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 Australia

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

Tier 1. Set the Baseline of Minimally Acceptable Security:

Since the conclusion of its Call for Views in August 2021, Australia's DHA has been relatively quiet in public on its path forward for the regulation of consumer IoT. Whatever its ultimate action, it is evident that Australia aims to take a more hands-on approach than its past measures. To establish a minimum baseline, the DHA should:

- **Select a regulatory approach for mandating basic security requirements for devices sold in its market**. Australia has multiple approaches at its disposal and should continue to study the benefits and drawbacks of programs in the UK, Singapore, and elsewhere. The options it is most seriously considering are either a mirror image of the UK's minimum security standards or a four-level "graded shield" that appears very similar to Singapore's CLS. Australia's voluntary Code of Practice, which aligns with ETSI EN 303 645, should provide a strong foundation that will have prepared Australian businesses for more stringent enforcement.
- **If pursuing a minimum security standard, align its approach with the PSTI Bill's planned enforcement measures**. At a minimum, these measures should include the "top three," banning universal default passwords, mandating vulnerability reporting contacts, and transparency on security updates. Preferably, it would also include additional provisions on securing personal data, encrypted communications, and minimum acceptable support periods for security updates. Currently, Australian Consumer Law does not require firms to adhere to any principles meant to reduce cyber risk, "only that they cannot make misleading or deceptive representations about the cyber security of their products."[1] This baseline could be achieved either through a new law, modeled on the UK's PSTI Bill, or an expansion of Australia's existing Consumer Law to incorporate protections against the most basic flaws in cybersecurity in its definition of "acceptable quality" and "fit for purpose."[2]
- **If pursuing a multi-level labeling approach, follow a strategy of gradual mandates by product category.** Given that it seems most drawn to a multi-tier label mirroring CLS, the clearest path for Australia is to follow Singapore's strategy and gradually mandate a tier 1 label by product type, beginning with high-priority items like internet routers. The labeling

[1] DHA, "Strengthening Australia's Cyber Security Regulations and Incentives."
[2] DHA, "Strengthening Australia's Cyber Security Regulations and Incentives."

scheme should include a broad definition of in-scope products, drawing from ETSI's definition of smart devices. In addition to expanding mandates by product category, DHA can also raise the baseline over time by advancing along the other "axis" of incorporating more security provisions from higher security levels into its base tier.

Tier 2. Incentivize Above the Baseline:

The approach for incentivizing action to instill even greater security measures in its smart device market is highly related to Australia's method for enforcing its baseline. As DHA notes, these measures need not be mutually exclusive. To promote a higher tier of security, Australia should:

- **Select a cybersecurity labeling approach**. A study conducted by the Behavioral Economics Team of the Australian Government compared the effects of multiple label options on consumers, finding that "participants were more likely to choose a device with a cyber security label than one without a label, by 13–19 percentage points."[132] While the graded shield was most impactful, it found that "expiry labels were still effective" and "a high security level or long expiry date increased the likelihood of choosing a device."[133] Each of these options appears likely to have its own benefits and drawbacks, but it is time to choose one and move forward with it.
- **If pursuing an expiry date-label, study its effect and publish the findings**. If it follows through on this proposal, Australia would be the first to introduce a label that indicates the length of time manufacturers will provide security updates to the product. Studying this approach can help answer several questions about the impact of cybersecurity labels, particularly around the sunsetting phase. For example, are consumers incentivized to purchase devices at a discount that are about to go "off warranty"? As stated earlier, there is nothing wrong with national-level experimentation, as it can be beneficial in formulating new approaches that may be suitable for broader adoption.
- **If pursuing a "graded shield" label, agree to mutual recognition with Singapore and other participating countries**. The four-level labeling scheme that Australia appears likely to pursue bears many similarities with Singapore's CLS. In this case, the two countries should aim to bring their programs into close harmony, including the definitions of in-scope devices, the security provisions included in each tier, and the processes for self-attestation and third-party testing. Over time, the DHA should work with the CSA to ensure that the programs evolve together with consistency. Australia should then join the bilateral agreement with Finland for mutual label recognition, as well as a proposed agreement with Germany.