Title: Cyber Trust Mark™
IoT Security Trust Mark™ Certification & Labelling Scheme
Consultation Submission *(on Measure 1)*
to the Department of Home Affairs,
Australian Cyber Security Strategy: Legislative Reforms Paper
Ref: https://www.iotsecuritytrustmark.org/
Class: **SEC=CONFIDENCE: COMMERCIAL**

To Whom It May Concern:

Thank you for the invitation, and opportunity, to submit a paper in response to the consultation of the Australian Cyber Security Strategy Legislative Reforms.

We seek to provide input and views, in our domain of expertise on *Measure 1 – Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices.*

There is no doubt that the issue outlined under Measure 1 of the paper is very real and presents a range of issues for IoT Device/'smart device' consumers, whether they are individuals or organisations.

To that end in this document we have specifically answered the questions raised in the consultation paper.

As the paper observes, voluntary approaches, enabling industry to "self-regulate" only go so far, with product manufacturers often overlooking guidelines and recommendations, taking the approach that they will only act when regulation is raised.

Lessons can be learned by observing previous experience of international peers in their jurisdictions.

Standards

In May 2022 the World Economic Forum published a joint statement[1] calling for a consensus on a consumer IoT security baseline, with over 100 signatories. The Australian Government should take note of this call for a global consensus and not seek to invest in the creation of new Australian standards, or cyber security labels, that are only relevant and applicable domestically, particularly as there are pre-existing standards and labelling schemes that may be adopted. Not only is the duplication of such endeavours expensive financially, but they are also time consuming.

For example, the resulting Product Security and Telecommunications Infrastructure (PSTI) legislation in the United Kingdom commenced with a Code of Practice in 2018, followed process[2] through 2021/2022 and only starts to come into enforcement effect 29th April 2024. PSTI being *"A Bill to make provision about the security of internet-connectable products and products capable of connecting to such products; to make provision about electronic communications infrastructure; and for connected purposes."*

As the consultation paper (page 10) states *"Adopting the ETSI EN 303 645 standard would bring Australia in line with our international partners, noting recent developments in smart device standards across other jurisdictions."* Cyber Trust Mark™ endorses this statement, in fact the IoT Security Trust Mark™ scheme' Baseline Requirements (BR) are the ETSI EN 303 645 standard (Cyber security for consumer Internet of Things: Baseline Requirements).

Further, from an Australian context, this point has been completed, with a new Australian Standard (AS) being published[3] last year (2023), which identically adopts the ETSI standard (AS ETSI EN 303 645:2023).

Should the Australian Government however choose to set a different standard over time, the IoT Security Trust Mark™ has been designed to enable the schemes Baseline Requirements to adapt and harmonise with any regional/domestic variations in standards conformance, providing they don't pose a conflict with other jurisdictions pre-existing cyber security standards and baseline requirements.

Labelling

While the Government notes that a voluntary labelling scheme for consumer-grade IoT devices is not in scope of the issues being considered by this Consultation Paper, it does recognise the requirement for a label to be interoperable with the standard. Cyber Trust Mark™ looks forward to contributing to that consultation also.

When it comes to this stated interoperability of standards derived conformity assessment, and the cyber security labelling of consumer-grade IoT products to baseline requirements there are a number of risks and challenges to bear in mind to ensure consumers, and the market, are not misled.

One cannot technically separate a standard (such as ETSI EN 303 645 or AS ETSI EN 303 645:2023) from conformity assessment, whether voluntary or mandated – the two must be considered hand-in-hand. ETSI have documented a full conformity assessment to the EN 303 645 standard, which runs to some 130+ pages.

There is a vast difference between assurance and conformance. Assessment, certification and labelling needs to be clear, dynamic *("live")* and not static or binary. Labels, particularly Government issued, could convey a false sense of security assurance. Constant surveillance of the product hardware and software bill of materials is required, along with clear steps to suspend or revoke certification at any time, thereby ensuring the label remains in good standing. These are some of the key pillars of Intellectual Property developed in the IoT Security Trust Mark™ scheme.

Consumers ultimately need to benefit from the safety and privacy that security delivers, product manufacturers require a low-impost, low-cost scheme which is delivered in a timely manner.

Our organisation has invested significant resources over a number of years in stakeholder consultation, design, development, and protection, of unique IP that satisfactorily addresses a number of key issues raised by stakeholders around the globe, from consumers, industry, governments and academia to product manufacturers. We would welcome further engagement with government, industry and consumer stakeholders in Australia.

The result of the effort is the IoT Security Trust Mark™ Certification & Labelling Scheme (STM), collectively known as Cyber Trust Mark™.

A robust, federated scheme, that is voluntary, global, scalable and harmonised with existing standards and labelling schemes internationally. To this effect, in 2021 a paper was delivered by Cyber Trust Mark™ and published by the US National Institute of Standards and Technology (NIST) *refer Attachment B.*

Federated in that it is open, transparent and involves several key parties in each territory that the scheme operates to ensure scalability, rigor, independence and longevity.

Scalable and harmonised therefore ensuring inclusion in smaller markets, such as Australia, to provide the same uniform security, safety and privacy protections to consumers as those enjoyed internationally.

For example, the scheme by design may be represented in domestic markets by an appointed local "Host Country Association" being an industry-led and/or consumer representative body or group. This encourages "in-market" industry participation and consumer involvement, thereby ensuring inclusivity and acceptance. There is a separate technical "Decision Authority" that oversees the technical aspects of the scheme. Likewise there is an open market of "Accredited Test Facilities", providing product manufacturers with a panel to access, engage and receive market competitive value for their conformity assessment requirements. In each country there is an opportunity to establish a scheme advisory body, providing further transparency and enabling clear channels and a method of feedback to continue scheme development, currency and assuring international harmonisation. The scheme is independent and entirely self-funding, ensuring it can endure.

While protected in a number of international jurisdictions, including the European Union, United Kingdom and United States, in relation to the Australian market specifically the Certification Trade Mark is registered here also and the Cybersecurity Labelling Scheme (CLS) has passed formal assessment and approval by the Australian Consumer & Competition Commission (ACCC) *(refer Attachment A).*

It is the only Mark that can issue cyber security labelling for consumer Internet of Things products internationally.

Despite having an international remit, the foundation of the scheme was proudly developed in Australia, by Australians and is currently headquartered here. The scheme employs a number of resources in this country, and its success contributes to the national economy, international recognition ensures export revenues.

[1] https://iotsecuritytrustmark.org/wp-content/uploads/2022/02/consumer-device-security-joint-statement_FINAL-2152022_PDF.pdf

[2] https://bills.parliament.uk/bills/3069/stages

[3] https://store.standards.org.au/product/as-etsi-en-303-645-2023

Questions raised in the consultation paper *(Pg 12)*

Cyber Trust Mark™ provides the following views to the Department in response to the queries raised on the design and implementation of a mandatory cyber security standard for IoT and smart devices.

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

Cyber Trust Mark™, for consistency and harmonisation would recommend the Australian Government look to international jurisdictions and consider adoption of their terminology, in particular the European Union and their Cyber Resilience Act (CRA), who, on this subject, clearly and succinctly stated from the outset (2022) the scope was *"mandatory cybersecurity requirements for products with digital elements, throughout their whole lifecycle."*[4]

This is expanded as "*A "product with digital elements" is defined as "any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately." The cybersecurity requirements would apply to all products that are either directly or indirectly connected to another device or network, including non-embedded software.*"[5]

The IoT Security Trust Mark™ Certification and Labelling Scheme employs this European Union definition to ensure clarity, many stakeholders, particularly manufacturers have been observed trying to obfuscate the reality of their product scope by hiding behind a range of terminology, such as smart-devices, connected-devices etc. Simply, if the product has digital elements then the manufacturer should support their cyber security conformance for the product' intended lifecycle.

2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?

The three principles of the AS/ETSI standard are an appropriate start for a minimum baseline for legislation and enforcement for consumer-grade IoT devices sold in Australia.

It should be noted however that the United Kingdom based their legislation on these three principles with some modification, that Australia may want to consider when legislating.

The three requirements developed by the UK are:

- No default passwords *(excluding EN 303 645 5.1-3 ~ 5.1-5)*

- Having a means to manage vulnerability reports *(excluding EN 303 645 5.2-2 & 5.2-3)*
- Transparency on how long the product will receive security updates *(excluding EN 303 645 5.3-1 & 5.3-2)*

3. What alternative standards, if any, should the Government consider?

   While not necessarily an alternative standard, Cyber Trust Mark™ would suggest the Australian Government considers referencing the recent Australian Standard that identically adopts the ETSI standard. This is designated as AS ETSI EN 303 645:2023 and is available for purchase from Standards Australia, it is noted however that ETSI offer their standard at no cost, therefore some stakeholders may consider Standards Australia's paywall to obtain this AS a barrier to market.

4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?

   Refer above to query 1 response. Furthermore, exceptions can lead at best to misunderstanding and at worse to loop holes being exploited, particularly for certain multinational manufacturers. Cyber Trust Mark™ would still suggest the Australian Government consider adopting the definition established by the European Union in their Cyber Resilience Act (CRA) they are clear and concise and not open to interpretation "*It will apply to all products connected directly or indirectly to another device or network except for specified exclusions such as open-source software or services that are already covered by existing rules, which is the case for medical devices, aviation and cars.*"[6]

5. What types of smart devices should not be covered by a mandatory cyber security standard?

   Cyber Trust Mark™ would suggest that devices covered by existing legislation not be covered (unless their legislation has lower cyber security requirements) for example, in the EU as above – "*medical devices, aviation and cars.*"

6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?

   Again take from our international colleagues experience, particularly the UK and DCMS with the PSTI bill[7], they published their guideline for industry in 2018, putting industry on notice to demonstrate self-regulation, they then prepared the bill and lodged it, November 2021, it finally reached Royal Assent December 2022, and it included a period for conformity until enforcement commences (which is April 29th this year, 2024) – so 16-months after the legislation passes.

7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for smart devices?

   No comment on the RPA framework, aside from the cost to monitor, police and enforce conformance to the standard for products and manufacturers will need to be well considered.

[4] https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products

[5] https://www.loc.gov/item/global-legal-monitor/2022-12-01/european-union-commission-proposes-new-cybersecurity-rules-for-products-with-digital-elements/#:~:text=A%20“product%20with%20digital%20elements,directly%20or%20indirectly%20connected%20to

[6] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[7] https://bills.parliament.uk/bills/3069/stages

Attachment A –
Australian Competition & Consumer Commission Final Assessment

AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Final Assessment of Certification Trade Mark Application No. 2203085 lodged by Security Mark Pty Ltd

The Australian Competition and Consumer Commission (the ACCC), in accordance with the requirements of the *Trade Marks Act 1995*, has completed its Final Assessment of the above Certification Trade Mark (CTM) application.

The ACCC's Final Assessment is that it is satisfied that:

(a) the approved certifiers demonstrate the attributes necessary to competently certify the goods and/or services in respect of which the CTM is to be registered;

(b) the rules governing the use of the CTM would not be to the detriment of the public; and

(c) the rules governing the use of the CTM are satisfactory having regard to the principles relating to restrictive trade practices set out in Part IV of the *Competition and Consumer Act 2010* (the Act) and the principles relating to unconscionable conduct (Part 2-2), unfair practices (Part 3-1), and safety of consumer goods and product related services (Part 3-3) in Schedule 2 (Australian Consumer Law) of the Act.

Signed..... **(Deputy Chair)**

Date..... 8 December 2022

Attachment B –
United States National Institute of Standards and Technology paper

Published September 2021:
https://www.nist.gov/system/files/documents/2021/09/03/IoT%20Security%20Mark_NIST%20IoT%20Certification%20call%20for%20papers%20v0.1-2.pdf

This paper describes relevant details of the Internet of Things (IoT) Security Trust Mark™ Certification Scheme *(STM or Scheme)* and how it addresses the common problems. We noticed your recent request calling for papers[1] and would like to draw your attention to the program of works that we have undertaken in developing and launching the IoT STM, currently in Pilot. The formation work was initially commenced in 2006 with the design for certification of products' electronic security for use in Information Assurance (IA) programs, renewed and directed towards IoT in 2017, formalised in 2019.

The Scheme has been developed to be global, scalable *(federated principles)*; technology and standards agnostic. It is rigorous and independent and offers good value *(self-funding*); without compromise. It complies with accepted conformance assessment "norms" *(such as NIST.SP.2000-01/02)*. STM is designed to support both product manufacturers/vendors as well as consumers, at all levels. We encourage vendors to innovate and incorporate good security, safety, and privacy by design principles in their development and manufacturing processes. We acknowledge without good, inherent, security in smart devices they cannot underpin consumer/user safety and/or their information privacy.

Traditional ICT cybersecurity practices have never worked effectively. Requiring consumers/users to implement reactive security controls, policies and procedures is not the answer. That issue will be amplified exponentially when it comes to IoT 'smart' devices. The paradigm needs to shift. Consumers should seek vendors' products that inherently offer them higher levels of security, and therefore safety and privacy. Vendors in turn should identify that the greater levels of safety and privacy assurance they can demonstrate to their market, by embedding good security-by-design principles, the more trusted they are. IoT Security needs to become a unique selling point delivered that informed consumers seek.

Unfortunately to-date regulation, compliance, and certification in general, *(security or otherwise)*, is seen as a cost centre and burdensome by vendors typically to be avoided if possible. The STM addresses the concerns held by many that costs and time to comply outweigh the benefits. Indeed, the Scheme needs to address this as it is self-funding and relies on offering practical value and timeliness as a measure of operating success. A good example of this timeliness is that a pass/failure is delivered

within 8~12 days on average and is capped by the Scheme at no more than 30-days. Supporting vendors who are striving to deliver the right thing with their IoT device security, by independently validating their security claims and ensuring they meet IoT Security Baseline Requirements (BR).

Not all certifications are equal, it is one thing to build a certification program that measures something against a predefined standard, say telecommunications emissions or electrical safety for example. However cyber security is an ever-moving target. It would be virtually impossible to define a "one-size-fits-all" standard that is applicable to the diverse nature of products that may at any point in time be connected to the Internet globally. STM successfully addresses this diversity by being a security certification and labelling framework that incorporates flexibility to adopt and incorporate the criteria of IoT Security Baseline Requirements (BR) used for STM evaluation from several diverse sources as they evolve, such as global standards bodies; *(i.e. ETSI, ENISA, NIST),* and Codes and Guidelines (or legislative requirements) produced by Governments, or their Departments and Agencies. The STM also combines evaluation and assurance to Baseline Requirements, but also verifies vendors security claims.

Internet of Things security is not just the issue of one country or jurisdiction, international experience demonstrates this. Supporting this, in late 2019, Ministers from the United States, United Kingdom, Canada, Australia and New Zealand, the Five Eyes (FVEY) countries, agreed and signed a Statement of Intent regarding the security of the Internet of Things[2]. They recognise the problem and consequences, and publicly acknowledge that the solution to good IoT security is not something that any single country alone can solve. Further that they require the industry itself to step up to avoid making the same mistakes made with ICT cyber security. The STM Scheme covers this, being designed to be a global program, and most importantly scalable, it employs a federated governance model, appointing a number of stakeholders in key positions of responsibility, while maintaining consistency, transparency and independence.

Other programs may rely on vendor self-attestation of security, while this may provide some level of assurance to consumers, vendors stating their security claims, it is no guarantee of security. Often written to requirements that are open to interpretation by the organisation applying the claim of compliance, or even the individuals' level of expertise in the matter. Indeed, in the past other industries have seen consortia of vendors organised to influence standards or "self-certify" ultimately to the detriment of the consumer, who their technologies are inherently supposed to serve. The STM operates with Accredited Test Facilities (ATFs), who are independent, ISO 17025 accredited testing laboratories, their approved Test Officers work with vendors to create Vendor Claims Documents (VCDs) which are in-turn approved by a third-party Decision Authority (DA) prior to any STM evaluation commencing. Ensuring transparency and independence while maintaining value and timeliness.

A remark often levelled at security compliance programs is that it is only as good as the day of audit/test. And while this is indeed true, the IoT Security Trust Mark™ Scheme incorporates significant levels of ongoing surveillance by a technical Decision Authority, ensuring that any known vulnerabilities and exposures are reported to certified product vendors and the product certification is suspended until that vulnerability is addressed.

The Security Trust Mark™ Evaluated Products List (STM-EPL) lists each product that has been evaluated and includes a Test Report Summary (TRS) from their STM ATF. The STM EPL is fully searchable by consumers/users researching products, and it also incorporates the STM 'traffic light system' which enables consumers to easily visually identify the currency of certification according to the colour displayed next to the evaluated product. Green for currently certified, Amber for suspended, and Red for expired. That leads on neatly to the final point, labelling.

The IoT Security Trust Mark™ Certification itself is one thing, however the labelling of certified products is another. The market provided feedback that labelling in some instances may be beneficial, but not all. And as such the STM offers a voluntary label (STM QR code), at no further cost, which vendors may apply to their certified products should they choose. This unique code for each certified product links directly to the STM Evaluated Product List. Thus, ensuring high levels of usability for IoT consumers.

Ultimately IoT consumers must be empowered to make informed decisions when it comes to buying smart devices with inherent security, underpinning their safety and privacy.

The IoT Security Trust Mark™ Certification and voluntary labelling scheme is currently in open Pilot, and seeking expressions of interest from various stakeholders, including Vendors seeking Pilot participation, and prospective; Affiliates, Host Country Associations (HCAs), Decision Authorities (DAs) and Accredited Test Facilities (ATFs).

All enquiries can be made via the organization's website:
https://www.iotsecuritytrustmark.org/

For further information of relative STM stakeholders there are a series of documents that set out in detail various requirements under the IoT Security Trust Mark™ Scheme:

Description of Scheme (DOS) v1.6, 503KB, 24-pages, PDF (ISBN 978-0-9953944-2-1)
Vendor Guideline (VG) v1.5, 759KB, 27-pages, PDF (ISBN 978-0-9953944-9-0)
Accredited Test Facility Guideline (ATFG) v1.6, 926KB, 37-pages, PDF (ISBN 978-0-9953944-8-3)
Decision Authority Guideline (DAG) v1.3, 791KB, 25-pages, PDF (ISBN 978-0-9953944-7-6)

These are available upon execution of the STM Mutual Non-Disclosure Agreement (MNDA)

[1]https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/workshop-and-call-papers-cybersecurity-labeling

[2]https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things

www.iotsecuritytrustmark.org