



Security Conference 2022

Transforming Mindsets, Harmonising Standards - Cybersecurity Labelling Scheme (CLS) & Beyond

Soon Chia, LIM

Director (Cyber Security Engineering Centre),
Cyber Security Agency of Singapore

04/10/2022





Enhancing Cybersecurity

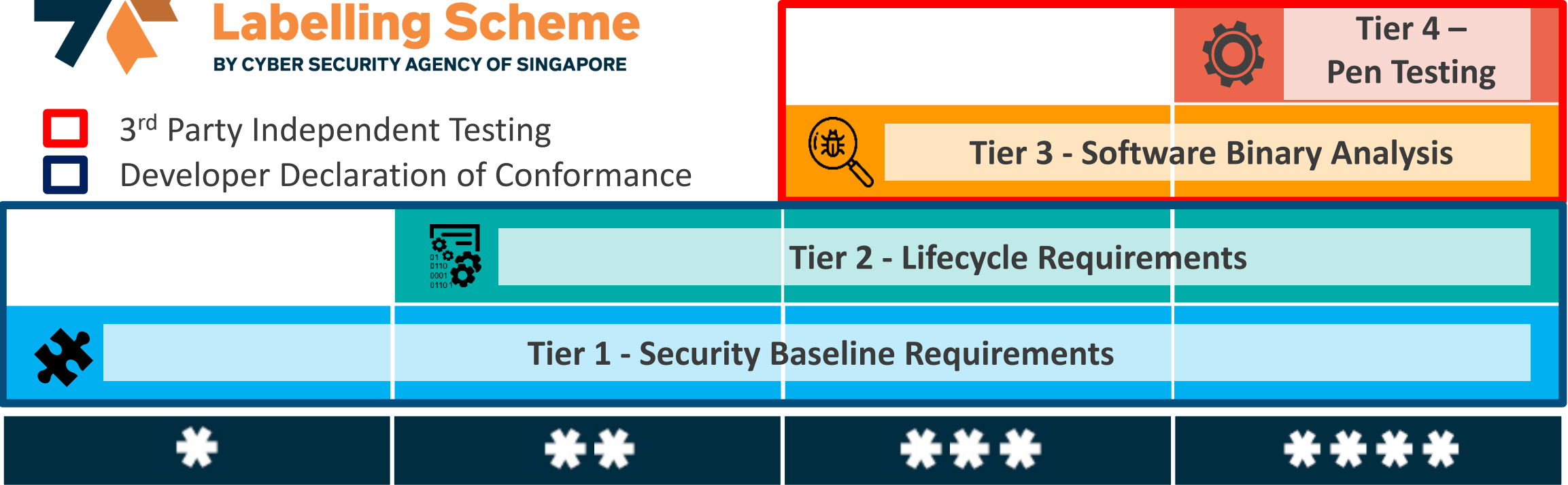


Overview of Cybersecurity Labelling Scheme (CLS)



Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE

-  3rd Party Independent Testing
-  Developer Declaration of Conformance



1. **Cost effective:** Combination of self-declaration and 3rd party independent testing caters to different needs and risk appetite
2. **Robust:** Caters for consumers, developers and economy
3. **Risk-based approach:** Primarily voluntary scheme; Mandated for specific critical devices (e.g. Wifi router)
4. **Interoperable:** Leveraging on **ETSI EN 303 645** which is widely adopted, it facilitates mutual recognition
5. **Does not stifle innovation:** Progressive steps allows flexibility for developers based on their readiness and market dynamics.

Benefits of Cybersecurity Labelling

TRANSPARENCY



Consumers

Make cybersecurity provisions transparent to consumers and enable them to differentiate the against poorly secured devices

BRANDING



Developers

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

MUTUAL RECOGNITION



Economy

Grow the economy by working with international partners for mutual recognition to reduce duplicated testing and improve market access



- **Reduce attack surface, enhance security**
- **Safer and more secure cyberspace**



Leveraging EN 303 645

An international standard for the assurance of consumer IoT

ETSI EN 303 645



Catalyst for global adoption

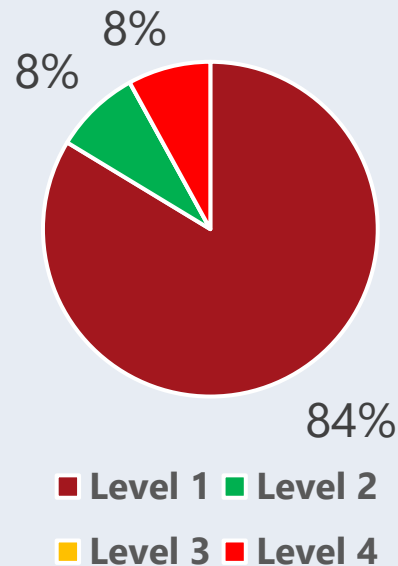
The only standard focused on consumer IoT

Provides basis for global adoption and mutual recognition among countries

Raising cyber hygiene levels through the CLS

More than **200** labelled devices since launch in Oct 2020

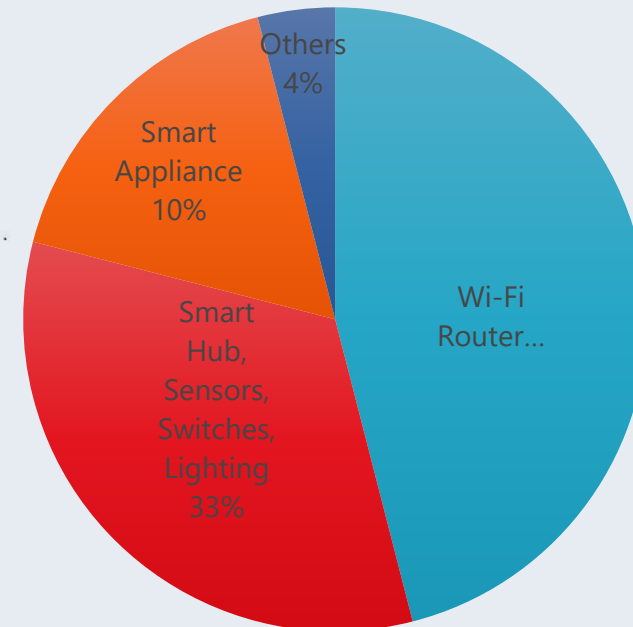
Applications for CLS by levels



Manufacturers seeking higher levels of security labelling

Current observation indicates increased interest to develop more secure products, with developers applying for higher levels after obtaining level 1.

Device Categories



Keen Interest in adoption by the Industry



Leading global brands includes such as Google, Linksys, Asus, TP-Link, Koble, Philips Industry recognises how CLS could **gain consumer confidence**....

ASUS Cybersecurity Labelling Scheme
RT-AX88U & GT-AX11000 WiFi 6 Routers
Certified Level 4 Under The Cybersecurity Labelling Scheme

Cybersecurity Levels & Assessment Tiers			
Cybersecurity Level ★★★★	Tier 1 Security Baseline Requirements	Tier 2 Lifecycle Requirements	Tier 3 Software Binary Analysis
	Tier 4 Penetration Testing		
	Developer Declaration of Conformance	Third Party Independent Laboratory Testing	

For business enquiries: Enterprise_Sg@asus.com

STAY CYBER-SAFE
Cybersecurity Labelling Scheme (CLS) Level 1
Philips Hue Bridge V2.1
REGISTRATION ID: CSA/090225/V0009

PROLINK Xtend Pro WHOLE HOME MESH WI-FI SYSTEM PRC2402M
REGISTRATION ID: CSA/150224/T0006

Tack
REGISTRATION ID: CSA/180125/V0002

Meet the new Nest Wifi.
Strong connection. Every direction.

CYBERSECURITY LABEL
REGISTRATION ID: CSA/290924/U0021
MORE INFO AT: www.go.gov.sg/csa-clt

CYBERSECURITY LABEL
REGISTRATION ID: CSA/020225/V0008

CYBERSECURITY LABEL
REGISTRATION ID: CSA/150128/V0001

LazMall HOME@UTO zigbee Zigbee WiFi Hub
REGISTRATION ID: CSA/170128/V0008

LazMall HOME@UTO zigbee SMART WALL SWITCHES (1/2/3 Gang)
REGISTRATION ID: CSA/071221/U0012

KOBLE Smart Hub (Zigbee)
REGISTRATION ID: CSA/180224/L0002

ASUS RT-AX92U (1-PK) AX6100 Tri-Band WiFi 6 (802.11ax)

ASUS ZenWiFi AX (XT8) AX6600 Tri-band Whole Home Mesh

ASUS ZenWiFi AX Mini (XD4) BLACK (2 PACK) Whole Home

Aztech KSMT-110-WF Smart Station

Aztech Zigbee Smart Hub

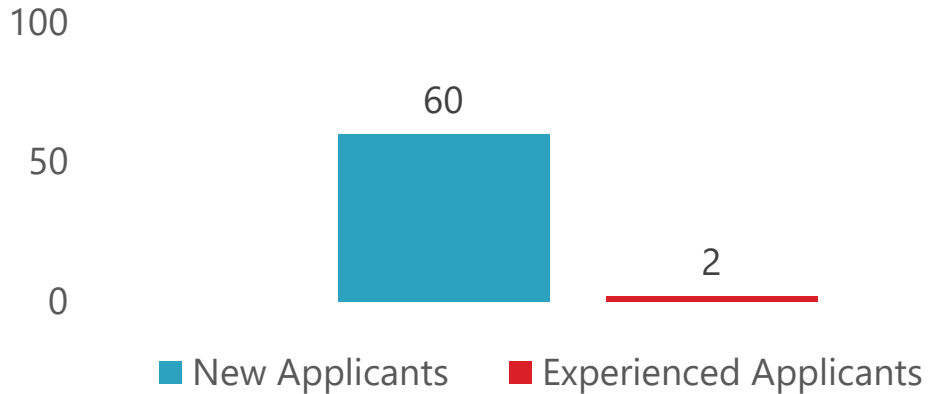
HOME@UTO zigbee Zigbee WiFi Hub

HOME@UTO zigbee SMART WALL SWITCHES (1/2/3 Gang)

CLS continues to evolves

EFFICIENCY AND SCALABILITY

Average No. of Days taken for CLS Level 1



Manufacturers not ready for CLS Level 1
Ave Labelling applications take 60 days!!

Time, Support and Guidance Required
Manufacturers needed time to make engineering changes to meet requirements, to put in place support policy.

Asking for more and higher assurance
Turn-around time within a few days for experienced developers.

EVOLVING NEEDS

- **Default password and authentication**
 - Newer devices are requiring user to setup new account and password during initial set up
 - Need to emphasize on having strong passwords and authentication rate limiting
- **Increased scope for self-declaration**
 - Given familiarity with the 3 basic requirements, possible to encourage manufacturers to move up CLS, and towards full conformity of EN303 645
 - Review level 2 & 3 with collaborators to incorporate full EN 303 645 requirements
- **CLS-Ready**
 - Composite evaluation for high assurance components to be labelled once and use for many.
 - Enabled IoT devices to attain high assurance cost effectively

Future of CLS: Extension to medical IoT

Challenges



Inadequate protection of sensitive medical data.



Devices using default passwords are fairly common in the industry.



Unsecured communication protocols being used by devices.

Approach

To improve medical devices security through the use of a Cybersecurity Labelling Scheme for Medical Devices [CLS (MD)].

Applicability:

Medical Devices (regulated under the Health Products Act) that either handles sensitive data or are connected to systems, devices and services.



Minimum Baseline:

Guidance for medical devices to attain cybersecurity capabilities that commensurate with the expected cyber threats.



Phased Approach for Adoption:

Starting from voluntary phases to mandatory requirement.

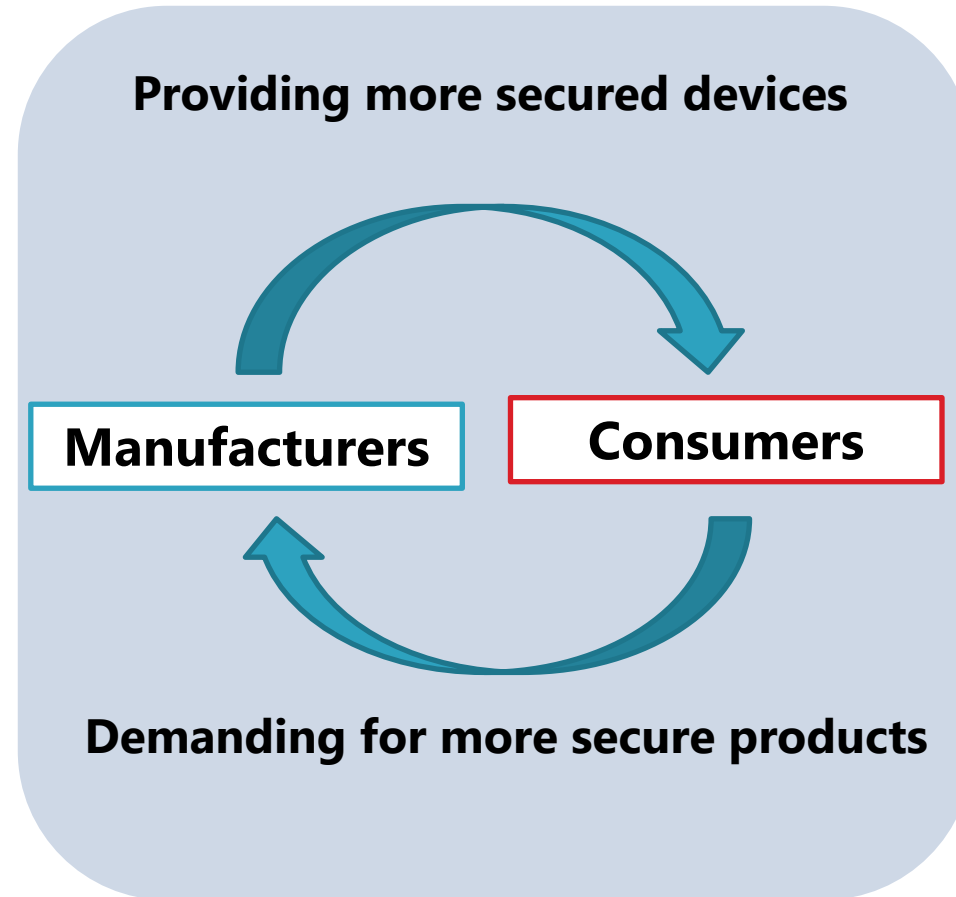
Transforming Mindsets

Through agile governance



Transforming Mindsets

Towards a
proactive and
sustainable
industry



Getting
consumers
digital future
ready

Towards a Proactive and Sustainable Industry

AGILE GOVERNANCE



Paradigm shift away from conventional developer-centric, compliance-focused approach

Fast pace of emerging technology. Waiting for legislation for compliance, often too little too late.

One step in the door – Low entry bar that don't stifle innovation.

Progressive level – nudging and aspire for higher assurance

COMPETITIVE BRANDING



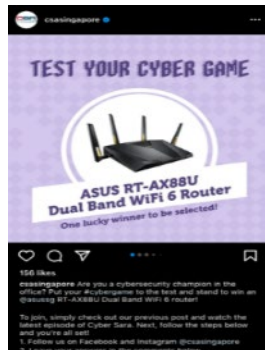
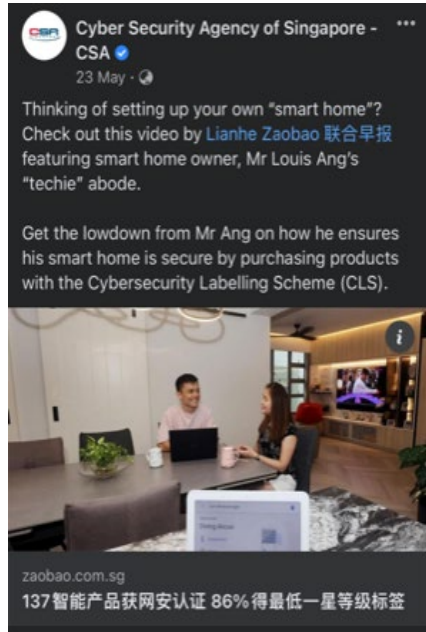
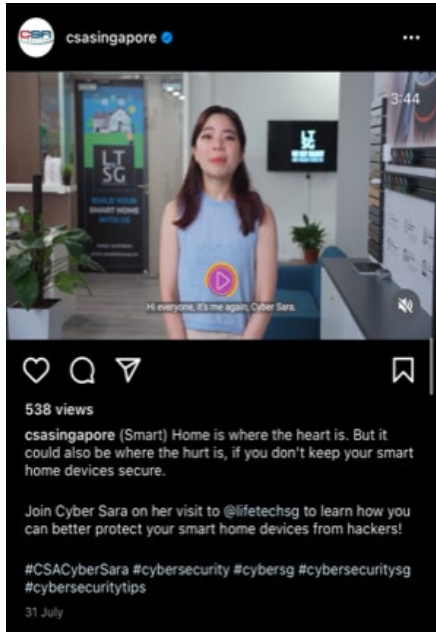
Leverage on market dynamics, and competitive branding to differentiate products

Top-tier companies – Not settling with the second best. Aiming for CLS 4

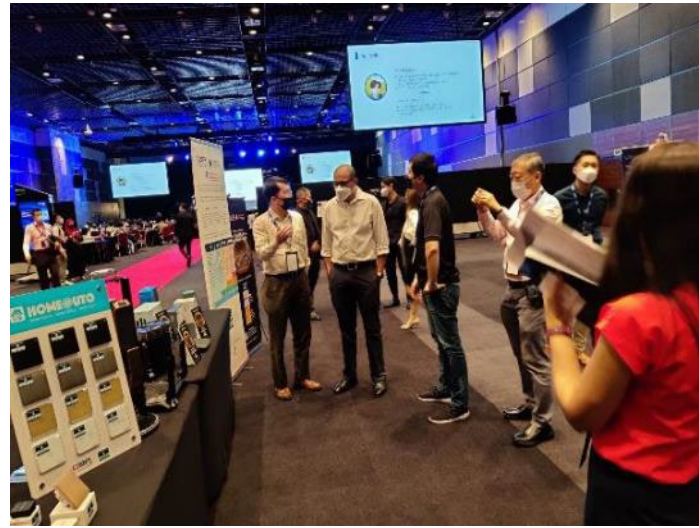
Lower-tier companies seeks to onboard more products for baseline assurance, while exploring higher level with more attaining common baseline

Getting Consumers Digital Future Ready

Social Media



Public Roadshows



Not just about labelled products....
..... its about transforming mindsets to be ready for our digital future!

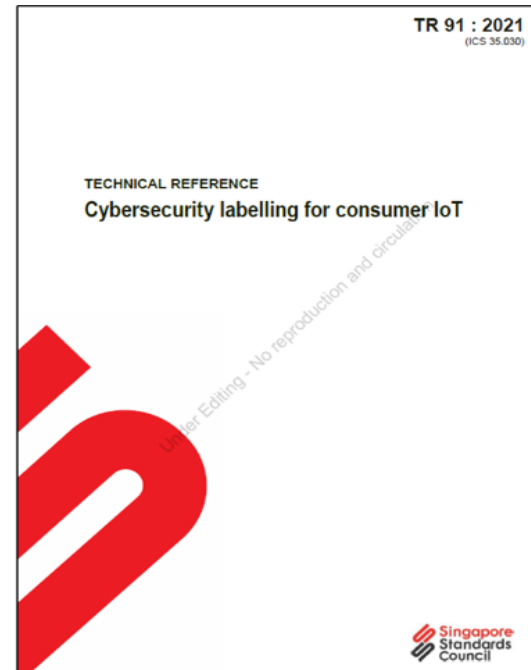
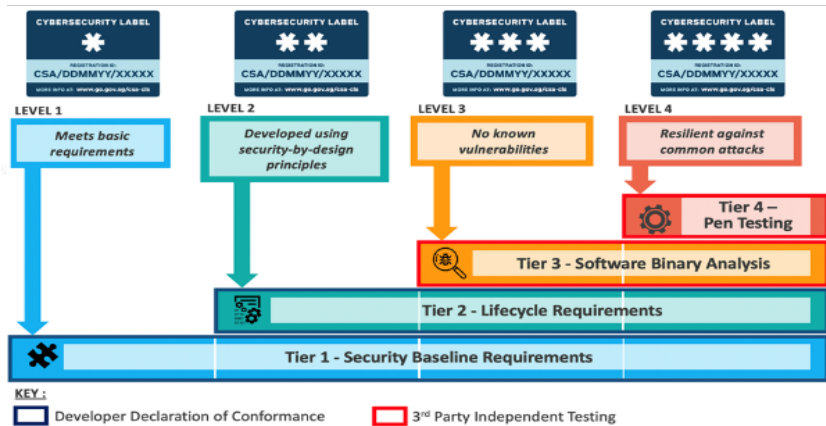
Harmonising Standards

... Internationally to avert further fragmentation



Translation of CLS to a National Standard

Technical Reference on Cybersecurity Labelling for Consumer IoT (TR 91)



Crystallised design principles and concepts of the CLS labels and assessment tiers to provide guidance to manufacturers, developers, testing bodies and suppliers of consumer IoT devices

Publication of the national standard announced at the Singapore International Cyber Week in Oct 2021

Early Efforts for International Recognition



White House considers cybersecurity ratings to boost visibility

- US is contemplating the use of cybersecurity ratings and standards for US software
- CLS was cited as an example of how cybersecurity ratings were provided for IoT devices to provide more transparency



- Labelled product by Singapore at CLS 3 /4 will be accorded a Finnish Label
- Finnish labelled product will be accorded a CLS 3 label

Results of Mutual Recognition Agreement

Mutual recognition between Singapore and Finland allows products tested under either party to be recognized mutually.

Example of products with Finland's Traficom Cybersecurity Label accorded Singapore's CLS level 3



Philips Hue Bridge smart lighting device

Polar Vantage M2



Polar Unite

Polar Grit X Pro



Polar Ignite 2

Polar Vantage V2



Example of products labelled under Singapore's CLS issued with Finland's Traficom Cybersecurity Label



Asus Zen wifi XD6

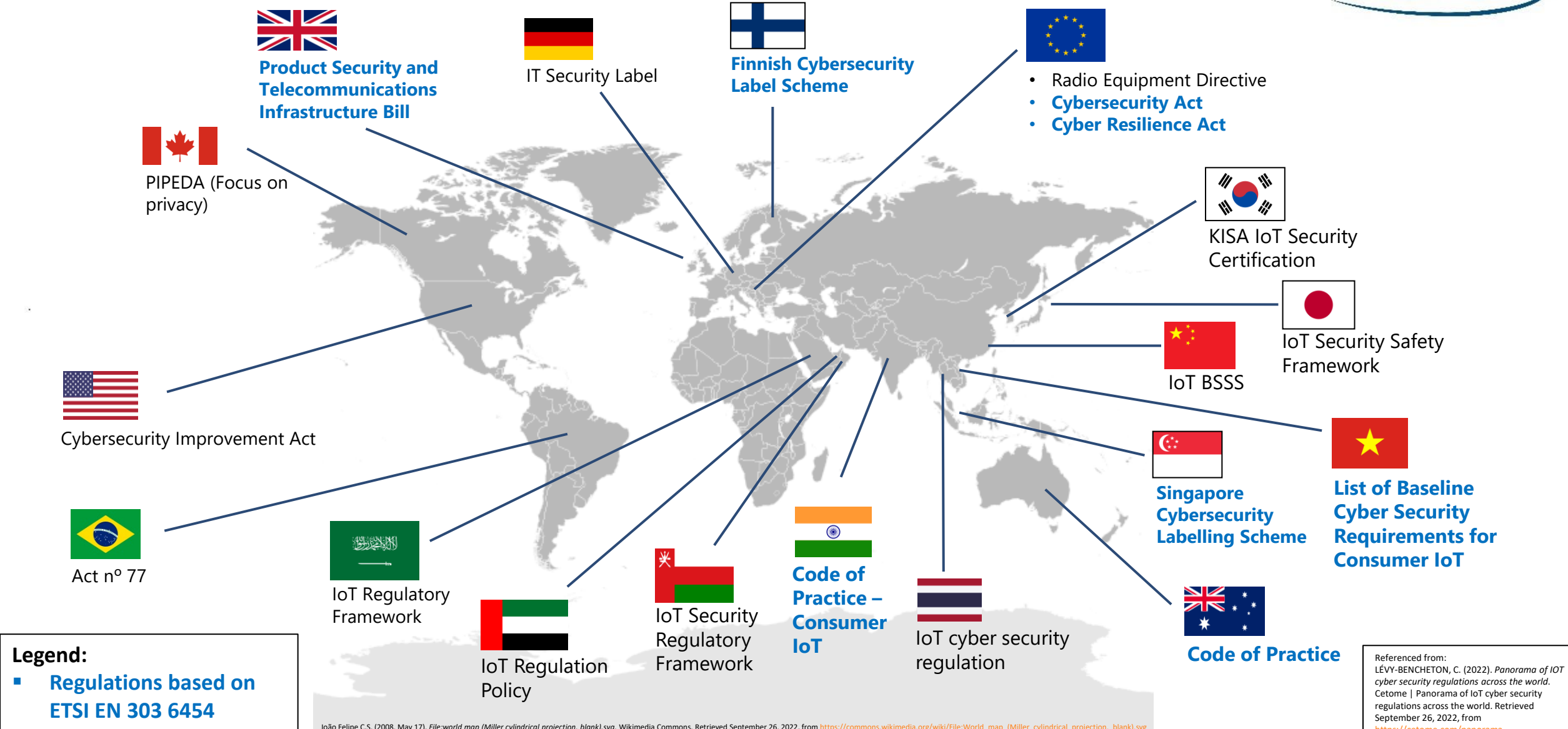


Asus AX82U



Asus TUF AX5400

IoT Cyber Security Regulations across the World



João Felipe C.S. (2008, May 17). File:world map (Miller cylindrical projection, blank).svg. Wikimedia Commons. Retrieved September 26, 2022, from [https://commons.wikimedia.org/wiki/File:World_map_\(Miller_cylindrical_projection,_blank\).svg](https://commons.wikimedia.org/wiki/File:World_map_(Miller_cylindrical_projection,_blank).svg)

Referenced from:
 LÉVY-BENCHETON, C. (2022). *Panorama of IoT cyber security regulations across the world*. Cetome | Panorama of IoT cyber security regulations across the world. Retrieved September 26, 2022, from <https://cetome.com/panorama>

Feedback on Industry's Woes



Fragmentation of standards:

Multiple standards/schemes are in existence and being developed today. This poses a significant challenge in mutual recognition.



Duplicated testing and increased compliance:

Impacts manufacturers' competitive advantage from the time-to-market aspect and adds an additional barrier to market access.



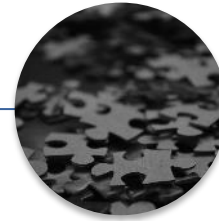
Increased cost of compliance, hampering market access

Compliance to the increasing number of schemes drives up cost. This poses challenge to market access, and growth of digital economy

Universal Cybersecurity Labelling Framework (UCLF) for consumer IoT



Facilitates **mutual recognition** of labelling schemes IoT (regardless of whether they are binary or multi-level)



Harmonising standards, avoid fragmentation

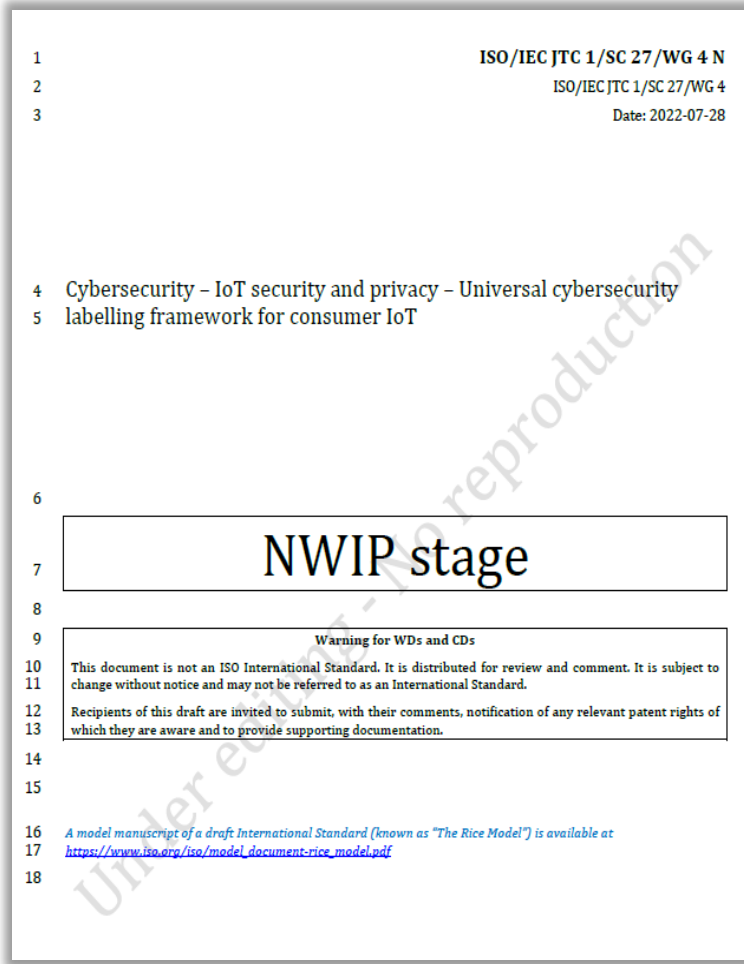


Improves market access by eradicating duplicated testing across countries



Facilitate market access by reducing of compliance.

Global participation needed for development of ISO 27404



New Work Item Proposal (NWIP)

- SC 27 ballot on NWIP (Form 4) and initial standards draft
- 12-week voting on the proposed work item, scheduled to end on 15 Nov 2022
- Experts' participation in standards development needed

SICW 2022 – 18-20th October



“Singapore International Cyber Week is **Asia-Pacific’s most established** cybersecurity event for **global policy makers, thought leaders and industry experts.**”

A promotional banner for Singapore International Cyber Week. The background is light blue with a network of white lines and nodes. The text is centered and reads: 'Singapore International Cyber Week' in a large, dark blue font, followed by '18-20 October 2022' in a smaller, dark blue font. Below this, there are four logos arranged horizontally, each with a label above it: 'HELD IN' with the Singapore logo (SG in a red circle and 'singapore Passion Made Possible' in red and black); 'ORGANISED BY' with the CSA SINGAPORE logo (CSA in red and blue, SINGAPORE in blue); 'EVENT PARTNER' with the 'image engine' logo (image in purple, engine in blue); and 'OFFICIAL CAR' with the Lexus logo (Lexus symbol in silver and 'LEXUS EXPERIENCE AMAZING' in black).

International IoT Security Roundtable (IIOTSRT)



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

NEW - Tech Panel for medical devices this year with leading global experts

Singapore International Cyber Week 2022



We look forward to see you in SICW 2022!

Thank You!