Atlantic Council

Security in the Billions

Toward a Multinational Strategy to Better Secure the IoT Ecosystem

Patrick Mitchell, Liv Rowley, and Justin Sherman
with Nima Agah, Gabrielle Young, and Tianjiu Zuo

Implementation for Singapore

The purpose of this is to demonstrate how Singapore should act to help develop a multinational strategy to better secure the IoT ecosystem.

Tier 1. Set the Baseline of Minimally Acceptable Security:

While Singapore's CLS for consumer IoT is largely voluntary, it provides the regulatory infrastructure for a program that gradually expands to establish a baseline level of security for all devices. Internet routers sold in its market already must meet the provisions of the CLS Tier 1 label, which map directly to the UK's "top three" requirements that will be enforced with its proposed PSTI Bill. In consultation with IMDA and other partners, the CSA should:

- **Make the Tier 1 label mandatory for more product categories**. Internet routers have been a wise starting point: they have an outsize presence in today's botnets and can have security knock-on effects that threaten consumers' other smart home devices. Perhaps unsurprisingly, routers now account for over half of the CLS labels issued.[1] The CSA should consider the next highest priority product categories that will need to meet these minimum security measures, incorporating criteria like the (lack of) maturity in the category's cybersecurity features and the privacy risk to individuals if compromised. IP cameras, connected baby toys, and smart locks are strong candidates.
- **Add to the security provisions required as part of the Tier 1 label, especially those related to secure development practices**. CLS includes 76 security provisions, with roughly half required by one or more of its tiers, while the others are merely recommended. The first tier currently has 13 required provisions. Tier 2, which primarily concerns product lifecycle and secure development practices, has 17 required provisions—eight drawn from ETSI EN 303 645 and nine from the IMDA's IoT Cyber Security Guide. Over time, the CSA should aim to collapse the most impactful Level 2 requirements into Level 1, while removing those not seen as value-added. Alternatively, the CSA could keep the same provisions in each CLS level and gradually require that devices meet the second level. Since both CLS Levels 1 and 2 rely on manufacturer self-attestation, these changes should not require any operational changes in administering the program.

Tier 2. Incentivize Above the Baseline:

CLS has seen dramatic growth since the beginning of 2022, with the number of labels issued tripling during that timeframe. But the gains are not evenly distributed: of the 176 labels issued by CSA as of July 2022, 148 are at the Level 1 designation, an additional 16 are at Level 2, and 10

[1] CSA, Cybersecurity Labelling Scheme (CLS) Product List.

are for Level 4.[2] As mentioned earlier, many of the recipients of labels are internet routers, where the Level 1 label is mandatory. A key selling point of its multi-tier system is the ability to provide manufacturers with a reason to go above and beyond the bare minimum. To this end, CSA should:

- **Conduct a review of the program's effectiveness in addressing the core problems associated with IoT insecurity and publish the findings**. As the country with the most mature cybersecurity labeling program, Singapore is in a unique position to gather information on the successes and challenges of this regulatory approach. How have consumers adapted their purchasing behavior since its launch? Has the number of insecure devices sold in Singapore decreased? What have been the challenges for firms? Have there been impacts beyond Singapore's borders? This review could also help improve the structure of the program. For example, it might review the fitness of the CLS tier structure. The inclusion of more levels makes sense if it adds to the range of choice for consumers and manufacturers to select the appropriate certification level that meets their needs. If no one selects it—currently the case for CLS Level 3—it is possible to simplify the scheme. The report's "Measuring Success" section includes some example metrics that could help gauge a topic that is notoriously difficult to quantify. The results will be helpful for Singapore, but just as critically, for the large number of countries and industry bodies that are experimenting with cybersecurity labels for IoT products.
- **Pursue an agreement with Germany for mutual recognition of cybersecurity labels**. Finland and Singapore's agreement shows that binary and multi-tier labeling approaches need not conflict. Germany, which recently launched its own binary label in January 2022, should also join the bilateral agreement between Singapore and Finland for mutual recognition. All three countries draw largely from the same list of ETSI EN 303 645 security provisions. Partnering with a market of Germany's size will add significant momentum for Singapore's approach to securing IoT, while reducing the burden of duplicate testing and certification for firms. This approach should be pursued for any country that adopts an IoT labeling program found to be largely compatible with the existing Singaporean program.
- **Consider measures to encourage broader adoption of the labeling scheme**. Anecdotal evidence suggests that many security-minded firms have been eager to participate in the program, but the CSA should continue to search for ways to increase its attractiveness. While the program will eventually need to generate revenue to cover its costs, CSA could extend the moratorium on application fees for an extended period, or even subsidize testing for devices at higher levels of security.

[2] CSA, Cybersecurity Labelling Scheme (CLS) Product List.