




Cybersecurity Labelling Scheme (CLS)



Soon-Chia, LIM
Director (CSEC) / Head CCC
Cyber Security Agency of Singapore

Singapore: Many Smart Ideas, One Smart Nation



- National Digital Identity
- Digital Government Services
- Smart Nation Sensor Platform
- Smart Urban Mobility
- Smart Homes
- Health Services
- E-Payments



SINGAPORE IS A COMMON CRITERIA CERTIFICATE AUTHORISING NATION



THE STRAITS TIMES

Debate on ministries' budgets: Communications and Information

Parliament: Certification boost for Singapore's cyber security products

🕒 PUBLISHED MAR 5, 2019, 5:00 AM SGT

Having globally recognised tests done here will lead to time and cost savings of over 20%: Janil



Hariz Baharudin (mailto:harizbah@sph.com.sg)

Cyber security products developed in Singapore can be certified as well on an internationally recognised standard here, a move that will shorten the time plus lower the costs and barriers that local developers face in getting their products accepted worldwide.

Certification Schemes

Singapore Common Criteria Scheme



BY CYBER SECURITY AGENCY OF SINGAPORE

National IT Evaluation Scheme



BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme



BY CYBER SECURITY AGENCY OF SINGAPORE

- Promoting CC/NITES regime - mandatory consideration for product assurance
- Strong local and international interest in Cybersecurity Labelling Scheme
- Exploring IEC 62443 (Industrial IoT) to enhance cybersecurity for OT/IloTs

International IoT Security Roundtable

- **Share** ideas and experience
- **Shape** technologies and architectures
- **Steer** standards and accelerate growth of smart cities at international level



Principles, Governance and Legislation

Cybersecurity and Privacy by Design

IoT Security Standards and Guidelines

Evaluation and Certification

Future-Proof Legislation

Ecosystem Development

Responsible Industry

Supply Chain Security

Product Life Cycle Support

Technical References and Standards

Device Identities and Root of Trust

Secure OS, Cloud and Applications

Secure Communications and Infrastructure

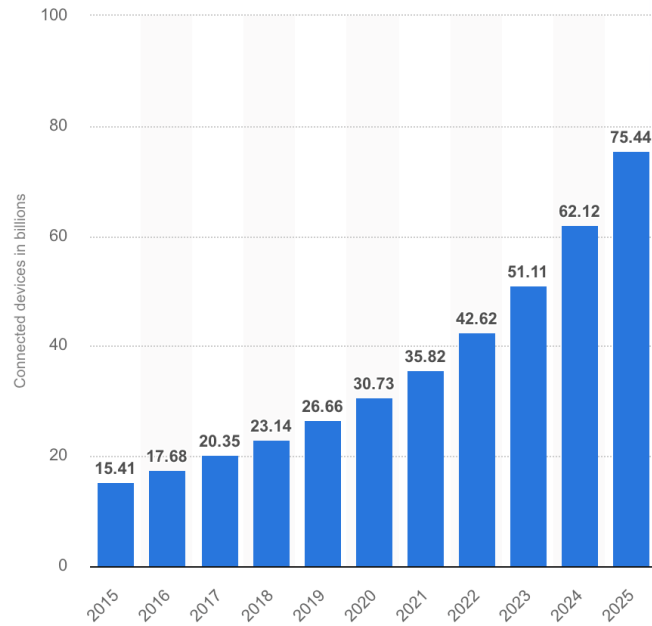
Security Monitoring and Analytics





<https://youtu.be/JJubrOX0FWY>

Growing IoT Cybersecurity Concerns



Russia-linked Strontium APT targets IoT devices to hack corporate networks



Statista Research Department: 75 billion IoT devices connected to the internet by 2025.

1

Short time-to-market, quick obsolescence, limited device resources

3

Evaluation and certification overheads

2

Scalability – Not practical for a single nation/organisation to evaluate and certify thousands of IoT products

4

Security is hard to quantify, and opaque to customers

Intent of Cybersecurity Labelling Scheme



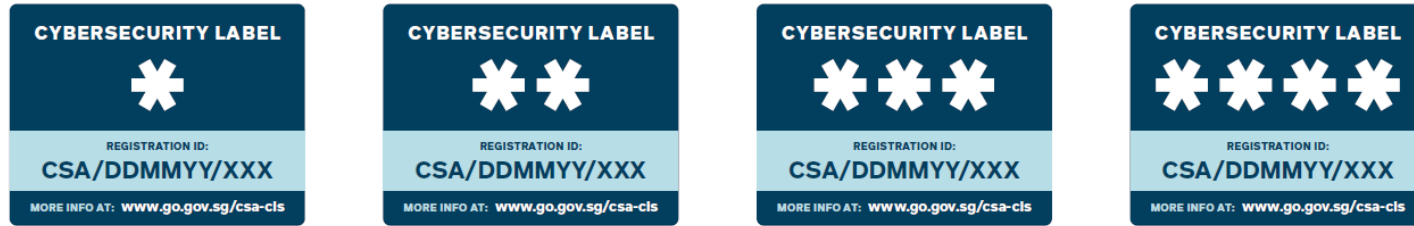
Making cybersecurity provisions transparent to consumers and enabling them to differentiate against poorly secured devices



Help manufacturers to differentiate themselves in the market and thus, incentivise manufacturers to produce more secure devices



To grow the economy, working with International Partners for mutual recognition to reduce duplicated testing and improve market access

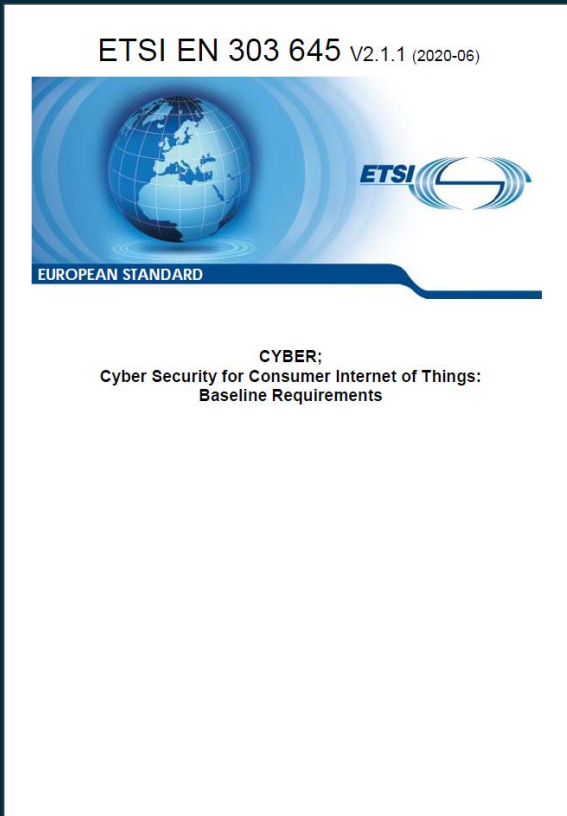


- 3rd Party Independent Testing
- Developer Declaration of Conformance

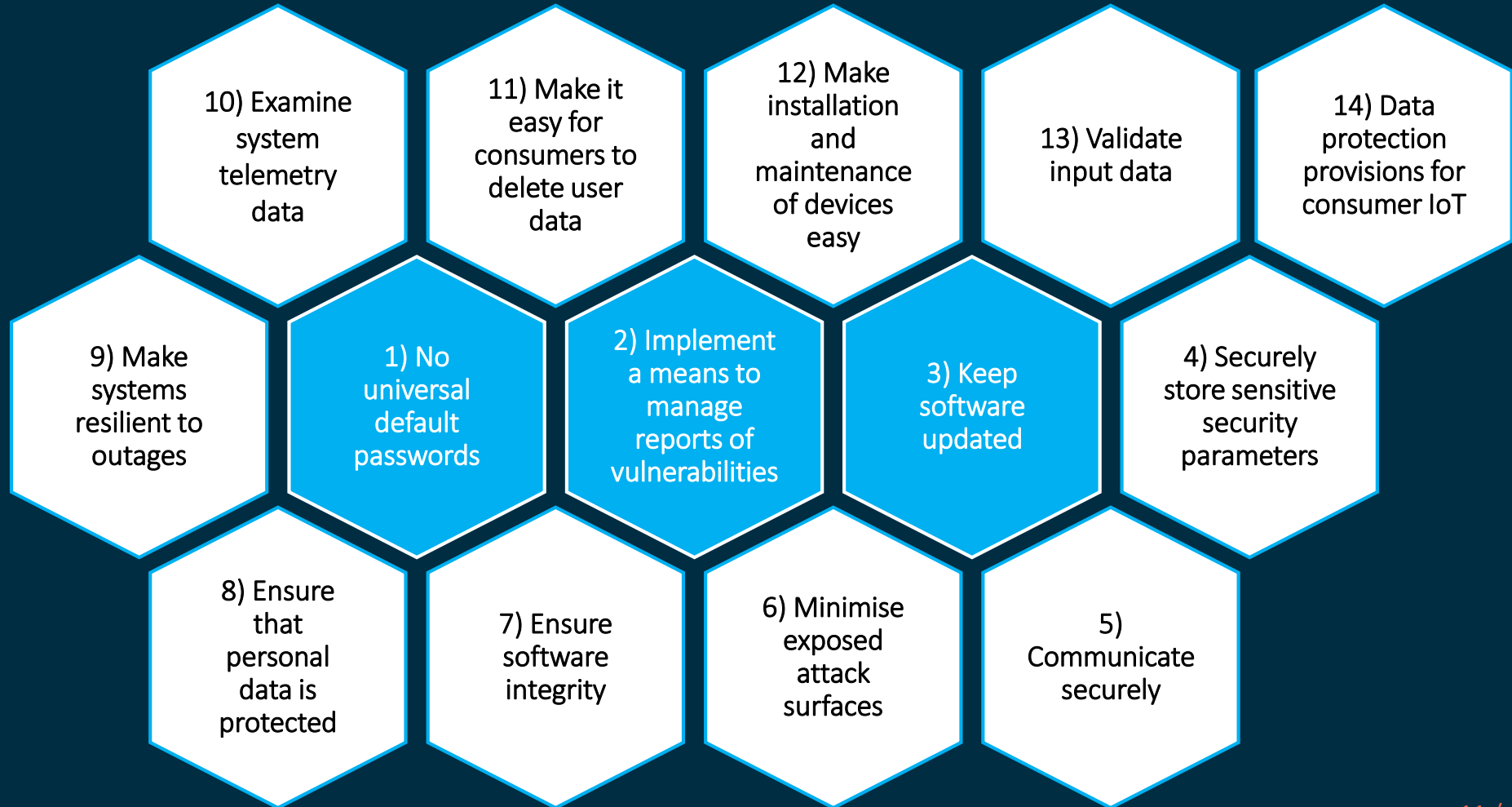
		Tier 4 – Pen Testing
	Tier 3 - Software Binary Analysis	

		Tier 2 - Lifecycle Requirements	
	Tier 1 - Security Baseline Requirements		

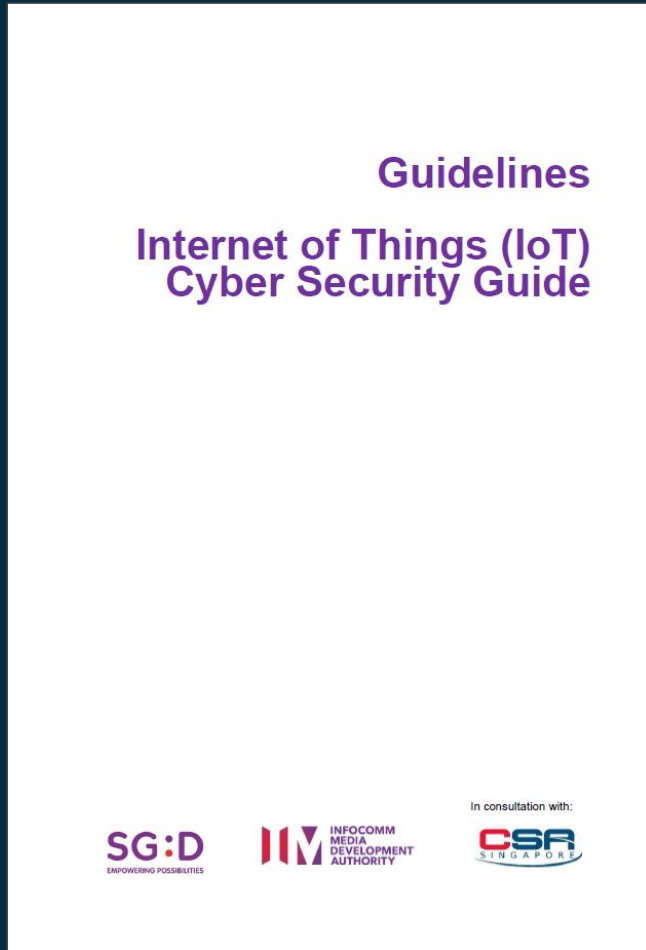
Assessment Tier 1 – Security Baseline Requirements



ETSI EN 303 645



Assessment Tier 2 – Lifecycle Requirements



Process

1. Developers to send completed conformance checklist (with supporting evidences) to CCC.
2. Conformance Checklist will be reviewed by CCC prior to approval.

Assessment Tier 3 – Software Binary Analysis

Quick Checks using Automated Tools

Software Binary Analysis

Expected duration: 3 – 5 days

Coverage:

Firmware Binary

Companion Mobile Application Analysis (if any)
(Android and iOS)

Test Scope:

Software Composition Analysis

Software Errors

Mobile Application Analysis

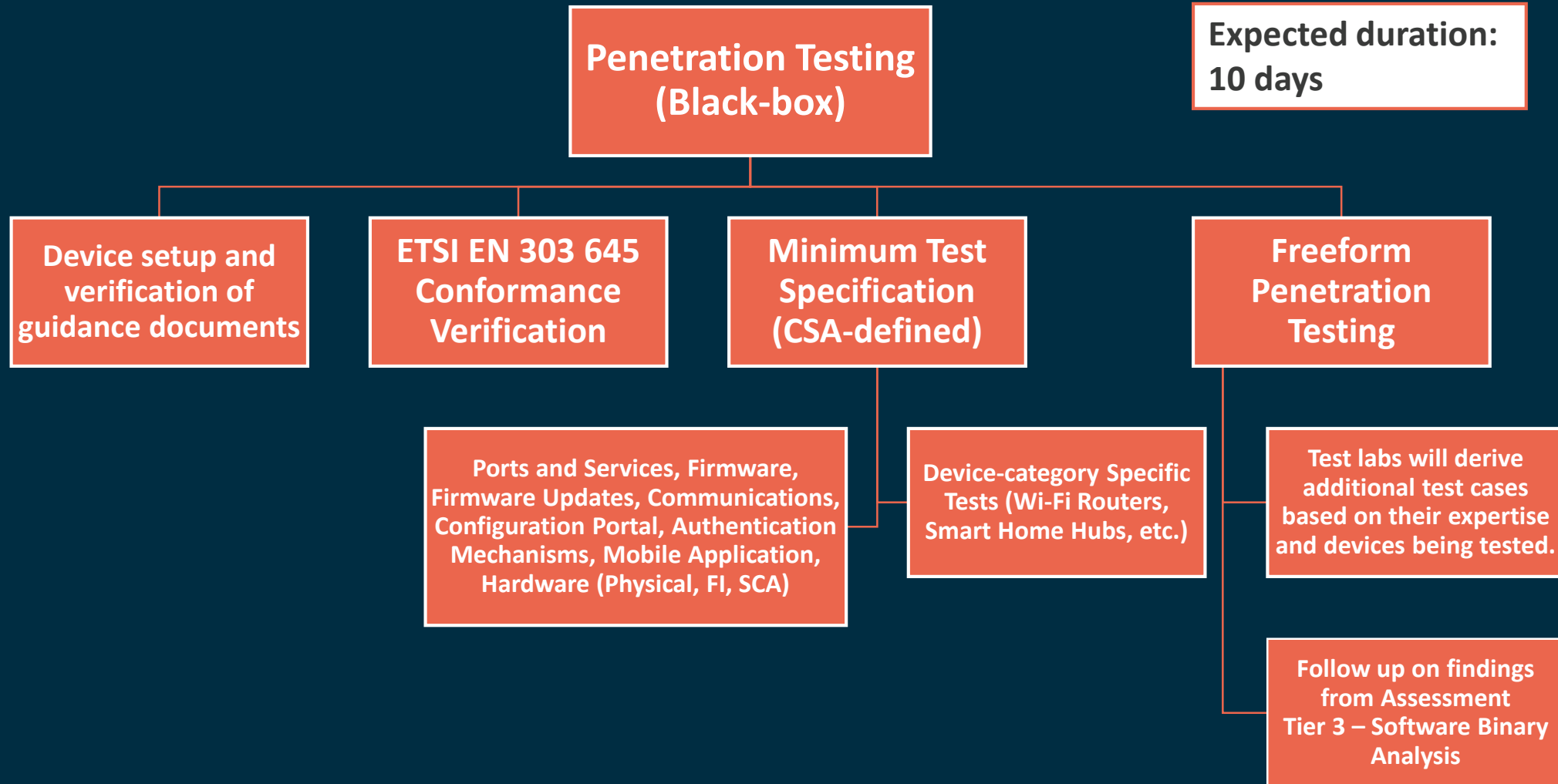
Third-party software component and related vulnerabilities

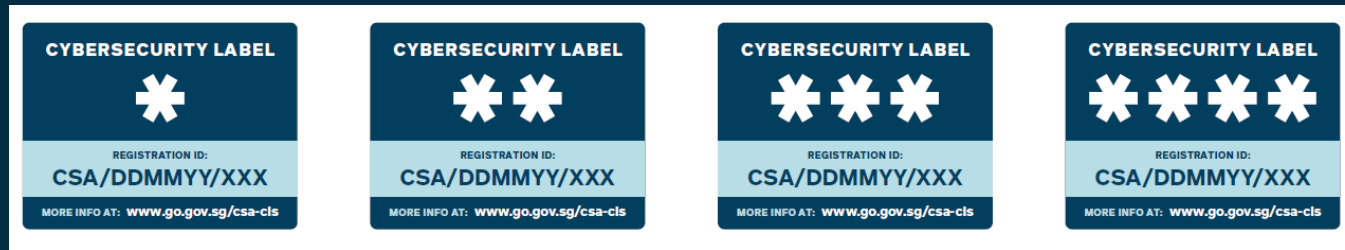
Hard-coded sensitive keys and materials

Buffer Overflow, Use After Free, NULL Pointer Dereference, etc.

Permissions and Services, embedded credentials etc.

Assessment Tier 4 – Penetration Testing





Cybersecurity Labelling Scheme – Key Attributes

- The CLS is launched as a **voluntary** scheme for a start.
“**Not Letting Perfection be the Enemy of Good**”
- It is **not a static scheme** – evolving with dynamic threat landscape, and **let ‘water finds its level’** based on market interest, acceptance and readiness.
- It is **flexible – not one size fits all**. Self-declaration for basic hygiene, independent 3rd party assessment for higher assurance
- **Cost-effective and Consistent**
- Link: <https://go.gov.sg/csa-cls>



Wi-Fi Routers



Smart Home Hubs

Validity of Label

- Validity of label is tied to the length of time for which the device be supported with security updates, up to a maximum of 3 years
- Device should receive updates regularly. Typical update cycles range from 30 to 90 days, subjected to the nature of the product.
- If a device is found to be not conformant to requirements, the label shall be revoked.
- CSA shall conduct random surveillance on labelled products sold in the market.

Testing Laboratories for CLS

Laboratory Name	
<p><u>An Security Pte Ltd</u> Address: 124 Geylang Lorong 23, #02-01 ArcSphere, Singapore 388405</p>	<p><u>T-Systems International GmbH</u> Address: Bonner Talweg 100, 53113 Bonn, Germany</p>
<p><u>Brightsight B.V.</u> Address: Brassersplein 2, 2612 CT Delft, The Netherlands</p>	<p><u>TUV Informationstechnik GmbH</u> TUV NORD GROUP Address: Langemarckstr. 20, 45141 Essen, Germany</p>
<p><u>Riscure BV</u> Address: Delftechpark 49, 2628 XJ Delft, The Netherlands</p>	<p><u>UL Verification Services Pte Ltd</u> Address: 1 Fusionopolis Walk #10-01 Solaris Tower Singapore 132628</p>

CLS Publications

Publications	Description
CLS Pub #1 – Overview of the Scheme	Provides an overview of the scheme <ul style="list-style-type: none"> - Scheme objectives, description, organisation and management - Overview of the testing process
CLS Pub #2 – Scheme Specifications	Provides detailed process overview of the 4 assessment tiers
CLS Pub – Minimum Test Specifications and Methodology for Tier 4	Provides detailed information about the minimum testing that is to be performed by testing laboratories during Assessment Tier 4

Thank You

