THE CLS(IOT) 9
4.1 Overview 9
4.2 Cybersecurity Labelling Levels 9

5 CYBERSECURITY LEVELS 10
5.1 Overview of CLS(IoT) Cybersecurity Levels 10
5.2 CLS(IoT) Level 1 – Security Baseline Requirements 10
5.3 CLS(IoT) Level 2 – Adherence to International Standards 11
5.4 CLS(IoT) Level 3 – Lifecycle Requirements and Software Binary Analysis 12
5.5 CLS(IoT) Level 4 - Penetration Testing 13

6 GENERAL PROCESS FOR LABELLING OF INTERNET-CONNECTED DEVICE 15
6.1 Process Overview 15
6.2 Pre-Application Phase 20
6.3 Application for Labelling 20
6.4 Declaration of conformity 21
6.5 Task Kick-off Meeting (TKM) 22
6.6 Testing Phase (Only for Level 3 onwards) 22
6.7 Conclusion - Awarding of the CLS(IoT) Label 22
6.8 Changes to Conditions for Labelling 22
6.9 Cryptography 23

7 GROUPING OF APPLICATIONS 24

8 APPLICANT OBLIGATIONS 25
8.1 Vulnerability Disclosure 25
8.2 Defined Support Period for Security Updates 25

9 MUTUAL RECOGNITION 26

10 ASSURANCE CONTINUITY 27

11 RENEWAL OF LABEL 27

12 REQUIREMENTS FOR CLS(IOT) TEST LABORATORY 28

13 CYBERSECURITY LABEL 29
13.1 Label 29

13.2 Label Validity 29
13.3 Requirements of the Cybersecurity Label....29
13.4 How the Cybersecurity Label is to be Affixed or Displayed....30
13.5 Labelling Principles....30
13.6 CCC Audit and Testing....31

14 USE OF PROTECTIVE MARKS, LOGOS AND ADVERTISEMENT 32
14.1 Advertisement and promotion of labelled devices 32
14.2 Response to Misuse 33

15 REVOCATION, TERMINATION AND WITHDRAWAL 34
15.1 Revocation of the Cybersecurity Label 34
15.2 Termination of On-Going Applications 35
15.3 Withdrawal from On-Going Application Procedure 36
15.4 Survival....36

16 INFORMATION PROVIDED BY/TO THE CCC 37
16.1 Public Information....37
16.2 Confidential Information....37
16.3 Proprietary Information 38
16.4 Retention of Records....38

17 MUTUAL COOPERATION....39

18 CONFLICTS OF INTEREST 40
18.1 General Obligation to Avoid Conflicts of Interests....40
18.2 Duty to Disclose Conflict of Interests 40
18.3 Conflict of Interest Guidelines....40

19 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS....42

20 FEES....43
20.1 General Policy 43

21 LIABILITY 44
21.1 Disclaimer....44
21.2 Indemnity....44

REFERENCES 46

ACRONYMS....47

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

1 INTRODUCTION

1.0.1 This document provides an overview of the Cybersecurity Labelling Scheme for IoT [CLS(IoT)]. It outlines the scheme objectives, description of the scheme, its organisation and management, as well as an overview of the testing process.

1.0.2 This document also sets out the requirements and procedures for the labelling of the internet connected device under the CLS(IoT). It also establishes the technical oversight role of the Cybersecurity Certification Centre (CCC) in the CLS(IoT) and sets out general terms and conditions for the manufacturer and/or the Testing Laboratory (TL) that apply for such a label.

2 BACKGROUND

2.1 IMPETUS FOR CLS(IOT)

2.1.1 Cities around the world have ushered in the era of digital transformation and Singapore is no different as we work towards our vision of a Smart Nation. The Smart Nation empowers the Singapore economy through technology and digital innovation and aims to bring about a better quality of life for all. The Government, through policies and initiatives such as the Safer Cyberspace Masterplan, also aims to better prepare and equip Singapore to embrace the ever-changing digital landscape.

2.1.2 The Smart Nation initiative rests on bridging communications and enabling digital services. This brings about the phenomenon of manufacturing every type of device to be “smart”. From traffic cameras to lampposts and even the most mundane of devices like kitchen appliances and baby monitors, they are now part of the “Internet of Things” or IoT.

2.1.3 IoT can bring about huge benefits to enterprises’ productivity and individuals’ quality of life. As IoT gets rapidly proliferated, the issues relating to cyber security threats become increasingly important. Devices with poor security may be easily exploited by individuals or groups with malicious intents to form botnets and potentially used to participate in Distributed Denial-of-Service (DDoS) attacks, as evident from incidents such as the Mirai and Silex malwares.

2.1.4 The “IoT Security Landscape” which is jointly published by CSA Singapore and Ministry of Economic Affairs and Climate Policy, Netherlands, cites “Evaluation and Certification” among one of the security challenges. While there are well-established certification schemes for IT security products such as Common Criteria (CC) or ISO/IEC15408, the same cannot be seen for IoT and cybersecurity provisions for IoT continue to remain opaque to general consumers.

2.1.5 The intent of the Cybersecurity Labelling Scheme for IoT is to improve the transparency of cybersecurity provisions. Under this scheme, the cybersecurity label would provide an indication of the level of security in the products. Consumers are thereby empowered to make informed purchasing decisions. By enhancing consumer security awareness, this scheme seeks to incentivise manufacturer to develop products with better security for the market, leading towards a safer and more secure cyber space.

2.2 BASELINE SECURITY IN CONSUMER PRODUCTS

2.2.1 A majority of consumer IoT products has inadequate cybersecurity provisions. Fundamental security weaknesses such as universal default passwords continue to be prevalent. In addition, consumer smart devices are often characterised by a short time-to-market cycle for new versions to reach the market, where there is less emphasis for good cybersecurity

design to be incorporated from the start. Due to such characteristics, formal evaluation and certification schemes such as Common Criteria that provide higher security assurance might be deemed infeasible as the evaluation costs and duration are prohibitive relative to the margins for these devices.

2.2.2 Hence, the Cybersecurity Labelling Scheme for IoT is designed to be rapid and cost-effective. The scheme seeks to provide a basic level of security assurance through the elimination of common vulnerabilities and the use of a simple, tiered, and progressive assessment model for IoT devices that avoids resource-intensive security evaluations. The CLS(IoT) should provide a basic level of security hygiene in which it is typically expected for consumer IoT devices to be able to deter casual adversaries utilizing common attack vectors such as default factory credentials or exploiting vulnerable protocols.

2.2.3 It is important to note that the Cybersecurity Labelling Scheme for IoT does not offer formal security assurance. Given sufficient time, determined adversaries who possesses advanced skillsets and tools would likely be capable of compromising such IoT devices, regardless of whether it is labelled. Users seeking higher security assurance (e.g., enterprise, manufacturing, industrial applications, and healthcare) are strongly recommended to consider devices certified under formal evaluation and certification schemes. Details relating to these higher assurance schemes are available on the CSA website (https://go.gov.sg/sccs-about).

3 ORGANISATION AND MANAGEMENT OF CLS(IoT)

3.1 The CLS(IoT) is owned and managed by the Cybersecurity Certification Centre (CCC), under the ambit of the Cyber Security Agency of Singapore (CSA).

3.2 The overall policy of the CLS(IoT) scheme is set by the Cybersecurity Certification Centre (CCC). The CCC is responsible for the direction of the CLS(IoT) scheme, ensuring that the organisation and management of the functions of testing achieve high standards of competency, impartiality, and consistency. The CCC approves standards, publications, and projects.

3.3 The CCC establishes the requirements for the testing laboratories and oversees the testing laboratory approval process. The testing laboratory is approved only after it is assessed to be compliant to the requirements specified in Chapter 12 – Requirements for CLS(IoT) Test Laboratory.

4 OVERVIEW OF THE CLS(IoT)

4.1 OVERVIEW

4.1.1 The Cybersecurity Labelling Scheme for IoT [CLS(IoT)] is a voluntary scheme, for a start. Products that apply for the Cybersecurity Label shall undergo a series of assessments and tests, depending on the level of Cybersecurity Label that the manufacturer wishes to attain.

4.2 CYBERSECURITY LABELLING LEVELS

4.2.1 The CLS(IoT) comprises four (4) cybersecurity levels, with each higher level being more comprehensive in the assessment.

4.2.2 The requirements of testing under each of the cybersecurity levels are summarised in Table 1 - Cybersecurity Levels below.

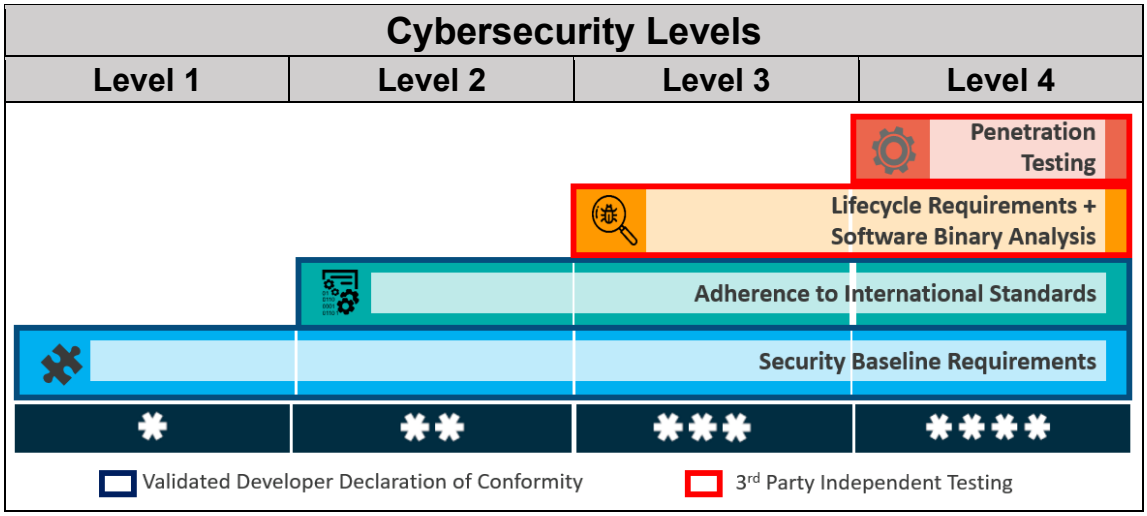


Table 1 - Cybersecurity Levels

4.2.3 Under each labelling level, depending on the level of Cybersecurity Label that the manufacturer wishes to attain, the product shall be subjected to the applicable cybersecurity levels.

4.2.4 There are 4 different cybersecurity levels, covering different security requirements. The cybersecurity labelling levels are briefly described in Chapter 5 – Cybersecurity Levels. Detailed requirements about each of these levels are provided in CLS(IoT) Publication #2 – Scheme Specifications [1].

5 CYBERSECURITY LEVELS

5.1 OVERVIEW OF CLS(IOT) CYBERSECURITY LEVELS

Cybersecurity Level	Assessment Tier	Format	Involved Roles
1	Security Baseline Requirements	Manufacturer's declaration of conformity to be reviewed by the testing laboratory.	CCC; Manufacturer; Testing Laboratory The CCC is the approval authority for all CLS(IoT) cybersecurity levels.
2	Adherence to International Standards		
3	Lifecycle Requirements and Software Binary Analysis	Lifecycle Requirements to be reviewed by testing laboratory based on Manufacturer's declaration of conformity. Software Binary Analysis to be performed by testing laboratory.	
4	Penetration Testing	Assessment to be performed by testing laboratory.	

Table 2 - Overview of CLS(IoT) Cybersecurity Levels

5.2 CLS(IOT) LEVEL 1 – SECURITY BASELINE REQUIREMENTS

5.2.1 CLS(IoT) Level 1 seeks to address the most common IoT security problems by requiring manufacturers to conform to the top 3 security baseline requirements within the ETSI EN 303 645 – Cyber Security for Consumer Internet of Things [2][1], namely no universal default passwords, implementing means to manage vulnerability reporting, and keeping device software updated.

5.2.2 The manufacturer shall engage an approved CLS(IoT) Testing Laboratory and submit to them the completed Declaration of Conformity and Supporting Evidence document, specifying conformity status to the security provisions within the technical specification.

5.2.3 The completed declaration of conformity and supporting evidence shall be reviewed by the Testing Laboratory. If the Testing Laboratory determines

[1] For Home Gateway applications, Level 1 also seeks to address requirements within ETSI TS 103 848 – Cyber Security for Home Gateway: Security Requirements as a vertical from Consumer Internet of Things [7].

that the completed declaration of conformity and supporting evidence meet the requirements, the manufacturer may submit a CLS(IoT) application towards CCC.

5.2.4 The CLS(IoT) application shall contain the following:

i. Completed Declaration of Conformity

ii. Supporting Evidence

iii. Testing Laboratory's Assessment of the completed Declaration of Conformity and Supporting Evidence

5.2.5 CCC shall review the Testing Laboratory's assessment of the completed Declaration of Conformity and supporting evidence prior to approval. Non-conformity to the security requirements shall result in the failure of this activity.

5.2.6 The CCC is the approval authority for the CLS(IoT) Level 1.

5.3 CLS(IOT) LEVEL 2 – ADHERENCE TO INTERNATIONAL STANDARDS

5.3.1 CLS(IoT) Level 2 seeks to ensure adherence to international standards.

5.3.2 The manufacturer shall declare conformity to all mandatory requirements within the specified international standard, which is the ETSI EN 303 645 – Cyber Security for Consumer Internet of Things [2][2].

5.3.3 The manufacturer shall engage an approved CLS(IoT) Testing Laboratory and submit to them the completed Declaration of Conformity and Supporting Evidence document, specifying conformity status to the security provisions within the international standard.manufacturer

5.3.4 The completed declaration of conformity and supporting evidence shall be reviewed by the Testing Laboratory. If the Testing Laboratory determines that the completed declaration of conformity and supporting evidence meet the requirements, the manufacturer may submit a CLS(IoT) application towards CCC.

5.3.5 The CLS(IoT) application shall contain the following:

i. Completed Declaration of Conformity

ii. Supporting Evidence

iii. Testing Laboratory's Assessment of the completed Declaration of

[2]For Home Gateway applications, Level 2 also seeks to address requirements within ETSI TS 103 848 – Cyber Security for Home Gateway: Security Requirements as a vertical from Consumer Internet of Things [7]

Conformity and Supporting Evidence

5.3.6 CCC shall review the Testing Laboratory's assessment of the completed Declaration of Conformity and supporting evidence prior to approval. Non-conformity to the security requirements shall result in the failure of this activity.

5.3.7 The CCC is the approval authority for the CLS(IoT) Level 2.

5.4 CLS(IOT) LEVEL 3 – LIFECYCLE REQUIREMENTS AND SOFTWARE BINARY ANALYSIS

5.4.1 There are 3 components within CLS(IoT) Level 3:

a. Meeting Mandatory Requirements. To ensure that devices meet the mandatory requirements of the specified international standard.
b. Lifecycle Requirements. To ensure that devices are developed according to security-by-design framework and processes.
c. Software Binary Analysis. To analyse the device's software (Device firmware and companion mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses such as buffer overflow.

Mandatory Requirements

5.4.2 The mandatory requirements are defined within CLS(IoT) Level 2.

Lifecycle Requirements

5.4.3 The lifecycle requirements seek to ensure that devices are developed according to a security-by-design framework and processes. The development of these devices can be supported through the adoption of lifecycle processes consisting of general secure software development activities (e.g., threat modelling, secure engineering approach), and by having supporting processes in place to be able to respond to new vulnerabilities.

5.4.4 The referenced lifecycle requirements are specified in the IMDA IoT Cyber Security Guide [3].

5.4.5 The manufacturer shall complete and submit the Declaration of Conformity and Supporting Evidence document (located in the Publication section of the CSA CLS webpage) specifying conformity status to the security provisions within the international standard. The completed declaration of conformity and supporting evidence shall be reviewed by the Testing Laboratory. If the Testing Laboratory determines that the completed declaration of conformity and supporting evidence meet the requirements, the manufacturer may submit a CLS(IoT) application towards CCC.

5.4.6 The CCC is the approving authority for the Testing Laboratory's report on the completed declaration of conformity and rationale.

Software Binary Analysis

5.4.7 The connected device's software (device firmware and companion mobile applications) shall be analysed for malware, known vulnerabilities in third party libraries used, and for software weaknesses such as buffer overflow.

5.4.8 The analysis shall be performed with the aid of a combination of binary, malware, and mobile application scanners.

5.4.9 The manufacturer's Testing Laboratory of choice shall review and interpret the scan results. At the end of the activity, the testing laboratory shall submit a report outlining test results, identified issues and corresponding method of resolution to the CCC.

5.4.10 The CCC is the approving authority for the Testing Laboratory's report.

5.4.11 The expected duration of time spent by the lab on software binary analysis is around 5 days (assuming 8-man hours per day, equating to a total of 40-man hours, and this duration excludes administrative/logistical overheads such as project management and delivery of test units.

5.5 CLS(IOT) LEVEL 4 - PENETRATION TESTING

5.5.1 There are 4 components within CLS(IoT) Level 4

a. Meeting Mandatory Requirements. To ensure that devices meet the mandatory requirements of the specified international standard.
b. Lifecycle Requirements. To ensure that devices are developed according to security-by-design framework and processes.
c. Software Binary Analysis. To analyse the device's software (Device firmware and companion mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses such as buffer overflow.
d. Black-box Penetration Testing. To assert that the device is reasonably resistant to common attacks and to prove that there are no obvious or critical vulnerabilities.

Mandatory Requirements

5.5.2 The mandatory requirements are defined within CLS(IoT) Level 2.

Lifecycle Requirements

5.5.3 The lifecycle requirements are defined within CLS(IoT) Level 3.

Software Binary Analysis

5.5.4 The software binary analysis requirements are defined within CLS(IoT) Level 3.

Black-box Penetration Testing

5.5.5 The black-box penetration testing shall consist of the following sub-activities:

i. Device setup and verification of the guidance documents
ii. Verification of the declaration of conformity and supporting evidence
iii. Minimum Test Specifications
iv. Search for potential vulnerabilities in the public domain

v. Vulnerability analysis of the device using the results from the software binary analysis, guidance documentation, and product security design documents to identify potential vulnerabilities in the device.
vi. Penetration testing to confirm that the identified potential vulnerabilities cannot be exploited.

5.5.6 The manufacturer shall provide sufficient production samples of the device and related user guidance documents to the testing laboratory to facilitate testing.

5.5.7 The Testing Laboratory shall provide a report summarising the tests performed and the results.

5.5.8 The CCC is the approving authority for the testing laboratory's report.

5.5.9 The expected duration of time spent by the lab on security evaluation is around 15 days (assuming 8-man hours per day, equating to a total of 120-man hours), and this duration excludes administrative/logistical overheads such as project management and delivery of test units.

6 GENERAL PROCESS FOR LABELLING OF INTERNET-CONNECTED DEVICE

6.1 PROCESS OVERVIEW

6.1.1 The labelling of internet-connected devices shall be performed within the framework of the CLS(IoT).

6.1.2 The key roles and responsibilities within the CLS(IoT) are as follows:

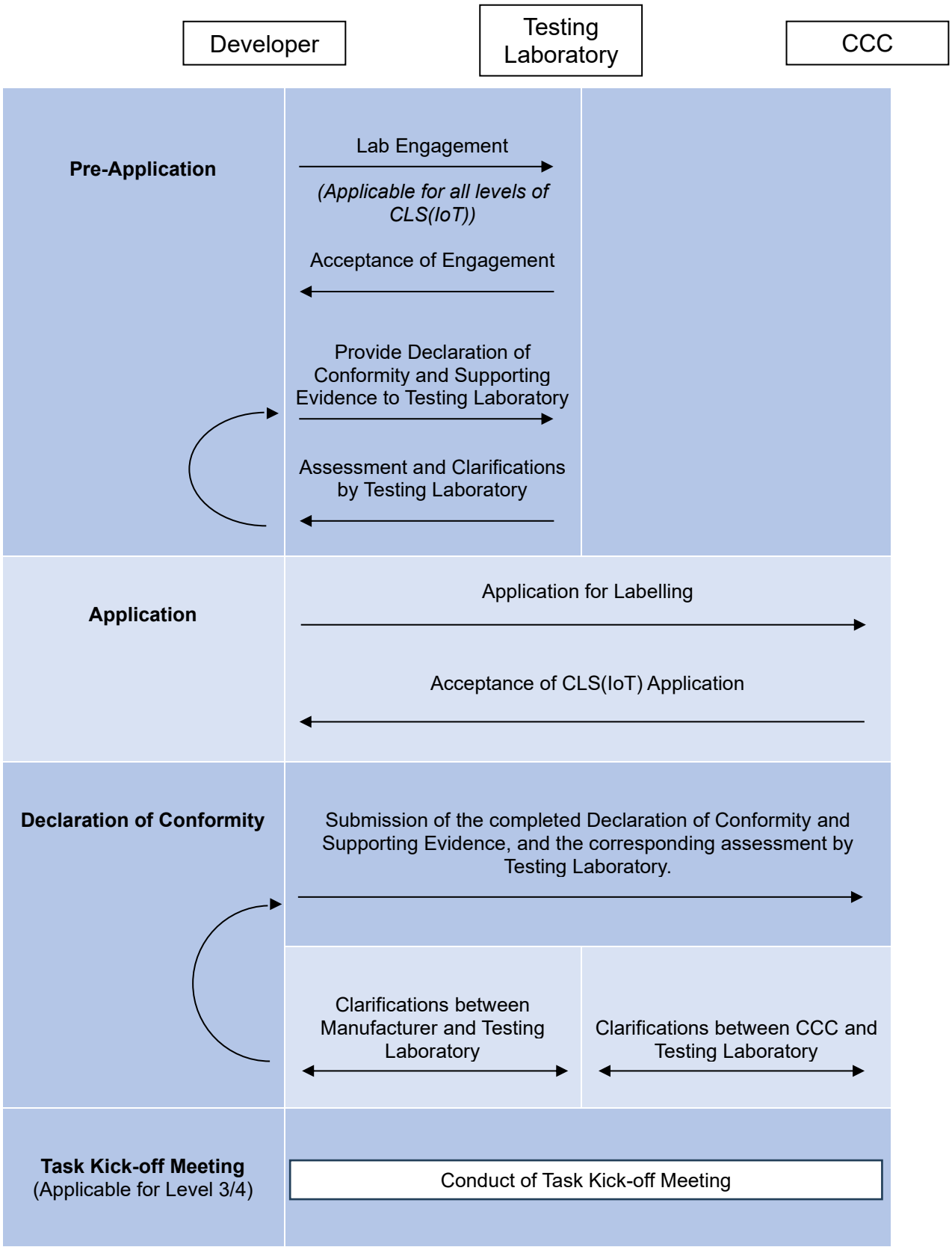
a. CCC: The Cybersecurity Certification Centre (CCC) operates under the ambit of CSA. Being the scheme owner, CCC oversees the entire management and operations of the scheme, reviews and validates the work performed by the testing laboratory to ensure consistency and quality of the testing. CCC is the authority to issue the CLS(IoT) label and to conduct random checks on manufacturers and retailers to ensure that the CLS(IoT) labels are correctly used.

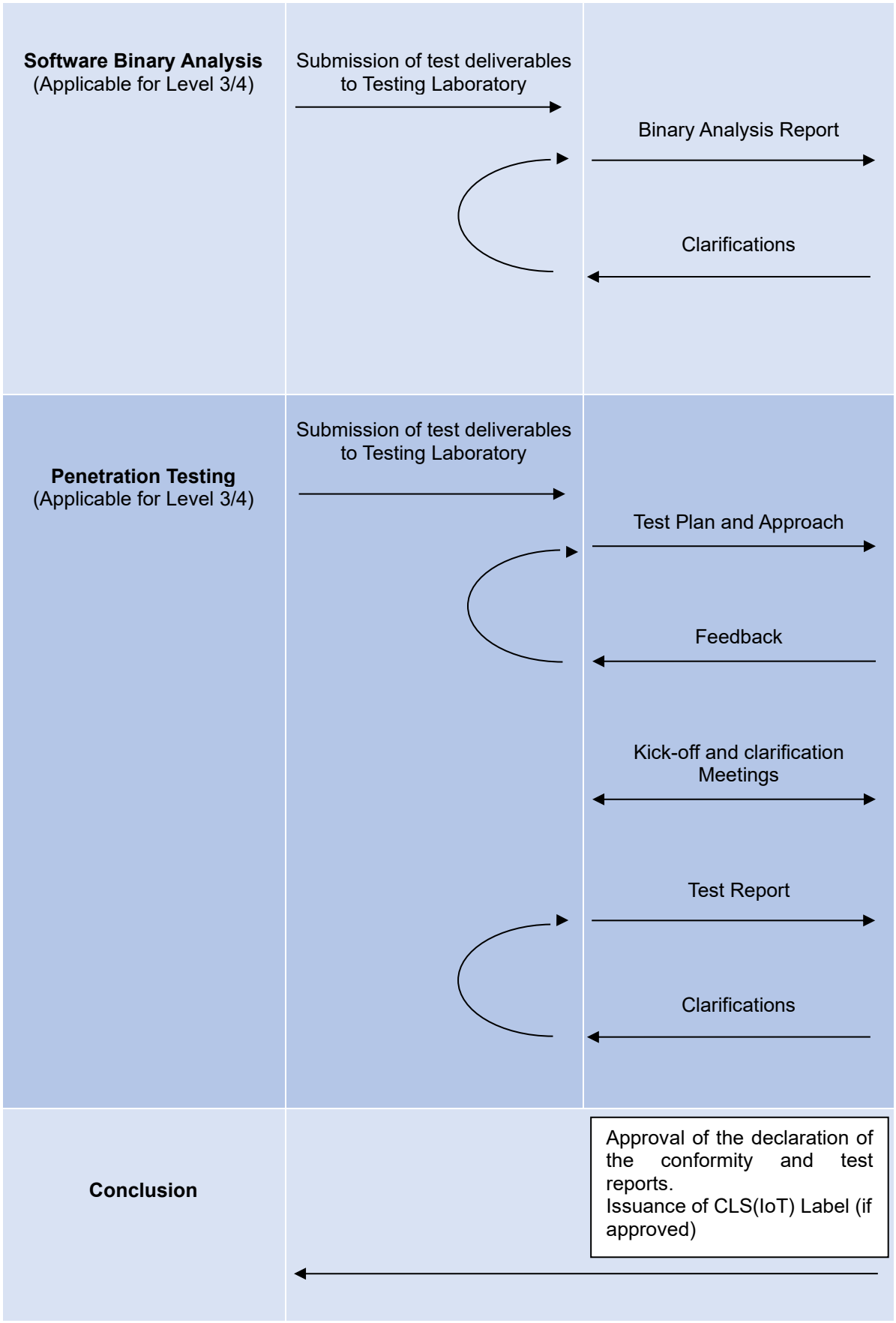
b. Manufacturer [3]: The manufacturer is the applicant who develops, manufactures, or creates the consumer product. The manufacturer is responsible for providing the information required by the CLS(IoT) and supports the Testing Laboratory for the conduct of the testing. In lieu of the manufacturer, the application can be sponsored by either a distributor or retailer. The application can also be submitted by a Testing Laboratory on behalf of the applicant.

c. Testing Laboratory (TL): The TL is an independent commercial testing laboratory which is approved under the CLS(IoT). The TL performs the review of the declaration of conformity and supporting evidence (mandatory provisions of CLS(IoT) and the lifecycle requirements) prior to the final approval by the CCC. The TL conducts assessment tests on the consumer product provided by the manufacturer and reports its results to the CCC.

[3] An exemption is made for Wi-Fi routers intending to attain only CLS(IoT) Label Level 1: Apart from the manufacturer, the developer can also be an importer that intends to supply the Wi-Fi router in Singapore.

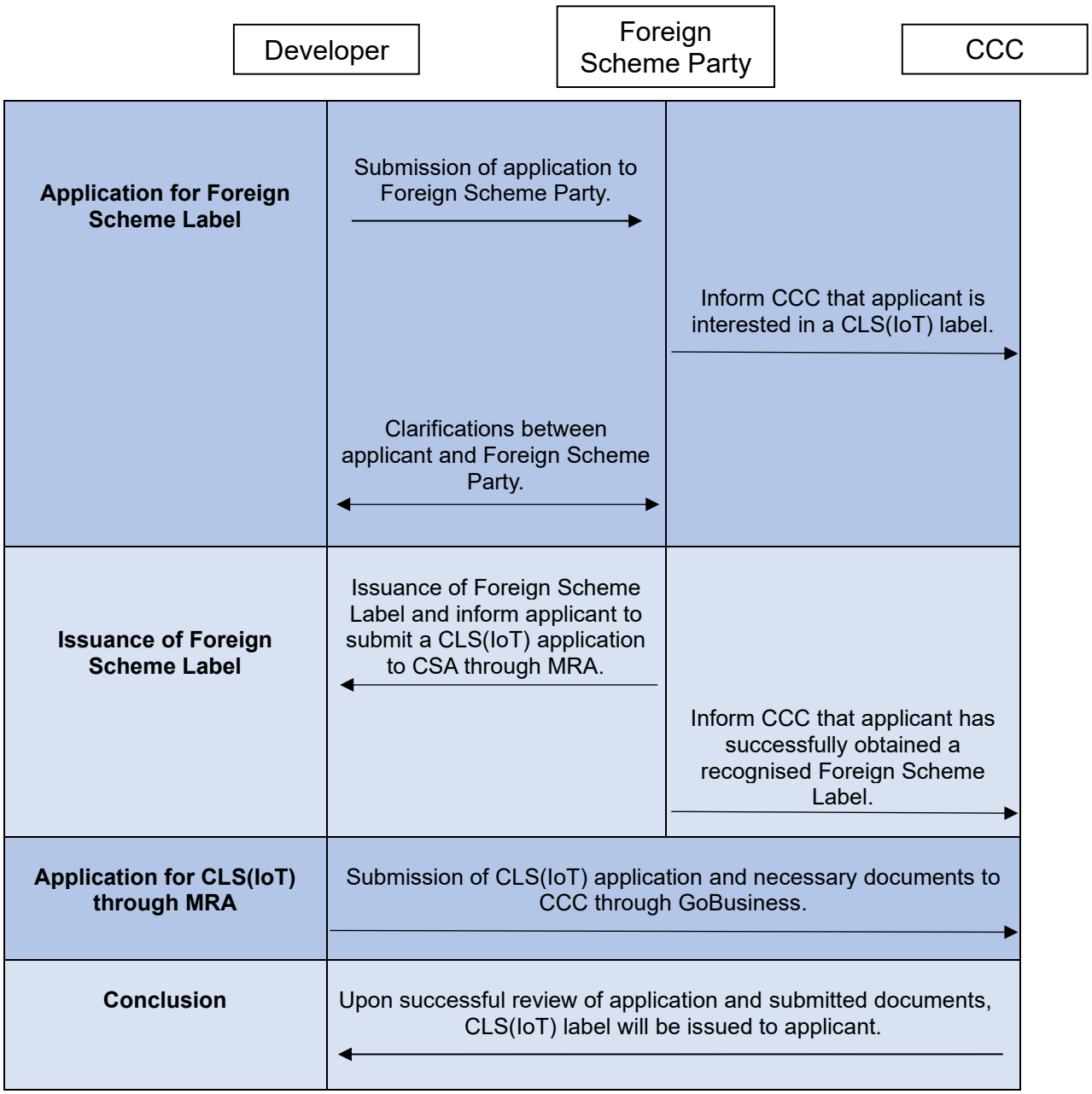
6.1.3 The following diagram illustrates the main phases to the CLS(IoT) labelling process.



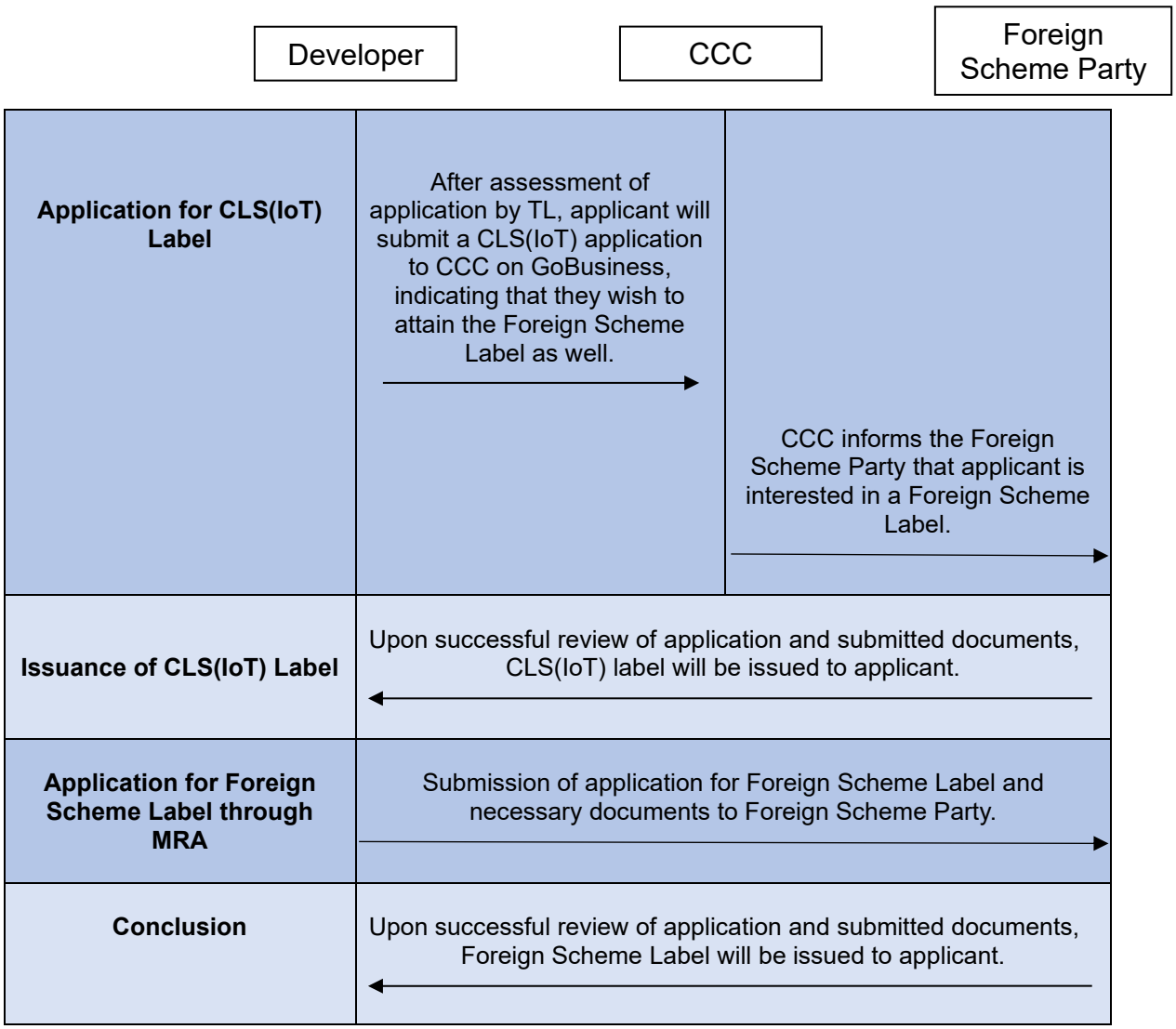

Software Binary Analysis
(Applicable for Level 3/4)
Submission of test deliverables to Testing Laboratory
Binary Analysis Report
Clarifications
Penetration Testing
(Applicable for Level 3/4)
Submission of test deliverables to Testing Laboratory
Test Plan and Approach
Feedback
Kick-off and clarification Meetings
Test Report
Clarifications
Conclusion
Approval of the declaration of the conformity and test reports.
Issuance of CLS(IoT) Label (if approved)

6.1.4 For CLS(IoT) applications through Mutual Recognition Agreements (MRAs), the processes below shall be followed. More information regarding MRAs can be found in Chapter 9 of this publication or on the CLS(IoT) website (https://go.gov.sg/csa-cls).

a. For applicants who wish to apply for the Foreign Scheme Label before applying for CLS(IoT):



b. For applicants who wish to apply for CLS(IoT) before applying to the Foreign Scheme Label:



6.2 PRE-APPLICATION PHASE

6.2.1 Feasibility Study

Apart from commercial considerations, a manufacturer intending to apply for label should carefully study the requirements of the CLS(IoT) and determine which level of the labelling scheme is suitable for the product.

The manufacturer shall ensure that the required evidence is available before making an application. Depending on the level, this could include:

a. Development process documents and/or work instructions
b. Product guidance documents and screenshots of supporting evidence,
c. Product hardware, firmware, companion mobile applications, etc.

If the intended application is for CLS(IoT) Level 3 and 4, prior to the application, the TL shall conduct a readiness assessment of the manufacturer and Device Under Test (DUT). The intention of this procedure is to prevent project delays by ensuring that required components (documentation, etc.) of the projects are available and that the device is in a suitable state for testing.

6.2.2 Lab Engagement

For all levels of CLS(IoT), the manufacturer is required to engage a TL to perform the associated tasks required at the specific levels. The terms of engagement shall be as negotiated between the manufacturer and the TL. CCC will not be involved in any contractual arrangements between the manufacturer and the TL, nor shall CCC be a party to the contract between the manufacturer and the TL.

6.2.3 Enquiry for Labelling

a. Enquiry for labelling under the CLS(IoT) should be addressed to the CCC at the following address:

   via email at cls_iot@csa.gov.sg

   Or

   The Technical Manager,
   Cybersecurity Labelling Scheme for IoT
   Cybersecurity Certification Centre
   Cyber Security Agency of Singapore (CSA)
   5 Maxwell Road MND Complex #03-00 Tower Block
   Singapore 069110

6.3 APPLICATION FOR LABELLING

6.3.1 All applications for labelling are to be made under the CSA CLS(IoT) license at the GoBusiness portal (https://www.gobusiness.gov.sg). More details of the application process are located at the CLS(IoT) website (https://go.gov.sg/csa-cls).

6.3.2 The following deliverables (depending on the intended CLS(IoT) Label level) shall be submitted during the online application:

CLS(IoT) Label	Submission Requirements
Level 1	• Declaration of Conformity and supporting evidence • TL's assessment of the completed Declaration of Conformity and Supporting Evidence
Level 2	• Declaration of Conformity and supporting evidence • TL's assessment of the completed Declaration of Conformity and Supporting Evidence
Level 3	• Declaration of Conformity and supporting evidence • TL's assessment of the completed Declaration of Conformity and Supporting Evidence • Binary Files (Device firmware and companion mobile applications are to be provided to the TL)
Level 4	• Declaration of Conformity and supporting evidence • TL's assessment of the completed Declaration of Conformity and Supporting Evidence • Binary Files (Device firmware and companion mobile applications are to be provided to the TL) • Penetration Testing Report

Table 3 - Application Submission Requirements

6.3.3 All documents and deliverables to be submitted shall be provided in English.

6.3.4 For devices intended for Level 4, a unit of the DUT shall be provided to the CCC during the project application phase.

6.3.5 More specific application requirements and on the declaration of conformity are available at the CSA CLS(IoT) website.

6.3.6 Upon the submission of the application, CCC shall review the application and inform the applicant via email of the acceptance or rejection of the application.

6.4 DECLARATION OF CONFORMITY

6.4.1 The specific requirements on the Declaration of Conformity are specified in CLS(IoT) Publication #2 – Scheme Specifications [1].

6.5 TASK KICK-OFF MEETING (TKM)

6.5.1 After the application has been accepted under the CLS(IoT), the CCC will contact the TL and the manufacturer for the Task Kick-off Meeting (TKM). The outline for a typical TKM agenda is as follow:

- For all parties to introduce and identify the point-of-contacts (CCC, testing laboratory, manufacturer) involved in the application
- For the CCC to provide a brief description of the CLS(IoT) scheme, the application process, and to outline objectives, expectations, limitation and issues.
- For the manufacturer to provide a brief description of the device, including how the device is used, what are the various components, and the corresponding interfaces/connections.
- For the TL to provide a brief description of the application work plan, to explain the scope of evaluation and the timeline, to outline the objectives/expectations/limitation/issues, and to schedule relevant dates, frequency and venue for subsequent meetings.

6.6 TESTING PHASE (ONLY FOR LEVEL 3 ONWARDS)

6.6.1 The required testing tasks are dependent on the CLS(IoT) level that the manufacturer wishes to attain. Detailed requirements of the each of the CLS(IoT) levels are detailed in CLS(IoT) Publication #2 – Scheme Specifications [1].

6.6.2 In the instance of Wi-Fi routers at CLS(IoT) Level 1, the manufacturer can be the importer that intends to supply the Wi-Fi router in Singapore. The importer shall be solely responsible for ensuring that all required information from the manufacturer is available.

6.7 CONCLUSION - AWARDING OF THE CLS(IOT) LABEL

6.7.1 Upon completion of testing, and if the product is deemed to fulfil CLS(IoT) requirements, CCC will issue the CLS(IoT) label and the labelled consumer products shall be listed on the CSA CLS(IoT) website.

6.8 CHANGES TO CONDITIONS FOR LABELLING

6.8.1 CCC reserves the right to make changes to CLS(IoT) Publications and to any conditions for labelling under the CLS(IoT). If such changes substantially affect ongoing test activities, CCC shall be entitled to require the manufacturer to submit a fresh application for labelling.

6.9 CRYPTOGRAPHY

6.9.1 The CLS(IoT) does not address the inherent qualities of cryptographic algorithms. Manufacturers are encouraged to implement cryptographic algorithms based on industry standards. Proprietary cryptographic algorithms are generally discouraged.

7 GROUPING OF APPLICATIONS

7.1.1 The CLS(IoT) allows models from the same product family to be grouped together under a single application to facilitate application efficiency.

7.1.2 The eligibility criteria are as follow:

- For Level 1 and 2 applications, the different models from the same product family shall utilise similar firmware code with same functionalities contributing to security. The differences in the firmware shall be minor, limited to differences in user interface (look and feel) and differences in the drivers due to the different underlying hardware chipsets used.

- For Level 3 and 4 applications, the hardware and software components that contribute to the security (e.g., processor/SoC chipset, Wi-Fi/Bluetooth/Zigbee chipset, security modules, trusted platform modules, etc.) must be the same across models.
    - If there are differences in the hardware and software across the models, they shall be limited to components that do not contribute to the security of the device (e.g., physical look & feel, supported Wi-Fi/LAN connection speed, user functionalities). For devices with different hardware components that contribute to the security of the device, these devices shall be tested separately.

8 APPLICANT OBLIGATIONS

8.1 VULNERABILITY DISCLOSURE

8.1.1 One of the fundamental requirements under CLS(IoT) is for the manufacturer to implement a Vulnerability Disclosure Program. Whenever a vulnerability is reported to the manufacturer, the manufacturer shall notify CCC as early as possible, detailing the vulnerability, the impact, remediation plans and timeline.

8.2 DEFINED SUPPORT PERIOD FOR SECURITY UPDATES

8.2.1 Another fundamental requirement under the CLS(IoT) is for the manufacturer to provide information on the defined support period. The defined support period refers to the minimum period in which the manufacturer agrees to provide security updates to the device. Security updates to the device should be provided in a secure and timely manner.

8.2.2 Minimally, the defined support period must be provided on the manufacturer's website.

9 MUTUAL RECOGNITION

9.1 CSA intends to engage other like-minded partners for mutual recognition of the CLS(IoT) with the objective of eliminating duplicated assessments across national boundaries.

9.2 As of this publication, Singapore has signed Memorandums of Understanding (MoU) with Finland, and Mutual Recognition Arrangements (MRAs) with Germany and Republic of Korea (ROK) to mutually recognise the Cybersecurity Labels issued by the Cyber Security Agency of Singapore, the Transport and Communications Agency of Finland (Traficom), the Germany Federal Office for Information Security (BSI), and Korea Internet & Security Agency (KISA).

9.3 Under the MoU with Finland, smart connected products that have met the requirements of Finland's Cybersecurity Label are recognised as having met the requirements of Level 3 of Singapore's CLS(IoT), and products with CLS(IoT) Level 3 and above are recognised by Finland to have met their requirements.

9.4 Under the MRA with Germany, smart consumer and home gateway products that have met the requirements of Germany's IT Security Label are recognised as having met the requirements of Level 2 of Singapore's CLS(IoT), and products with CLS(IoT) Level 2 and above are recognised by Germany to have met their requirements.

9.5 Manufacturers who have met the requirements of Finland's Cybersecurity Label or Germany's IT Security Label can be awarded the CLS(IoT) label, and vice versa subjected to the applied CLS(IoT) level.

9.6 Under the MRA with The Republic of Korea (ROK), CSA will recognise products issued with Certification of IoT Cybersecurity (CIC) Basic Level and above to have fulfilled CLS(IoT) Level 3 requirements. Similarly, KISA will recognise products labelled with CLS(IoT) Level 3 and above to have fulfilled CIC Basic Level.

9.7 Recipient manufacturers of the CLS(IoT) label via mutual recognition shall ensure that they conform to the requirements surrounding the use of the CLS(IoT) label as defined in Chapter 14 of this publication.

9.8 CLS(IoT) labels obtained through mutual recognition partnerships are not valid for use towards applications for other schemes. As an example, a manufacturer who has attained the Cybersecurity Label from Traficom would be eligible to attain the CLS(IoT) Cybersecurity label through the mutual recognition partnership. However, the manufacturer shall not use the granted CLS(IoT) label towards an application for the BSI IT Security Label.

10 ASSURANCE CONTINUITY

10.1.1 Assurance Continuity defines the approach to minimising redundancy in product assessment, allowing a determination to be made as to whether independent assessments need to be re-performed as changes are made to a labelled product to address security issues, minor bugs, improve the operation of the hardware or peripherals, and to add support for new models of equipment.

10.1.2 For major changes that would invalidate the previous test results (i.e., a change in the underlying operating system used, use of a different programming language, the firmware has been reprogramed from scratch, use of a different security architecture), the manufacturer shall subject the CLS(IoT) Level 3 or Level 4 product to retesting with a TL.

CLS(IoT) Level / Type of changes	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Major change	Label remains valid		Retesting is required.	
Minor change/patch	Label remains valid.			

10.1.3 For minor software updates/patches, the CLS(IoT) label will continue to remain valid.

11 RENEWAL OF LABEL

11.1.1 Manufacturers are allowed to apply for a renewal of the current valid CLS(IoT) label up to 6 (six) months prior to its expiry, and retain the existing Label ID.

11.1.2 An expired label cannot be renewed. In this scenario, the manufacturer will be required to apply for a new label, and a new label ID will be issued.

12 REQUIREMENTS FOR CLS(IOT) TEST LABORATORY

12.1.1 The testing laboratory must satisfy all requirements as stated in CLS(IoT) Publication #3 – Requirements for Test Laboratory [4]).

12.1.2 The testing laboratory is allowed to provide both consultancy and evaluation services for the product under the CLS(IoT) if the testing laboratory is able to demonstrate with clear role and logical separation procedures in place as well as appointing qualified evaluators and qualified consultants for the project.

12.1.3 If the testing laboratory is part of an organisation that performs activities other than IT security evaluation (e.g., consultation to product manufacturer), the testing laboratory shall identify actual and potential conflicts of interest and ensure clear separation of control to ensure that there is no undue influence on the evaluation activities.

13 CYBERSECURITY LABEL

13.1 LABEL

13.1.1 A sample of the CLS(IoT) label as follows:



Figure 1 - Sample of CLS Label

13.1.2 The following details are provided in the label:

a. Cybersecurity level as denoted in the number of asterisk symbols present on the label.

b. Registration Identifier in the format of “CSA/IOTXXXXX”

c. QR code containing the URL to the device’s listing on the CLS(IoT) labelled product list webpage.

13.2 LABEL VALIDITY

13.2.1 Labels are valid for the period in which the manufacturer will support the device with security updates, up to a maximum of a period of 3 years.

13.2.2 While the general validity is for a period of a maximum of 3 years, the label could be revoked if any of the conditions in Section 15.1.1 is met.

13.2.3 Upon expiry of the label, a new CLS(IoT) application is required to obtain a new label.

13.3 REQUIREMENTS OF THE CYBERSECURITY LABEL

13.3.1 The Cybersecurity Label must:

a. Be of the following dimensions:
   i. Small: 2cm (width) by 1cm (height)
   ii. Regular: 4cm (width) by 3cm (height)
   iii. Large: 6cm (width) by 4.5cm (height)

b. Be of font, typeface, font colour as indicated in the label guide,

c. Be of the shape, colour and contain text that is of the typeface as what is specified by the label guide, legible and in the English language only,

d. Contain information that is consistent with or drawn from the test report for the tested good to which the Cybersecurity Label relates,

e. Be printed in an indelible manner and with a minimum resolution of 300 pixels per inch; and

f. Be made of such material as CCC may approve.

13.4 HOW THE CYBERSECURITY LABEL IS TO BE AFFIXED OR DISPLAYED

13.4.1 The digital copy of the label will be provided in .png and .pdf formats.

13.4.2 The Cybersecurity Label shall be affixed on either the product packaging or on the product itself **within 6 months from the date of issue**.

13.4.3 The Cybersecurity Label must be prominently displayed at all points of sale, whether in physical or online stores[4]. For physical stores, the label should preferably be affixed to the product packaging. For online stores, it should be integrated within the product webpage (in the description, images, or specifications). In all cases, the label must be clearly associated with the specific product model and presented in a way that is not misleading to consumers.

13.4.4 The Cybersecurity Labels can be displayed in all advertisements and promotional material of labelled products in local print, broadcast, and digital media. This includes, but is not limited to websites, online stores, and printed catalogues.

13.4.5 In cases where the available space is too small for the Cybersecurity Label to be seen clearly, the rating must be prominently displayed.

13.4.6 If the devices are to be affixed with the Cybersecurity Label, they must have affixed to each of them a Cybersecurity Label that satisfies the following requirements:

a. The Cybersecurity Label is not damaged, defaced or obliterated to prevent any information on the Cybersecurity Label from being read,

b. The Cybersecurity Label is affixed in a conspicuous and unobstructed position on the product.

13.5 LABELLING PRINCIPLES

13.5.1 Upon receipt of the CLS(IoT) label, the manufacturer agrees to continuously adhere to the following principles:

a. The labelled product continues to fulfil the security requirements for the level that the product is being labelled with.

b. CCC shall be informed immediately of any changes that could affect

[4] Manufacturers must comply with this requirement with effect from 01 October 2025.

the ability of the manufacturer/product to fulfil the CLS(IoT) requirements.

c. The manufacturer must not make any statements about its product labelling that CCC deems to be misleading or unjustified. Examples include all models labelled when it is only a specific model that has been issued with the label; claiming the product received a label of higher rating than what is being issued.

d. The manufacturer must not use the cybersecurity label in any way that could discredit the Cyber Security Agency of Singapore and the Cybersecurity Labelling scheme for IoT.

e. The label must not be modified and shall be used exactly as issued by CCC.

13.6 CCC AUDIT AND TESTING

13.6.1 CCC reserves the right to conduct random checks / surveillance and testing of the labelled products. The purpose of the audit is to ensure that labelled products are compliant to the requirements of the CLS(IoT) publications. Manufacturers are **not** expected to pay for the random check / surveillance.

13.6.2 For this purpose, CCC may choose to re-test the labelled device using a separate testing laboratory that was not used during the labelling process.

14 USE OF PROTECTIVE MARKS, LOGOS AND ADVERTISEMENT

14.1 ADVERTISEMENT AND PROMOTION OF LABELLED DEVICES

14.1.1 Proper and appropriate use of marks/labels is contractually imposed on the applicant, see **Error! Reference source not found.** above.

14.1.2 The following guidelines apply to the CLS(IoT) Label:

a. The CLS(IoT) Label may be used by a manufacturer in conjunction with advertising, marketing, and selling of its devices, where such products have successfully attained the CLS(IoT) label under the CLS(IoT) and are listed on the Labelled Product List (LPL).

b. The labelled product name and model number, as listed on the LPL, must be included in any product packaging or publicity materials in which the CLS(IoT) Label also appears.

c. Where any product packaging or publicity material refers to the labelled product and to other products, the layout of information relating to the products relative to the position of the CLS(IoT) Label should not be used in a manner that would or would likely mislead the public into thinking that a product is labelled under the CLS(IoT) when in fact it is not.

d. In relation to product displays, the CLS(IoT) Label should be displayed near the labelled product or its replica or image in a manner that makes it clear that the CLS(IoT) Label refers to the labelled product.

e. The CLS(IoT) Label must be used in the form depicted above. It shall not be altered in any way except for size and monochromatic colour schemes.

f. CSA reserves the right to require the manufacturer to submit samples of their proposed use of the CLS(IoT) Label for prior approval.

14.1.3 The following are examples of acceptable promotional language that can be used in conjunction with the advertising, marketing, and sale of a product for which the label is issued:

- “Labelled in conformity with the CLS(IoT) [Level 1/2/3/4]”
- “[Product Name and Model Number] by [Manufacturer] has been labelled under the Cybersecurity Labelling Scheme for IoT Devices, CLS(IoT), to meet [Level 1/2/3/4] requirements. Conditions for the Label can be found at https://go.gov.sg/csa-cls”
- “[Product Name and Model Number] by [Manufacturer] has been labelled under the terms of the Cybersecurity Labelling Scheme for

IoT Devices. Conditions for the label can be found at https://go.gov.sg/csa-cls."

14.1.4 As show above, all promotional language must include a statement to inform the audience of the website address https://go.gov.sg/csa-cls at which the conditions of the label under the CLS(IoT) can be found.

14.1.5 Labelling under the CLS(IoT) merely indicates that a product meets with specifically identified criteria under the CLS(IoT). It is not a guarantee or assurance by CSA or an assumption by CSA of any responsibility toward any person of the quality of the product or effects of using the product. Manufacturers and Testing Laboratories must avoid making statements that indicate this or may give this impression.

14.1.6 The following are examples of unacceptable promotional language:

- "[Manufacturer or its product or service] is endorsed/ recommended/ approved/ sponsored/supported/ guaranteed by the Cyber Security Agency of Singapore"

- "[Manufacturer or its product or service] is under a guarantee/warranty by the Cyber Security Agency of Singapore"

14.2 RESPONSE TO MISUSE

14.2.1 Any misuse of CLS(IoT) label shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to adopt the correct use;

b. CSA will remove all reference and material from the CLS(IoT) website mentioning the affected product or label;

c. CSA will publish on its website a note regarding any misuse.

14.2.2 Any false, misleading or improper statement about the CLS(IoT) shall, without prejudice to any other rights and remedies of CSA or its licensor(s), entitle CSA to take any or all of the following actions:

a. CSA will inform the relevant party to correct such false, misleading or improper statements about the CLS(IoT);

b. CSA will publish on its website a note regarding any misuse.

15 REVOCATION, TERMINATION AND WITHDRAWAL

15.1 REVOCATION OF THE CYBERSECURITY LABEL

15.1.1 CCC is entitled to revoke a CLS(IoT) label issued under the CLS(IoT) forthwith if:

a. The TL or manufacturer is in breach of any terms of CLS(IoT) Publications, and/or any other terms as agreed to in writing with CCC;

b. The manufacturer has failed to disclose any known or discovered vulnerabilities that, in CCC's opinion, can undermine the CLS(IoT) label;

c. The manufacturer fails to take any corrective measures during the period of grace given by CCC, to the satisfaction of CCC;

d. The manufacturer misuses the CLS(IoT) label, CLS(IoT) status, or any proprietary names and marks associated with CCC or CLS(IoT);

e. The manufacturer makes any statement that misrepresents any aspect of testing or the effect of the labelling under the CLS(IoT);

f. CCC finds that the TL was in a position of conflict that impaired its ability to conduct a fair and impartial testing of the device;

g. The labelled device no longer meets the conditions under which the label was granted or does not meet any changed conditions for labels introduced by CCC after the device was originally labelled.

h. CCC discovered that the manufacturer has made a false statement or declaration in any deliverables submitted to CCC.

15.1.2 Upon the revocation of a CLS(IoT) label, the manufacturer and the Testing Laboratory shall immediately cease all use of the CLS(IoT) label, or any proprietary names and marks associated with CSA, CCC, or the CLS(IoT), and desist from holding the applicable products out as being labelled under the CLS(IoT).

15.1.3 CCC will inform the manufacturer and the Testing Laboratory in writing of the revocation of the CLS(IoT) label and will remove the listing of the labelled product from the Labelled Product List (LPL). The project details will be put into the common Historical Product List (HPL).

15.2 TERMINATION OF ON-GOING APPLICATIONS

15.2.1 The CCC is entitled to terminate an ongoing application procedure without issuing a label at any stage forthwith by notice in writing to the manufacturer if:

a. The manufacturer has not paid any sums due to CCC in respect of the application;

b. The Testing Laboratory or the manufacturer has not engaged in any testing or application activity for more than 8 consecutive calendar weeks;

c. The application process extends beyond 6 calendar months from the date of acceptance from the CCC without a timely extension request (which must be submitted before the 6-month mark);

d. The application process exceeds 1 full calendar year from the date of acceptance from the CCC;

e. All necessary fixes, mitigations or changes to meet requirements are not completed within the allowed timeframe (either the initial 6 months or the extended periods, if approved). In addition, if the CCC deems the implemented resolutions insufficient (e.g., due to high residual risk) or inappropriate;

f. The Testing Laboratory or the manufacturer fails to take any action within the requisite timeframe in the application work plan, or otherwise stated by the CCC, and has not obtained the approval of the CCC to a revised timeframe;

g. The scope of the application changes such that the IoT device under application no longer fulfils the requirements for admittance into the scheme.

h. The manufacturer or the Testing Laboratory has suspended or terminated a project in accordance with the terms of the contract entered between them. In that event, the party that has suspended or terminate the project shall notify the CCC in writing of the suspension or termination within seven (7) calendar days thereof;

i. The Testing Laboratory’s quality of work or intermediate reports is/are repeatedly insufficient, the CCC requires frequent corrections, and/or the Testing Laboratory fails to meet the deadlines as outlined in the application work plan.

j. The manufacturer’s submissions repeatedly fail to address corrective actions, to provide required clarity, and/or fail to meet deadlines as outlined in the application work plan.

15.2.2 The CCC may also suspend or terminate an on-going application procedure under the CLS(IoT) for reasons given in 15.1.1 above. Suspension means that the CCC may allocate its resources to other projects. Suspension can apply for the same reasons as termination but may also apply in cases where the manufacturer and the Testing Laboratory need to change the application work plan due to findings or other reasons for project delay, and where the updated application work plan cannot be established within 30 calendar days after the CCC has requested a new version of the application work plan from the Testing Laboratory. Suspension aims to allow the manufacturer to focus on issues of testing and/or planning without the need for the CCC to keep resources allocated. The application procedure can resume after the CCC has sufficient evidence that the application work plan can be achieved and has the same or equivalent resources available as before suspension.

15.2.3 The CCC may consult with the Testing Laboratory and the manufacturer to confirm the status of the project before proceeding to inform them in writing of the decision to terminate the application procedure.

15.2.4 Upon the termination of an application procedure under the CLS(IoT), the CCC will close its file and the CCC resources assigned to the project will be released.

15.3 WITHDRAWAL FROM ON-GOING APPLICATION PROCEDURE

15.3.1 When a manufacturer wishes to withdraw an ongoing application procedure, the manufacturer shall inform the CCC in writing.

15.3.2 Nothing in this CLS(IoT) publication prevents a Testing Laboratory from withdrawing from an application procedure. The Testing Laboratory's rights to withdraw from an application procedure is subject to the terms of the agreement between the Testing Laboratory and the manufacturer. The Testing Laboratory shall give the manufacturer and the CCC advanced written notice of any withdrawal from an application procedure. Upon the withdrawal of the Testing Laboratory from an application procedure, the manufacturer may decide to try to continue the project with another Testing Laboratory or withdraw the project. The manufacturer shall inform the CCC of its decision in writing and obtain the CCCs approval of the replacement Testing Laboratory within such time as the CCC shall specify, failing which the application procedure shall be deemed withdrawn from the CLS(IoT).

15.4 SURVIVAL

15.4.1 Any obligations of a manufacturer or Testing Laboratory under the CLS(IoT) or their respective agreements with the CCC which by their nature would continue beyond termination or expiration thereof, including without limitation the obligations set out in sections 16, 18, 19, 21 of this publication, shall survive such termination or expiration.

16 INFORMATION PROVIDED BY/TO THE CCC

16.1 PUBLIC INFORMATION

16.1.1 CSA maintains a public website that contains a broad range of information about the CLS(IoT), including the publish of the labelled product list (LPL) and the archived product list (APL) containing information of the devices labelled under the CLS(IoT). Information that will be made publicly available includes the device's details (product naming, model number, etc.) and the test laboratory that is responsible for evaluating the device.

16.1.2 The information informs the public of the labelled devices that are available and provides a source of reference for users to verify the current status of issued labels.

16.2 CONFIDENTIAL INFORMATION

16.2.1 The manufacturer or the Testing Laboratory shall review and confirm promptly in writing the release of information by the CCC before it is made available to the public. Such confirmation shall be provided within the time stipulated by the CCC, failing which the information may be released by the CCC free from any obligation of confidentiality.

16.2.2 It is the responsibility of the manufacturer and the Testing Laboratory (as the case may be) to ensure that any information published by the CCC does not contain any proprietary or protected information.

16.2.3 Any information that is not publicly releasable must be explicitly marked or labelled as such by the manufacturer or the Testing Laboratory (as the case may be) before being delivered to the CCC.

16.2.4 Notwithstanding any of the above, the CCC will not be liable for the disclosure of information designated as confidential or proprietary if the CCC determines that withholding the information is contrary to law.

16.2.5 Except with the written consent of the CCC, the manufacturer and the Testing Laboratory shall not disclose to any person any information, documents, materials provided by the CCC where the same has not been made publicly available by CSA ("CCC Confidential Information").

16.2.6 The manufacturer and the Testing Laboratory shall not, without the prior written consent of the CCC make use of any CCC Confidential Information other than for the purposes of the project for which the CCC Confidential Information was disclosed to them.

16.2.7 The manufacturer and the Testing Laboratory shall keep confidential the CCC Confidential Information and shall only disclose it to their employees on a need-to-know basis for the purposes of the project for which the CCC Confidential Information was disclosed. Without prejudice to the generality of the foregoing, no CCC Confidential Information shall be stored or

distributed by the manufacturer or the Testing Laboratory outside its local protected IT infrastructure. The manufacturer and the Testing Laboratory each undertake to take such steps as shall be necessary to protect the CCC Confidential Information and to notify the CCC as soon as it becomes aware of any unauthorised use of the whole or any part of the CCC Confidential Information.

16.2.8 All documents and other materials containing the CCC Confidential Information shall, at the CCC's request, be returned or otherwise disposed of in the manner specified by the CCC.

16.3 PROPRIETARY INFORMATION

16.3.1 Nothing in this document shall affect any person's ownership rights in and title to that person's pre-existing Intellectual Property (IP) or IP independently brought into existence or acquired by that person without reliance on any CLS(IoT) IP. The term "IP" is defined in **Error! Reference source not found.** below. All documents and other materials provided by the CCC to the manufacturer, or the Testing Laboratory shall remain property of CSA and shall at the CCC's request be returned to the CCC or disposed of in the manner specified by the CCC.

16.3.2 Before delivering any IP to the CCC, the manufacturer and the Testing Laboratory shall ensure that it owns or has all the necessary right, power and authority to disclose such IP to the CCC.

16.3.3 Before requesting for the labelling of a device under the CLS(IoT), each manufacturer shall ensure that it owns the device or has all the necessary right, power and authority to make such a request.

16.3.4 The manufacturer and the Testing Laboratory shall, if required by the CCC, do all acts and execute or procure the execution of such documents as may reasonably be required in order to perfect, protect or enforce any of the CCC's rights hereunder to the IP provided by the manufacturer or the Testing Laboratory.

16.4 RETENTION OF RECORDS

16.4.1 CCC will maintain a record system providing a retention period of 5 years for documents related to the applications. The record system will be managed with procedures for the access to protected information, and for the creation, marking, storage, transmission, copying and disposal of protected information.

17 MUTUAL COOPERATION

17.1.1 The manufacturer and Testing Laboratory shall adhere to the timeframes set out in the application work plan (where applicable) or otherwise approved by the CCC for the performance of their respective obligations in relation to applications under the CLS(IoT) or (where applicable) activities under the Assurance Continuity.

17.1.2 The manufacturer and Testing Laboratory shall provide each other and the CCC, as applicable, with such information, documentation, and materials as they shall each require with reasonable promptness and attend such meetings with each other and/or the CCC as required from time to time.

17.1.3 The manufacturer and Testing Laboratory shall, as applicable, co-operate with each other and the CCC in order to fulfil their respective obligations under the CLS(IoT) in a timely and efficient manner.

18 CONFLICTS OF INTEREST

18.1 GENERAL OBLIGATION TO AVOID CONFLICTS OF INTERESTS

18.1.1 As noted above, the manufacturer may hire a Testing Laboratory to provide advice, assistance and consultancy services in the course of preparing for an application or Assurance Continuity under the CLS(IoT). Such services may include reviewing and preparing supporting evidence and assisting in resolving testing issues. As used in this section, the term “consultancy services” shall refer to the services described in this paragraph.

18.1.2 Hiring a Testing Laboratory to provide consultancy services is not strictly required, nor is the CCC involved in any party’s decision to do so. The scope of the consultancy services is a matter for negotiation between the Testing Laboratory and the party hiring it for such consultancy services.

18.2 DUTY TO DISCLOSE CONFLICT OF INTERESTS

18.2.1 For each application under the CLS(IoT), the Testing Laboratory shall notify the CCC of any known or potential conflict of interests relevant to that application.

18.2.2 The CCC will determine whether a conflict of interest exists on a case-by-case basis. The CCC is the final arbiter in determining whether a potential or actual conflict of interest exists and whether the Testing Laboratory should or should not participate in the application under the CLS(IoT).

18.3 CONFLICT OF INTEREST GUIDELINES

18.3.1 The guidelines in this section are intended to assist Testing Laboratories to avoid conflict of interest situations but are not exhaustive.

18.3.2 The Testing Laboratory shall not accept the of testing any product developed, manufactured, or sold by an entity that possesses an ownership interest in the Testing Laboratory or in which the Testing Laboratory has an ownership interest. The term “ownership interest” shall include any percentage of ownership which is greater than 5%.

18.3.3 The Testing Laboratory must not have entered into an agreement that would result in the Testing Laboratory directly benefitting financially from commercial sales of the device being evaluated or in which the Testing Laboratory has sole distributorship for the labelled device.

18.3.4 Neither the Testing Laboratory nor its parent company, affiliates or any individual Testing Laboratory staff member concerned with a particular testing shall have a vested interest in the outcome of that evaluation.

18.3.5 A Testing Laboratory staff member or testing team member cannot, under any circumstances:

- Be concurrently employed/appointed in another unit of the organisation or another organization which develops IoT devices;

- Own shares of organization which develops IoT devices; and

- Develop IoT devices for public circulation (e.g. open source) or commercial purposes.

18.3.6 The Testing Laboratory must ensure that there is sufficient separation of control and influence in order that its parent company or affiliates cannot exert undue influence on the outcome of testing activities and proprietary or confidential testing information cannot be inappropriately accessed by its parent company or affiliates.

19 MECHANISM FOR COMPLAINTS, DISPUTES AND APPEALS

19.1.1 The objective of the CLS(IoT)'s Complaints, Disputes and Appeals process[5] is to track feedback from stakeholders and to ensure that issues are resolved:

a. Manufacturers may contact CCC directly if they are dissatisfied with any services provided by the testing laboratories regarding their project. CCC holds all raised concerns in strict confidence.

b. Manufacturers or testing laboratories may contact the Head of Cybersecurity Certification Centre directly if they disagree with a decision. CCC holds all raised concerns in strict confidence.

19.1.2 CCC shall acknowledge the receipt of a formal complaint, dispute or appeal and looks into the content of the complaint, dispute or appeal to determine whether the complaint, dispute or appeal relates to test activities for which CCC is responsible.

a. If CCC does not accept the complaint, dispute, or appeal, this is explained in writing to the party lodging the complaint.

b. If CCC accepts the complaint, dispute, or appeal, it then processes it, recording and verifying all the necessary information (as far as possible) in order to reach a decision regarding the complaint, dispute or appeal.

19.1.3 To begin with, an attempt is made to reach an agreement regarding the disputed matter with the certifier responsible for the procedure concerned.

19.1.4 If any issue cannot be resolved to the satisfaction of the originating party, the originating party may contact CCC. Resolution of the issue is under the responsibility of the Head of the Cybersecurity Certification Centre, whose decision made on any issue raised is final.

[5] A dispute is a written statement to CCC indicating disagreement with a decision made by CCC. A complaint is a written statement to the CCC indicating dissatisfaction with a service provided by CCC or the Testing Laboratory. An appeal is a written statement to CCC indicating dissatisfaction with the resolution of a complaint or dispute.

20 FEES

20.1 GENERAL POLICY

20.1.1 The fees for CCC's work in connection with the labelling process shall be prescribed by CCC and published on the CSA website. CCC reserves the right to review the fees as and when necessary. These costs are based primarily on the type of procedure requested, the specific object to be labelled, the scope desired and the degree of assessment envisaged or required. However, the procedure costs are charged irrespective of the ordering party's attributes (company name, company size, registered office, division, etc.).

20.1.2 All fees are in Singapore dollars and are subjected to GST.

20.1.3 Labelling fees are always charged as agreed – regardless of whether a label has been issued or could not be issued due to technical deficiencies or other deficiencies, the applicant cancelled the procedure or CCC suspended the procedure due to failure to provide the necessary information.

20.1.4 If the manufacturer requires modifications to reports, expert opinions or labels that CCC has already approved, the additional effort will be charged to the manufacturer. This also applies to performing re-labelling, if these become necessary due to reasons caused by the manufacturer.

20.1.5 All fees mentioned in CLS(IoT) publications are exclusive of fees charged by testing laboratories for testing work performed.

20.1.6 Upon withdrawal, suspension, or termination of an application, there will be no refund of any fees or payments received by CCC, and no demands or claims shall be made against the CCC in connection with such withdrawal, suspension or termination of the application. Outstanding payments (if any) shall become immediately due and payable by the applicant. To subsequently obtain the cybersecurity label for the same device, a fresh application must be made.

21 LIABILITY

21.1 DISCLAIMER

21.1.1 CSA makes no representations, warranties or covenants of any kind, whether express, implied or statutory, with respect to the CLS(IoT), TLs, or any testing conducted, or labels awarded under the CLS(IoT), including without limitation any warranties of merchantability, satisfactory quality, fitness for a particular purpose or non-infringement of third party rights and any warranties that they are accurate, reliable or error-free. All implied warranties of any kind are excluded to the maximum extent permitted by law. Any person's use of and/or reliance on the CLS(IoT), TLs, or testing conducted, or labels awarded under the CLS(IoT) shall be at their own risk.

21.1.2 To the extent permissible by law, in no event will CSA, its officers, directors, employees or any other person acting under the direction of CSA be liable to a manufacturer, manufacturer, TL or any other person for any loss or damage under any theory of liability, whether direct, indirect, incidental, special, consequential or exemplary in nature, arising out of or in connection with the CLS(IoT) or any decisions by CSA or any such person in relation to the CLS(IoT) if made in good faith in the ordinary course of the discharge of the CSA's duties under the CLS(IoT), including but not limited to lost profits, loss of goodwill and business opportunities, costs of procurement of substitute goods or services, business interruption or loss of business information and data, even if the CSA has been advised of the possibility of such damages.

21.2 INDEMNITY

21.2.1 To the extent permissible by law, each Testing Laboratory shall indemnify, defend and hold harmless and release CSA and its agents, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits, actions, judgments, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the Testing Laboratory under the CLS(IoT) Terms, any act, neglect or omission by the Testing Laboratory or its agents, directors, officers, employees, successors, assigns and representatives and/or any dispute between the Testing Laboratory and a manufacturer or any other third party arising out of or in connection with the foregoing or the CLS(IoT).

21.2.2 To the extend permissible by law, each manufacturer shall indemnify, defend and hold harmless and release CSA and its agent, directors, officers, employees, successors, assigns and representatives thereof (collectively the "Releasees") from and against any and all claims, demands, suits, actions, judgements, damages, costs, losses, expenses (including all legal fees and expenses) and other liabilities arising from, in

connection with or related in any way, directly or indirectly, to the breach of any warranties or obligations of the manufacturer under the CLS(IoT) Terms, any act, neglect or omission by the manufacturer or its agent, directors, officers, employees, successors, assigns and representatives and/or any disputes between the manufacturer with a Testing Laboratory or any other third party arising out of or in connection with the foregoing or the CLS(IoT).

References

[1] Cyber Security Agency of Singapore, “CLS(IoT) Publication #2 - Scheme Specifications,” CCC SP-151-2 Version 1.4, April 2025.

[2] ETSI, “Cyber Security for Consumer Internet of Things,” ETSI EN 303 645 v2.1.1 (2020-06).

[3] Info-communications Media Development Authority of Singapore, “IMDA Internet of Things (IoT) Cyber Security Guide,” Version 1, March 2020.

[4] Cyber Security Agency of Singapore, “CLS(IoT) Publication #3 - Requirements for Testing Laboratory,” CCC SP-151-3 Version 1.1, September 2023.

[5] Cyber Security Agency of Singapore, “CLS(IoT) Publication #5 - Minimum Test Specifications and Methodology for Level 4,” CCC SP-151-5 Version 1.1, April 2021.

[6] Cyber Security Agency of Singapore, “CLS(IoT) Publication #1 - Overview of the Scheme,” CCC SP-151-1 Version 1.4, April 2025.

[7] ETSI, “Cyber Security for Home Gateway: Security Requirements as a vertical from Consumer Internet of Things,” ETSI TS 103 848 v1.1.1 (2022-03).

ACRONYMS

The following acronyms are used in CLS(IoT) Publication 1:

CC	Common Criteria for Information Technology Security Evaluation
CCC	Cybersecurity Certification Centre
CCTL	Common Criteria Testing Laboratories
CLS	Cybersecurity Labelling Scheme
CSA	Cyber Security Agency of Singapore
DUT	Device Under Test
ETSI	European Telecommunications Standards Institute
HPL	Historical Product List
IMDA	Info-communications Media Development Authority
IoT	Internet of Things
LPL	Labelled Product List
SCCS	Singapore Common Criteria Scheme
TL	Testing Laboratory