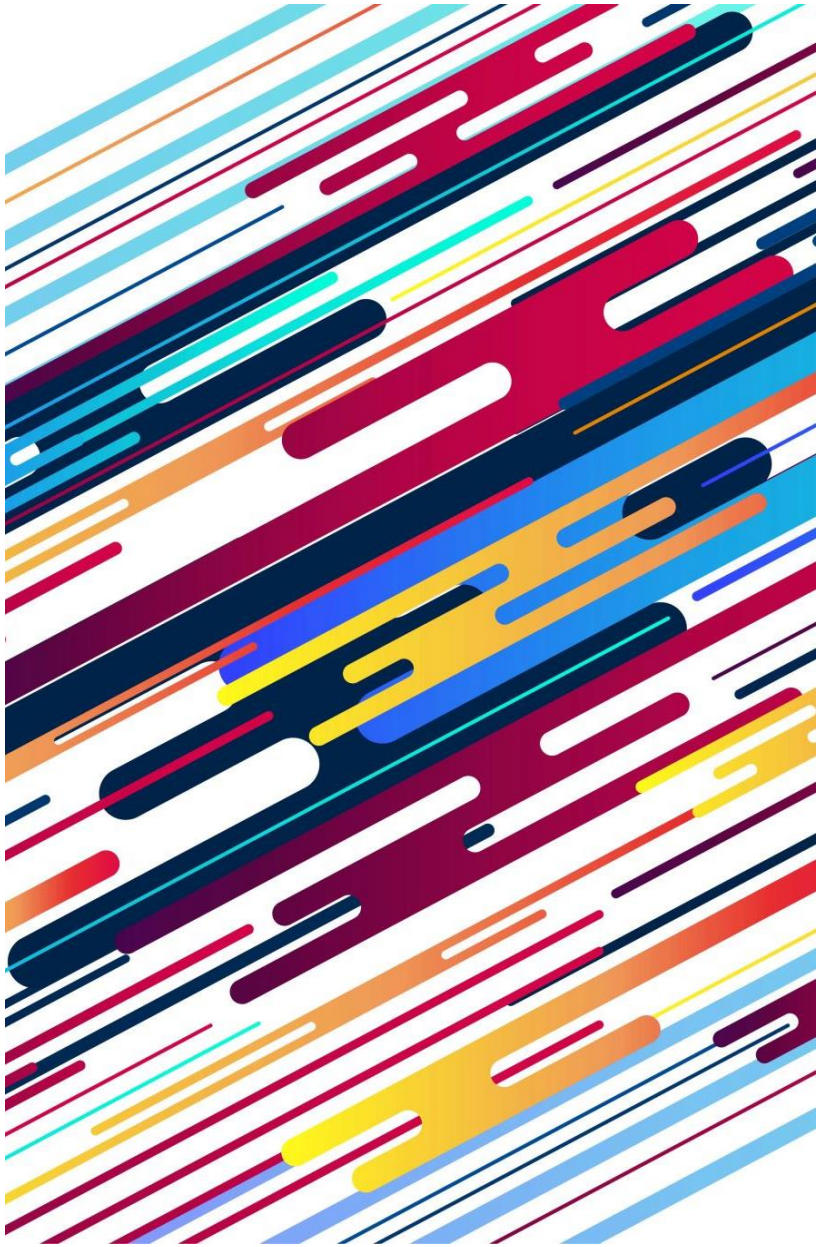


Cybersecurity Labelling Scheme
FOR MEDICAL DEVICES

Cybersecurity Labelling Scheme for Medical Devices, CLS(MD)

Public Consultation Briefing

Presented jointly by MOH, CSA, HSA, IHiS

Session held on **8 February** and **21 February 2023**

Highlights of the Consultation Paper

Highlights of the Consultation Paper

Sections	Section Header
2	Medical Devices In-Scope for CLS(MD)
6	Framework
6.1	Level 1 – Baseline Security Requirements
6.2	Level 2 – Enhanced Security Requirements
6.3	Level 3 – Software Binary Analysis & Time-Bound Black-box Penetration Testing
6.4	Level 4 – Time-Bound White-box Security Evaluation
7	Requirements for CLS(MD) Testing Laboratories
8.1	Proposed Design and Conditions of the Cybersecurity Label
8.2	Validity of the Label
8.3	Labelling Principles
8.4	Revocation of the Label
9	Operationalisation
10	Devices that are currently in use

Please note: *The whole Consultation Paper should be read together for completeness. While the above sections are highlighted, other parts of the Consultation Paper are not viewed of less importance.*

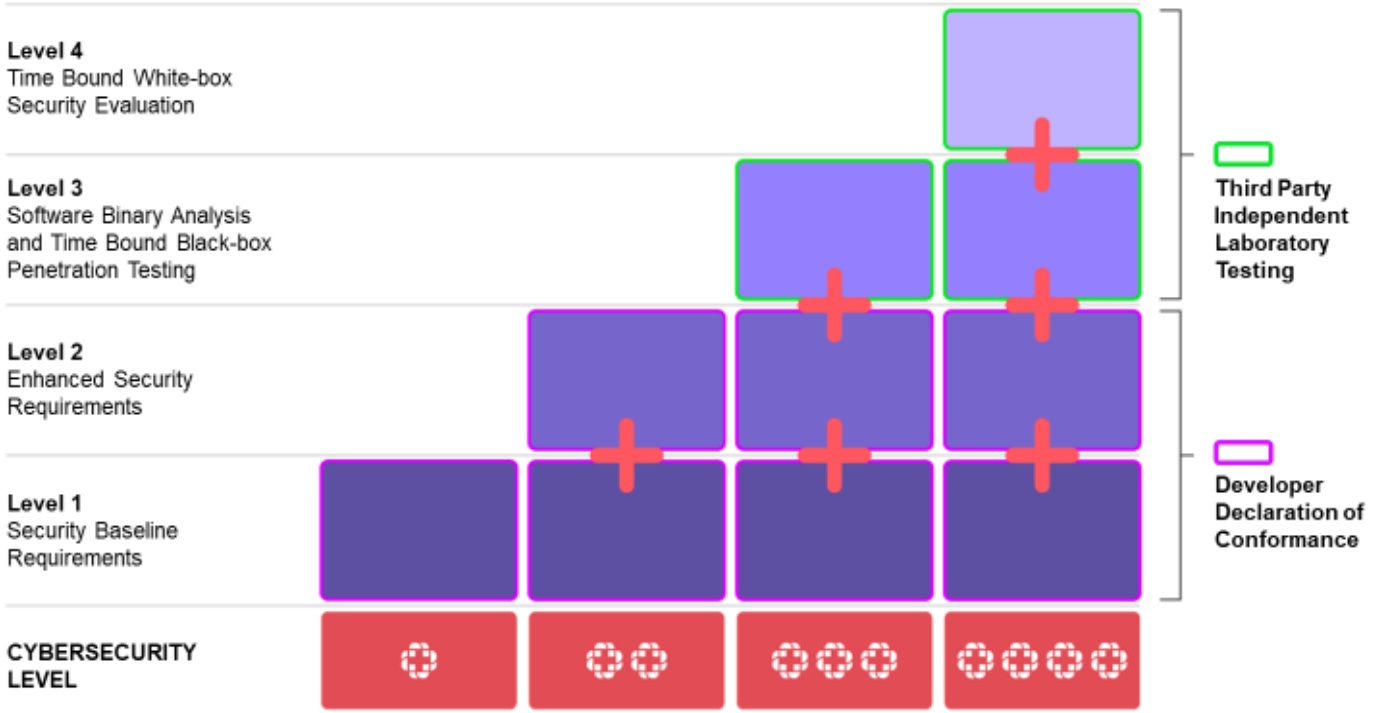
2. Medical Devices In-Scope for CLS(MD)

The scope of the CLS(MD) applies to **medical devices** as described in the First Schedule of the Health Product Act (Cap122D, 2008 Rev Ed) **and** have any of the following characteristics:

i. Handles **personal identifiable information (PII) and clinical data** and has the ability to collect, store, process, or transfer such data;

ii. Connects to other devices, systems, and services - Has the ability to communicate using wired and / or wireless communication protocols through a network of connections.

6. Framework



Levels	Descriptions
1 +	Manufacturers need to meet the existing mandatory HSA requirements based on international standards adopted by major MD regulatory bodies (e.g. US FDA, Health Canada, Japan MHLW, TGA Australia)
2 ++	Manufacturers need to meet the enhanced security requirements titrated from MDS2, Post-market policies and existing CLS standards.
3 +++	The software of the medical device (i.e., firmware, mobile applications if available) undergo automated binary analysers to ensure no known critical software weakness, vulnerabilities or malware. **&** The device will also undergo a timebound black-box(1) penetration testing to provide basic level of resistance against common cybersecurity attacks.
4 ++++	The device undergoes a timebound white-box(2) security evaluation to provide higher level of resistance against cybersecurity attacks.

(1) *Black-box penetration test: Evaluator performs testing using only limited information (i.e. only user guidance manuals that is provided with the device).*
(2) *White-box security evaluation: Evaluator is provided with information on the design/implementation of certain security functionalities (i.e. cryptographic functions). With more information, evaluator would be able to devise targeted tests and better assess the security functionalities of the device.*

6.1 Level 1 – Baseline Security Requirements *(Para 21)*

21. On top of the four existing requirements used by HSA in the review of medical devices seeking registration in Singapore, namely (Clauses 1, 7, 10, 20 in Annex B1), **Clauses 18 and 19 are also being considered for inclusion into Level 1.**

    - This means that medical devices must also meet these two clauses in addition to HSA's current 4 cybersecurity requirements to qualify for CLS(MD) Level 1, which is required for registration and market entry.

#	Clause Description
1	The manufacturer shall provide a vulnerability disclosure program (i.e. ISO/IEC 29147, etc.) covering the device.
7	Manufacturer shall have an on-going plan to remediate cybersecurity vulnerabilities to ensure device performance and safety is not compromised throughout the device's lifecycle.
10	The manufacturer shall have a Post-Market plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat, and respond.
20	The manufacturer shall consider cybersecurity risks/ vulnerabilities as part of their overall risk management process throughout the lifecycle of the medical device. It is highly recommended that manufacturer addresses cybersecurity risk related to universal default password and brute force attacks, where applicable. In addition, to provide evidence that the security of the device/effectiveness of the security controls have been verified.

#	Clause Description
18*	Where passwords are used and, in any state, other than the factory default, the **medical device passwords shall be unique per device or defined by the user**. Where pre-installed passwords are used, they shall be unique per device and sufficiently random.
19*	The device shall have a mechanism available which makes brute force attacks on authentication mechanisms impractical.

** These two clauses are deemed as basic cybersecurity hygiene practice and are also requirements in the CLS scheme for IoT devices. Since medical devices should at least be held to the same, if not higher cybersecurity standards, these two clauses are deemed as important for CLS(MD) Level 1.*

6.1 Level 1 – Baseline Security Requirements

Some information we would like to solicit feedback from the consultation:

1. What percentage of existing medical devices provided by your company can already meet the two clauses?
   - Please kindly provide some examples on these devices in the accompanying “Feedback.xlsx”.
2. What percentage of existing medical devices provided by your company are unable to meet the two clauses?
   - Please kindly provide details of some examples of these medical devices in the accompanying “Feedback.xlsx”.
     a. Device Categories (E.g. ventilator, ultrasound system)
     b. Reasons on why these devices are unable to comply. E.g. Not applicable, the devices were not developed to fulfil these requirements, the device’s usage scenario does not fit the requirements?
     c. What needs to be done so that they will be able to comply? Please specify the time frame required to achieve the compliance and provide information on what needs to be done during this period.
     d. Are these two clauses within the development plans for new medical devices? If not, when would these clauses be incorporated into the new medical devices?

6.2 Level 2 – Enhanced Security Requirements *(Para 22)*

22. Level 2 – Enhanced Security Requirements is premised upon the developer's declaration of conformity to a set of cybersecurity requirements (consisting of the four clauses in Level 1 and the remaining 34 clauses **-** please refer to the **Annex B2** for the details of these additional clauses). The manufacturer shall complete and submit a declaration of conformity for the 38 security requirements. CSA shall review the declaration of conformity and supporting evidence prior to approval of Level 2 label.

6.3 Level 3 – Software Binary Analysis & Time-Bound Black-box Penetration Testing

(Para 23)

23. Level 3 – Software Binary Analysis and Time-Bound Black-box Penetration Testing comprises the following components:

a. Declaration of Conformity to Security Requirements. The manufacturer shall complete and submit a declaration of conformity for the 38 cybersecurity requirements (clauses located in **Annex B1 and B2**). CSA shall review the declaration of conformity and supporting evidence prior to approval of Level 3 label.

b. Software Binary Analysis. The medical devices' software (firmware, companion mobile applications if any) will be analysed for **Common Vulnerabilities and Exposures (CVEs)** in third party libraries used, for malware, and for software weaknesses such as buffer overflow. The analysis will be performed with the aid of a combination of binary software composition analyser, malware scanner, and mobile application scanners. The scan results shall be reviewed and interpreted by the testing laboratory. At the end of this activity, the testing laboratory is expected to submit a report to CSA outlining the test results, identified issues, and corresponding method of resolutions to the issues.

c. Time-Bound Black-box Penetration Testing. A one-month time-bound black-box penetration testing by a testing laboratory is intended to **assert that the device is reasonably resistant to common attacks found applicable to medical devices, and to prove that there are no obvious or critical vulnerabilities**. Leveraging on basic tools and techniques as a trade-off for cost and effort, the penetration testing does not seek to assert that the medical device is resistant to all attacks. However, the penetration testing should provide basic assurance that the medical device is adequate to ward off the commonly known and straightforward attacks against such devices.

6.4 Level 4 – Time Bound White-box Security Evaluation *(Para 34 and 35)*

34. The time duration for adequate **black-box penetration testing and white-box security evaluation** are recommended to be **one month and three months respectively**.
    - *Time taken for actual testing work, not including the administrative tasks associated with the processing of the application.*

35. CSA considers **ETSI prEN17640** as the underlying security evaluation methodology more suitable for CLS Level 4, compared to a more formalised certification scheme such as Common Criteria (ISO/IEC 15408).

Feedback needed on:

1. The proposed time duration for Blackbox PT and White-box Security Evaluation.

2. The proposed methodology used for CLS(MD) Level 4 evaluation?

7. Requirements for CLS(MD) Testing Laboratories *(Para 36)*

36. The testing laboratory performing the Level 3 and Level 4 evaluations shall meet the following requirements:

i. **ISO/IEC 17025**: The testing laboratory shall be accredited or in the process of *accreditation (applicable for local laboratory only)* by the Singapore Accreditation Council (SAC)[10] or by other recognised Accreditation Bodies in accordance with the ISO/IEC 17025 for testing laboratories in the domain of IT/ICT/IoT security. The recognised Accreditation Body shall be a member of the International Accreditation Forum (IAF, https://www.iaf.nu/) and of the International Laboratory Accreditation Cooperation (ILAC, https://www.ilac.org/).

ii. **Quality System**: As part of ISO/IEC 17025 requirements, the testing laboratory shall have and comply with a quality system which is documented in a quality manual, defining the testing laboratory's policies and objectives, roles and responsibilities for managerial and technical staff members and procedures for control of documents and records.

[10] *The SAC is the National Accreditation Body for the independent accreditation of conformity assessment bodies in Singapore. More information regarding SAC is available at https://www.sac-accreditation.gov.sg/.*

7. Requirements for CLS(MD) Testing Laboratories *(Para 36) Continued*

iv. **Impartiality**: If the testing laboratory is part of an organisation that performs activities other than security evaluations (e.g. consultation to the developer, developer, etc.), 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 testing activities. The testing laboratory shall be an independent evaluation laboratory, free of any undue commercial, financial and other interest of the medical device it would be testing.

v. **Environmental Conditions**: The testing laboratory shall ensure that the environment in which it operates will not affect the correctness, reliability and confidentiality of the testing deliverables and results of the security testing and evaluation. For instance, access to and use of the testing laboratory premises must be controlled with effective separation of medical device security testing activities from other incompatible activities.

vi. **Methods**: The testing laboratory shall use methodology that conforms to the requirements of the CLS(MD) and any other applicable international or regional standards. All methods, procedures or instructions used during testing shall be documented. The testing laboratory shall ensure that specialised tools used are identifiable, subject to specific configuration management, and for the testing and results to be reproducible. The testing laboratory shall retain all records relating to the testing, including records of original observations, derived data and other relevant information, to establish an audit trail.

7. Requirements for CLS(MD) Testing Laboratories *(Para 36) Continued*

iv. **Security Policy**: The testing laboratory shall have an appropriate security policy, preferably conforming to ISO/IEC 27001 and shall be able to meet the security requirements for handling protected information related to the evaluation of medical devices. The security policy shall set out to maintain the high degree of security required to protect commercially sensitive information, specifying procedures for human resources security, physical and environmental security, communications and operations management and access control preferably with reference to the ISO/IEC 27001/2 standard. For guidance on implementing information security controls, the evaluation laboratory may refer to ISO/IEC 27002.

v. **Technical Competency**: The testing laboratory shall demonstrate to CSA that it is able to perform medical device security evaluations to the requirements of the scheme. The testing laboratory shall ensure the training needs of staff members are identified and provided for. The staff members of the testing laboratory are expected to demonstrate their technical competency, either by proof of qualification, a written test, or other appropriate means.

8.1 Proposed Design and Conditions of the Cybersecurity Label *(Para 39-42)*

39. The proposed designs and sizes of the Cybersecurity Labels are below:

Minimum Size
25x10mm

Medium Size
40x30mm

Large Size
60x45mm

40. The label shall be affixed on the packaging of devices that can be sold to non-qualified practitioners. This is to increase the awareness of the device cybersecurity capabilities for consumers to make informed purchases.

41. For professional-use-only devices, the affixing of the label is optional because measures are in place for professional bodies to purchase the appropriate devices.

42. Labelled devices will be listed in the CLS(MD) product list within the CSA website.

8.2 Validity of the Label *(Para 46-49)*

46. The **Level 1 Cybersecurity Label is valid for a period of three (3) years**, during which the developer is required to support the device with security updates. A self-declaration for CLS(MD) Level 1 requirements by the developer is required for renewal and to be submitted directly to CSA.

47. The **Levels 2/3/4 Cybersecurity Labels** are valid for the period in which the developer will support the device with security updates, up to a **maximum of three (3) years**.

48. The label could be **revoked** if any of the conditions in para 50 or 51 are met. (see next 2 slides)

49. Before expiry of the label, a new CLS(MD) application is required to obtain a new label. This process can be initiated three (3) months before the expiry date of the existing label.

8.3 Labelling Principles *(Para 50)*

50. Upon receipt of the CLS(MD) label, the developer 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. CSA shall be informed immediately of any changes that could affect the ability of the developer/product to fulfil the CLS(MD) requirements.
c. The developer must not make any statements about its product labelling that CSA 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; and claiming the product received a label of higher rating than what is being issued.
d. The developer must not use the Cybersecurity Label in any way that could discredit either MOH, CSA, HSA, IHiS, or CLS(MD).
e. The label must not be modified and shall be used exactly as issued by CSA.

8.4 Revocation of the Label *(Para 51)*

51. The developer is in breach of any terms of CLS(MD) requirements, and/or any other terms as agreed to in writing with CSA, if any of the following conditions is/are met:

    a. The developer has failed to disclose any known or discovered vulnerabilities that, in CSA's opinion, can undermine the CLS(MD) label;
    b. The developer fails to take any corrective measures during the grace period given by CSA, to the satisfaction of CSA;
    c. The developer misuses the CLS(MD) label, CLS(MD) status, or any proprietary names and marks associated with CSA or CLS(MD);
    d. The developer makes any statement that misrepresents any aspect of testing or the effect of the labelling under the CLS(MD);
    e. CSA finds that the testing laboratory was in a position of conflict that impaired its ability to conduct a fair and impartial testing of the device;
    f. 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 CSA after the device was originally labelled;
    g. CSA discovered that the developer has made a false statement or declaration in any deliverables submitted to CSA.

9. Operationalisation *(Para 52-55)*

52. Application for the CLS(MD) labelling for Classes B, C and D devices shall be made via HSA's **MEDICS platform**, as per current practice for new medical device registration application, except for Special Access Route (SAR) devices.

53. Medical devices will have met Level 1 requirements prior to local market availability except for SAR devices. **Higher-level labelling will be voluntary, subject to developer's own business development model and individual healthcare institution purchasing requirement.**

54. SAR devices can also apply for CLS(MD) labelling. SAR devices (and all medical devices in general) that are not CLS(MD) labelled may not be allowed to be connected to public healthcare network after an appropriate stipulated sunrise period. This sunrise period will be determined and proposed separately, depending on the readiness of the developer and sector.

55. For **Class A devices**, existing HSA's process for self-declaration remains. No CLS(MD) label will be issued by default. Manufacturers who wish to obtain the CLS(MD) Level 1 label for labelling on the device shall additionally apply directly to CSA, submitting the declaration form, as well as corresponding evidences. The application will be reviewed in a similar manner to those of Class B to D devices, and approval given for them to include the label.

9. Operationalisation *(Para 56)*

56. Due to the large volume and diversity of medical devices in the market, CSA would like to pace the **implementation of the scheme by prioritising device types** based on risk, impact to patient safety and risk, volume of use and connectedness. The proposed device categories are shown in Table 1 below and provided in the prescribed template for your feedback.

No.	Device categories
1	Radiological Imaging Devices (e.g. X-Ray, CT)
2	In-vitro Diagnostic Analysers (e.g. SARS-CoV-2 PCR machine)
3	Patient Monitors
4	Cardiac Electrical Implants (e.g. Pacemakers, cardiac monitor, implantable defibrillator)
5	Diabetic Management System (e.g. Continuous blood glucose sensor + Insulin pen + mobile app for insulin bolus calculation)
6	Insulin Pumps
7	Respiratory Ventilators
8	Clinical Decision Support Software (e.g. software to analyse CT chest images for detection of lesions)
9	Radiation Therapy System (For cancer treatment)
10	Medical Mobile Applications that run on general computing device (e.g. ECG app running on smartwatch)
11	Digital Therapeutic Software (e.g. deliver cognitive behavioural therapy for patients with substance Use Disorder)
12	Others

Feedback is needed:

- Do you agree with the paced implementation approach?
- Please select the top 3 devices from the list of device categories and the reasons.
- If “Others” is selected, please provide the device category and the relevant reason.

High level view of the Certification Process by CSA

Application

- Manufacturer to apply for CLS (MD) via Registration Platform (MEDICS & FORMSG).
- Manufacturer to provide Application Deliverables to CSA and Test Lab.
  - *Note: The manufacturer will need to engage a test lab if the intended application level is Level 3/4.*
- Manufacturer will receive Acceptance of application (Notification) if the application is accepted.

Testing and Evaluation

- Level 1/2: Manufacturer will provide the conformity and other application deliverables to CSA for CSA to perform the review of the conformity.
- Level 3/4: Manufacturer will liaise with the test lab for the software binary analysis penetration (L3), penetration testing (L3), and security evaluation (L4).
  - *The test lab will provide the test reports to CSA (L3 and L4). The lab together with the manufacturer shall work with CSA on any outstanding issues and required clarifications regarding the test reports.*

Approval and Issuance of Cybersecurity Label

- Manufacturer will receive an Approval notification if the application has been successful.
- Manufacturer will receive the Cybersecurity Label.
- The manufacturer's product will be updated in the CSA website under the CLS(MD) approved products list.

Progressive framework assessment and application process

Evaluation and Testing	Level 1	Level 2	Level 3	Level 4
Conformity to Security Baseline Requirements	Yes	Yes	Yes	Yes
Conformity to Enhanced Security Requirements		Yes	Yes	Yes
Software Binary Analysis			Yes	Yes
Time-Bound Blackbox Penetration Testing			Yes	
Time-Bound Whitebox Security Evaluation				Yes

In summary,

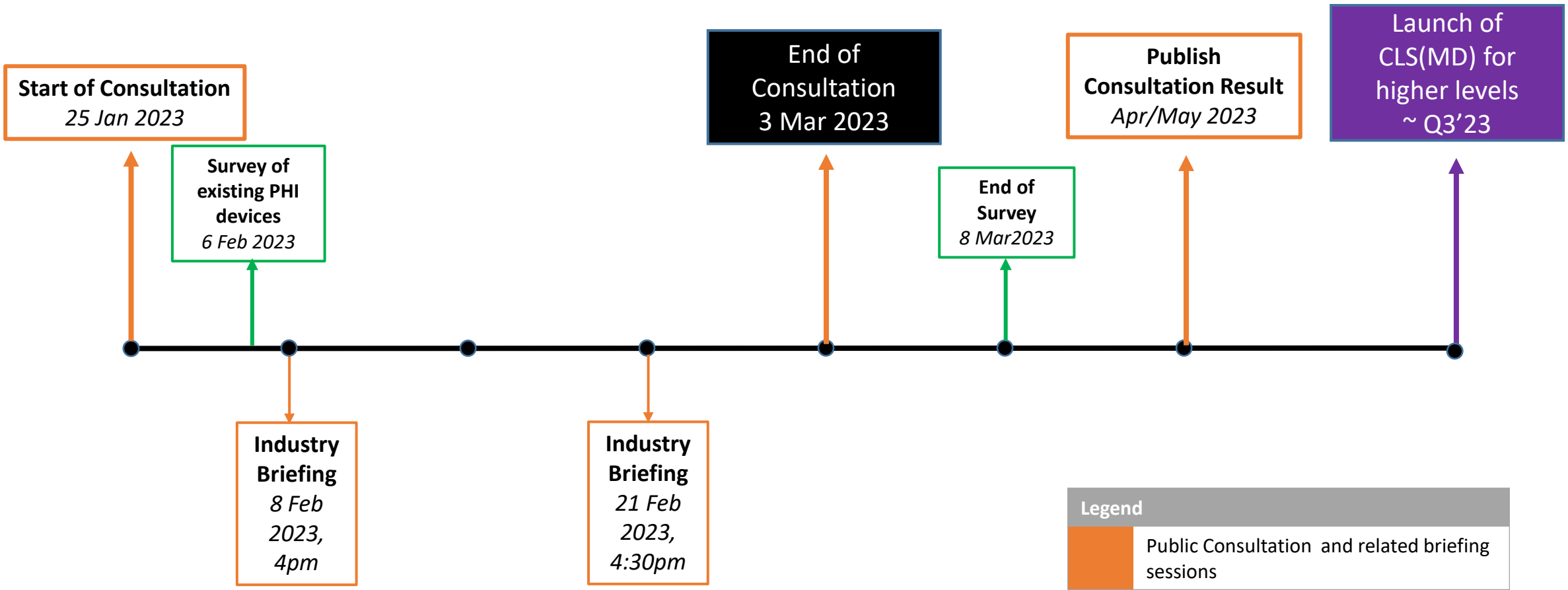
- CLS(MD) Level 1 applicants must meet the Security Baseline Requirements.
- CLS(MD) Level 2 applicants must meet the requirements from Level 1, and the Enhanced Security Requirements.
- CLS(MD) Level 3 applicants must meet the requirements from Level 2, conduct Software Binary Analysis and Time-Bound Blackbox Penetration Testing.
- CLS(MD) Level 4 applicants must meet the requirements from Level 3, and Time-Bound Whitebox Security Evaluation.

10. Devices that are currently in use *(Para 57 and 58)*

57. For classes A to D devices that were approved/declared prior to the implementation of the CLS(MD) and wish to obtain a CLS(MD) Level 1 label, manufacturers or vendors must perform a self-declaration for CLS(MD) Level 1 compliance with supporting evidence submission to CSA directly.

58. As existing devices have already been approved for use, they can remain in the market even if no labelling is sought. However, **device use policies may impose limitations on purchase and use, in view of the cybersecurity threat landscape.**

Timelines



Legend	
	Public Consultation and related briefing sessions
	Survey of existing PHI devices (for selected vendors)
	Scheme Launch with higher levels

Summary

3 Mar'23 is the final date for feedback submission.

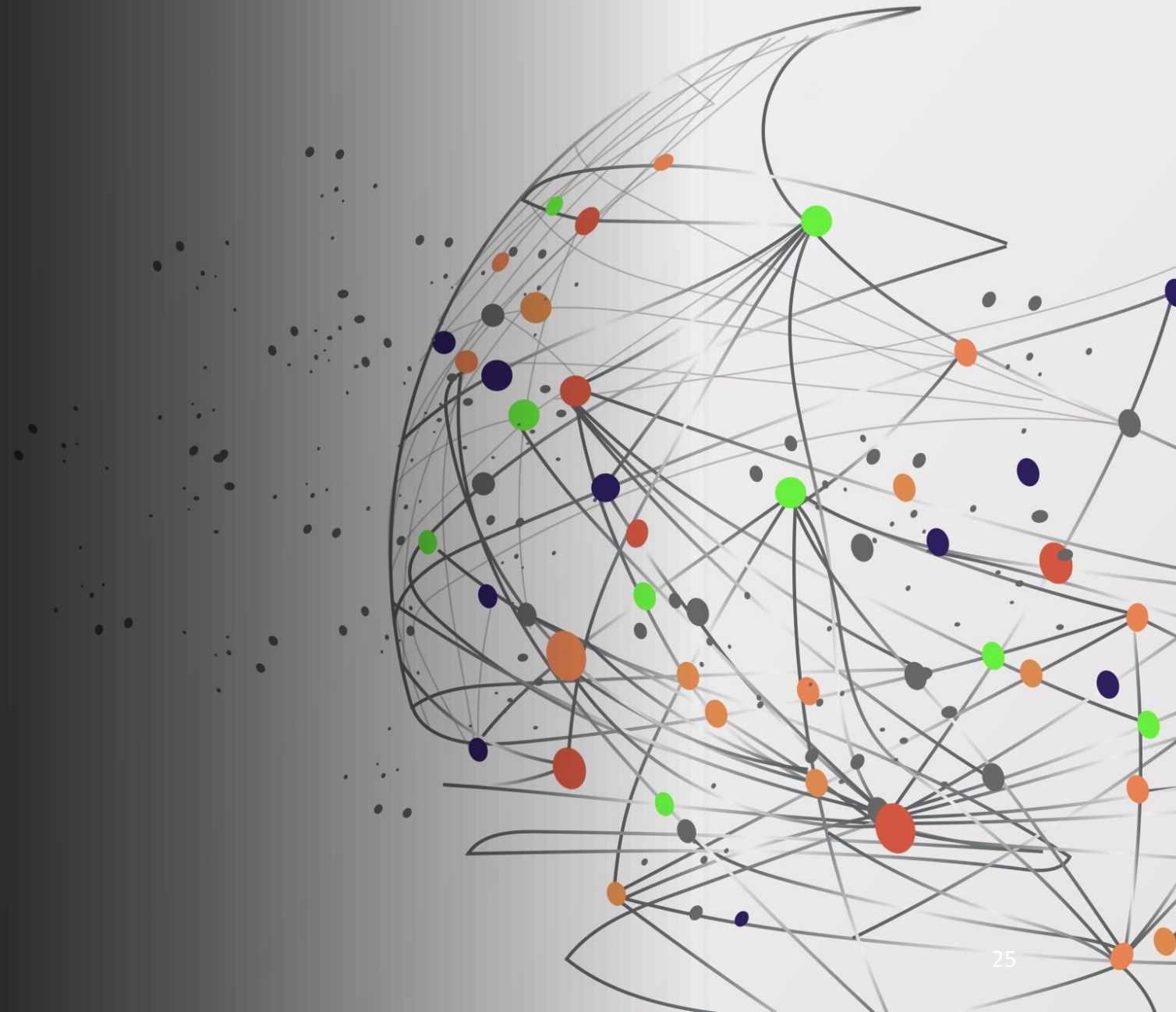
Please use the prescribed **template "Feedback Form.xlsx"** provided on the CSA website for your responses and

Send your feedback to certification@csa.gov.sg

Do write to us at certification@csa.gov.sg should you have queries relating to Consultation Paper

End of Presentation

Thank you



Link to the Consultation Paper and Feedback Form

https://go.gov.sg/cls-md-consultation