FACTSHEET

Security standards for smart devices

Part 2 of the *Cyber Security Act 2024* establishes the power for the Minister for Cyber Security to prescribe rules that will establish mandatory security standards for smart devices, also known as Internet of Things (IoT) devices.

Responsible entities and obligations

The Act places responsibility on manufacturers and suppliers of smart devices to ensure that those devices meet requirements in the specified security standard relevant to that product if there is intent for that device to be made available in Australia.

Manufacturers and suppliers of smart devices covered by the scope of the rules will be required to produce a statement of compliance confirming their claims that the device meets the requirements under the relevant standard. At a minimum, details of a statement of compliance should include:

- product type and batch identifier;
- name and address of each manufacturer of the product, an authorised representative of the manufacturer and, where applicable, each authorised representative that are in Australia;
- a declaration that the statement of compliance is prepared by or on behalf of the manufacturer of the product;
- a declaration that, in the opinion of the manufacturer, the product has been manufactured in compliance with the requirements of the security standard, and they have complied with any other obligations relating to the product as set out in the security standard;
- the defined support period for the product at the date the statement of compliance is issued;
- signature, name and function of the signatory; and
- the place and date of issue of the statement of compliance.
- If responsible entities that are not the manufacturer of the device intend to supply a device in Australia, they can request the relevant information from the device manufacturer.

Enforcement and regulation

The enforcement framework established in the Act includes enforcement notices and product testing capabilities, designed to encourage engagement with manufacturers and suppliers of smart devices and uplift industry best practice.

The powers established under the Act would provide the Secretary of Home Affairs the ability to issue enforcement notices to responsible entities if the entity is not complying with their obligations under the Act. The Secretary would be required to give notice of the intent to issue an enforcement notice, providing the responsible entity with an opportunity to respond prior to an enforcement notice being issued. These enforcement notices are:

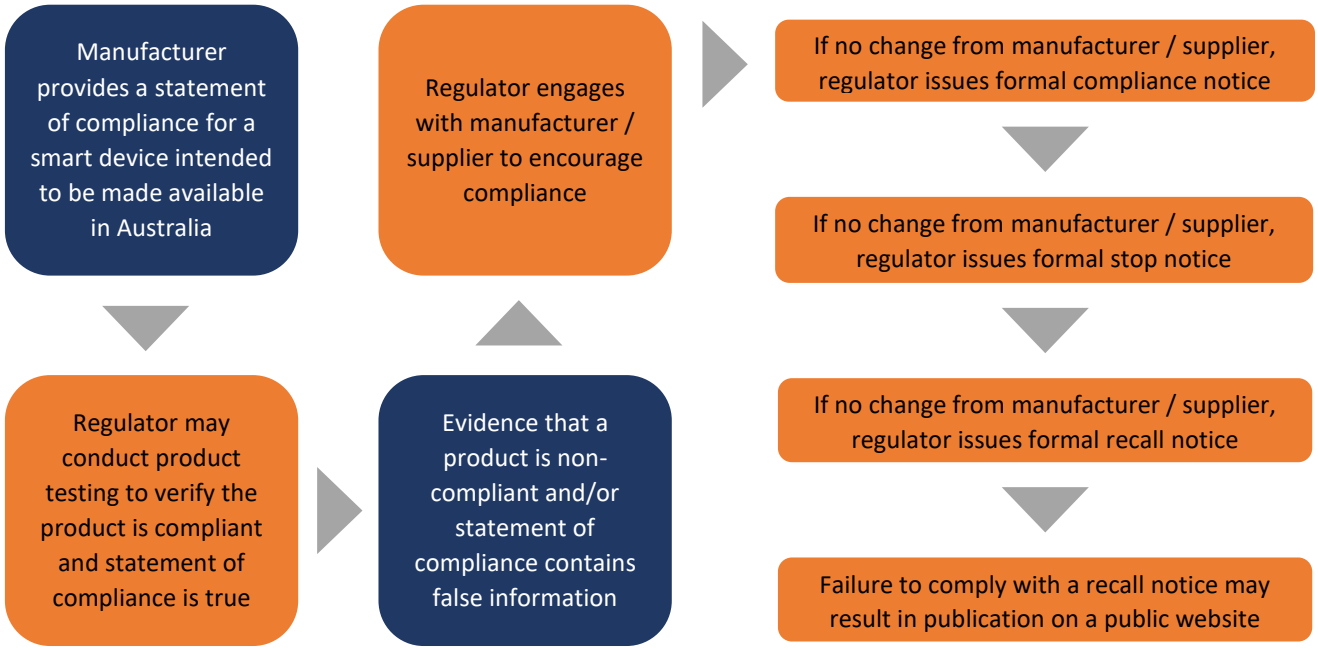
- Compliance notices, where a receiving entity would be required to take specified steps or actions to address an identified issue of non-compliance.
- Stop notices, where a receiving entity would be required to stop or refrain from doing a particular action or take a particular action.

- Recall notices, where a receiving entity would be required to take specified steps to arrange for the return of the product to the entity or the manufacturer of the product and (to the extent within the entity's control) ensure the product is not acquired in Australia and (to the extent within the entity's control) ensure that the product is not supplied to suppliers for supply in Australia.

Failure to comply with a recall notice may result in public notification. Information that could be published includes the identity of the non-compliant entity, details of the product and non-compliance, and risks posed by the product relating to the non-compliance.

An internal review of a decision to give a notice can result in the Secretary revoking or varying an enforcement notice given to an entity. This internal review is to ensure the Secretary followed due process in issuing an enforcement notice per the Act.

This flow chart illustrates how the regulatory and enforcement framework will function:



Consumer-grade smart device standard

The first standard intended to be introduced under Ministerial rules will uplift the cyber security of **consumer-grade** smart devices (with some device exceptions) by aligning with existing international approaches.

This standard will closely follow the *Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023* (UK) made under the *Product Safety and Telecommunications Act 2022* (UK), based on the first three principles of the ETSI EN 303 645 standard.

The standard is anticipated to include:

- **No universal default passwords** – where passwords are used in any other state other than factory default, all consumer smart device passwords need to be unique per device or defined by the user.
- **Implement a means to manage reports of vulnerabilities** – allowing security researchers and others to report issues, with status updates on the resolution of these issues.
- **Provide information about how long the device will be supported for** – manufacturers and suppliers must provide transparency to consumers about the minimum timeframe that the product will receive security updates.

In addition to being ***relevant connectable products*** (as defined in the Act), it is anticipated that the standard will apply to certain smart devices that could be reasonably be expected to be acquired by a ***consumer***, defined by section 3 of Australian Consumer Law.

The consumer-grade smart device standard is expected to cover smart devices that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources.

Similar to all rules intended to be introduced under this Act, a draft of the standard, which will be contained within draft Rules, will be released for a 28 day public consultation period. This standard will also have a 12 month transition period following the Rules coming into force.

A communications program will commence to provide additional clarity to manufacturers and suppliers about their new obligations, and educate consumers so they understand how the standard will affect them.

Excluded devices from the standard

The proposed format of the first rule will be an exclusion-based approach for the coverage of devices. Generally, devices will be excluded if:

- there is existing legislation that can adequately address the cyber security risks posed for these devices;
- there is work underway across Government to develop a higher or bespoke standard for these devices; or
- The complexity of these devices means that being mandated under these rules will risk a lower standard being met.