



FREQUENTLY ASKED QUESTIONS

Security standards for smart devices

These frequently asked questions (FAQs) provide general guidance only on the security standards mandated by the Cyber Security (Security Standards for Smart Devices) Rules 2025 (the Rules), authorised by the Cyber Security Act 2024 (the Act). The FAQs should be considered in conjunction with the text of this legislation.

The FAQs are not intended as legal advice. We suggest seeking professional or legal counsel to confirm your responsibilities under Australian law – including questions about specific products.

This version was published on 4 March 2026 and supersedes the version published on 10 December 2025.

Scope of the consumer grade smart device standards

1. What types of smart devices are within scope of the security standards?

The security standards for consumer grade smart devices apply to smart devices that meet the definition of a **relevant connectable product** (as defined in the Act) that will, or could be reasonably expected to, be acquired in Australia by a **consumer**, as defined in section 3 of the Australian Consumer Law. These are products that are intended by the manufacturer to be used – or would likely be used – for personal, domestic or household use or consumption.

Some consumer grade smart devices, such as smartphones and laptops, are exempt from the security standards. Please refer to section 8 of the Rules for further information on exemptions.

2. When do the security standards take effect?

The security standards apply to all in-scope products manufactured **on and from 4 March 2026**. Products manufactured before 4 March 2026 are **not required** to comply with the security standards, as the security standards were **not in effect on their date of manufacture**.

The obligation on suppliers to not supply non-compliant products will apply to products required to comply with the security standards (that is, in-scope products manufactured on and from 4 March 2026).

3. Do the standards apply to products intended for business use or business-to-business (B2B) products?

The security standards apply to smart devices that meet the definition of a **relevant connectable product** (as defined in the Act) that will, or could be reasonably expected to, be acquired in Australia by a **consumer** (as defined in section 3 of the Australian Consumer Law). These are products that are intended by the manufacturer to be used – or would likely be used – for personal, domestic or household use or consumption.

Under section 14 of the Act, security standards apply to whole classes of smart devices, not individual cases of acquisition. This means that, **if there is any case where a product could be acquired where the above conditions are met**, then that product must comply with the security standards in all cases.

Smart devices only fall out of scope of the security standards if there is no circumstance where the product meets the definition of a relevant connectable product that will, or could be reasonably expected to, be acquired in Australia by a consumer, and that are intended by the manufacturer to be used – or would likely be used – for personal, domestic or household use or consumption.

4. Are aftermarket vehicle systems within scope of the Rules?

An aftermarket vehicle system that meets the requirements in the security standards (as described above) would likely be within the scope of the security standards.

Aftermarket vehicle systems, such as audio and navigation systems, **are not currently considered road vehicle components** and are not included in the road vehicle component exemption in the Rules.

A product can only be considered as a road vehicle component if it can be tested against one or more of the Australian Design Rules (ADR) under the *Road Vehicle Standards Act 2018*. If there are no ADRs that relate directly to a particular type of product, this means the product is not covered by the road vehicle component exemption in the Rules.

Requirements in relation to passwords

5. Do all in-scope products require passwords?

No, the requirements for passwords only apply to **in-scope products that use a password** for the smart device's hardware or pre-installed software used in any state other than factory default, and where software is required to be installed for the product's intended usage.

For in-scope products with such a password functionality, the password must meet the requirements of the security standards, which include being unique per device or defined by the user. The standards **do not require** in-scope products to have such a **password functionality**.

6. Can the manufacturer use a default password for a device in factory default state?

Yes, but **only** while an in-scope product is **in factory default state**. The manufacturer can use a **default password** for the smart device's hardware or pre-installed software, and where software is required to be installed for the product's intended usage.

In any other state, the use of passwords for the in-scope product must meet the requirements of the security standards.

Requirements relating to reports of security issues

7. What are the requirements for publishing information on how to report security issues?

The manufacturer must publish **accessible, clear and transparent** information on how to report security issues for in-scope products. The information must be available **in English, free of charge, without a person requesting** the information, and **without requesting personal information** about the person making the report. For example, a manufacturer may publish the required information, meeting all requirements, on their website.

8. Can the manufacturer request contact information of the person reporting a security issue?

The manufacturer may request **reasonable contact information**, such as an email address, so they can **acknowledge the receipt of the report** and **provide status updates** to the person who submitted the report, as required by the security standards. Importantly, however, the manufacturer **must not require** that this contact information includes any personal information about the person making the report.

Any collection, use or disclosure of personal information by the manufacturer would still be subject to any applicable privacy laws, such as the *Privacy Act 1988*.

Requirements relating to defined support periods and security updates

9. Can the defined support period be a period of time, such as “in five years”?

The security standards require the defined support period to be a period of time **with an end date**, rather than an end to a period of time. Examples of a fixed end dates are “no earlier than 30 June 2027” or “ending on 30 June 2029”.

10. Can the defined support period be shortened or extended?

The defined support period **cannot be shortened** once it has been published.

Defined support periods **can be extended**. The new defined support period must be published by, or on behalf of, the manufacturer as soon as practicable, in the same manner by which the original period was published.

11. What are the requirements for publishing defined support periods?

The manufacturer must publish the defined support period for the smart device's:

- hardware,
- pre-installed software,
- software that is required to be installed for the product's intended usage, or
- software developed by, or on behalf of, the manufacturer that is used for, or in connection with, the product's intended usage,

where any of these components **can receive security updates**. The defined support period for each of these components must be published to comply with the requirements of the security standards. For example, the defined support period for a product's software and the defined support period for a product's first-party companion app must both be published as required by the security standard.

This information must be published in a manner that is **accessible, clear and transparent**. The information must be available **in English, free of charge, without a person requesting** the information, **without requesting personal information** about the person making the report, and in a way that is **understandable without prior technical knowledge**.

12. What does it mean to publish the defined support period in a way that is understandable without prior technical knowledge?

Publishing the defined support period is intended to **provide consumers with more information** about a product so they can more easily **factor cyber security into their purchasing decisions**.

The manufacturer must publish the defined support period for a product in such a way that it is **easy for a person without technical knowledge to understand** what the defined support period is and what it means, and so they can easily compare the defined support period of different products.

We suggest using **plain English** to convey information related to the defined support period. You may use a statement like the examples below to comply with the requirements of the security standards.

"This device will receive all available security updates until at least 30 June 2028."

"We will provide security updates for this app until 30 June 2026."

Additionally, the discovery of the defined support period **should not rely on a person's knowledge of the existence of the Act or the Rules**. For example, the defined support period should not only be published in the statement of compliance or in a regulatory section of a website.

13. Is the manufacturer required to publish the defined support period on its website?

If the manufacturer **supplies an in-scope product on its website**, or a website under its control, the manufacturer is required to:

- **Prominently publish the defined support period**, or any extension to a defined support period, **with other information** on the website that is **intended to inform consumers' decisions** to acquire the product. This applies to **each instance on the website** where information is published that is intended to inform consumer decisions to acquire the product, and;
- **Publish the defined support period**, or any extension to a defined support period, **alongside or otherwise given equal prominence** to the publication of the **main characteristics** of the in-scope product. This applies to **each instance on the website** where the main characteristics of the product are published.

For example, a manufacturer may have a comparison page listing out the main characteristics of multiple products, a dedicated webpage for each product listing out the main characteristics, and another webpage for consumers to purchase the product. In this example, the manufacturer would be required to publish the defined support period on each of these webpages.

Requirements relating to the statement of compliance

14. What information must be included in a statement of compliance?

At minimum, the statement of compliance must include the following information.

- the product type and batch identifier
- the name and address of:
 - the manufacturer of the product
 - an authorised representative of the manufacturer
 - each (if any) of the manufacturer's other authorised representatives that are in Australia
- a declaration that the statement has been 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
 - the manufacturer has complied with any other obligations relating to the product in the security standard
- the defined support period for the product at the date the statement of compliance is issued
- the signature, name and function of the signatory of the manufacturer
- the place and date of issue of the statement of compliance.

An [example statement of compliance template](#) is available on the Home Affairs website.

15. What are the requirements for including a batch identifier on the statement of compliance?

The statement of compliance **must include a batch identifier**, if one is available for the product. The information in a statement of compliance is required to **differentiate between products** that may appear to be similar, but may have different details regarding their compliance with the security standards. Manufacturers must ensure that end-users and suppliers can use the information in a statement of compliance to **easily identify which statement of compliance applies to a product**.

The batch identifier must identify the **specific group of products manufactured or processed together**. The Rules do not stipulate the exact form the batch identifier must take.

We know that each manufacturer uses different processes to manufacture their products. There are operational and security complexities that may impact what information can be provided as the batch identifier. Manufacturers have flexibility to choose what information is **best suited for this purpose**. Manufacturers are not prohibited from **using wildcards and other identifying information** about the product to satisfy this obligation. However, manufacturers must ensure that any information provided for this purpose **clearly identifies the specific group of products manufactured or processed together** and that the **particular product that the statement of compliance relates to is in that group**.

16. The Australian standards are similar to the United Kingdom's (UK) cyber security standards. Can manufacturers use their UK statement of compliance in Australia?

The UK Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (UK Regulations) are similar to Australia's Rules, including setting out the requirements for a statement of compliance. Manufacturers of products supplied to the UK market can use the same statement of compliance provided in accordance with the UK Regulations, when supplying that product to the Australian market, as long as that statement of compliance **meets all requirements** set out in **the Act and section 9 of Australia's Rules**. An [example statement of compliance template](#) is available on the Home Affairs website.

Enforcement and regulation

17. How will compliance with the standards be monitored?

The Technology Assessment and Regulation Office within Home Affairs is responsible for regulating the cyber security of smart devices. This includes supporting the Secretary of the Department of Home Affairs to exercise their enforcement and other regulatory powers, relating to the security standards for smart devices, under Part 2 of the *Cyber Security Act 2024*.

Our enforcement framework is designed to **encourage engagement with manufacturers and suppliers** of in-scope smart devices and **uplift industry best practice**. We will take an education-first and uplift-focused approach to regulation and ensure Australian end-users are kept at the centre of our activities.

The Act allows the Secretary of the Department of Home Affairs to undertake enforcement action to ensure entities comply with their obligations under the Act. This action includes issuing compliance notices, stop notices and recall notices. The Secretary may engage experts to examine a product or statement of compliance. The Secretary may also request a statement of compliance from the manufacturer or supplier to ensure the entity has met their obligations under the Act and the Rules.

If an entity fails to comply with a recall notice, the identity of the entity, the details of the product and non-compliance, and the risks posed by the product may be published on the website of the Department of Home Affairs.