Security Standards for Smart Devices

Overview

The Cyber Security Act 2024 grants the Minister for Cyber Security the authority to implement mandatory security standards for smart devices, also known as Internet of Things (IoT) devices. These standards aim to enhance security measures, mitigate cyber risks, and improve consumer protection in the digital landscape.

Responsibilities of Manufacturers and Suppliers

Entities involved in the manufacturing and supply of smart devices intended for the Australian market must ensure their products comply with the applicable security standards.

As part of compliance, manufacturers and suppliers will be required to issue a Statement of Compliance, which should include:

Product type and batch identifier

Manufacturer's name and address, including authorized representatives in Australia
A formal declaration confirming that the product adheres to the security standard
Defined support period indicating how long security updates will be provided
Signature of an authorized signatory and the date of issue
Distributors who are not the original manufacturers may request compliance documentation from the device maker before supplying the product in Australia.

Enforcement and Regulatory Compliance

The Act establishes an enforcement framework to ensure adherence to security standards. The Department of Home Affairs has the authority to issue enforcement actions against non-compliant entities, including:

Compliance Notices – Directs an entity to rectify non-compliance by taking specific actions.
Stop Notices – Orders an entity to cease particular actions that breach security standards.
Recall Notices – Requires a product to be withdrawn from the market if it fails to meet security requirements.
Failure to comply with a recall notice may result in public disclosure, including the

identity of the non-compliant entity and details of the security risks posed by the product.

A review mechanism is in place to ensure fair and transparent enforcement. The Secretary of Home Affairs may revoke or modify enforcement notices following an internal review.

Consumer-Grade Smart Device Standard

The first set of mandatory security requirements will apply to consumer-grade smart devices, aligning with international best practices.

The standard will cover essential security measures such as:
✓ Elimination of universal default passwords – Devices must require unique passwords or allow users to define their own.
✓ Vulnerability management – Manufacturers must provide a clear process for reporting and resolving security vulnerabilities.
✓ Transparency on product support – Consumers must be informed about the minimum duration for which security updates will be provided.

This regulation will apply to smart devices that are reasonably expected to be acquired by consumers under Australian Consumer Law.

Examples of covered products include:
📱 Smart home assistants
🎥 Smart security cameras and baby monitors
📺 Smart TVs and connected appliances
⌚ Smartwatches and wearable devices

Implementation Timeline & Industry Preparation
The draft standard will undergo a 28-day public consultation period, followed by a 12-month transition phase before becoming fully enforceable.
A public awareness campaign will be launched to educate manufacturers, suppliers, and consumers about their responsibilities and rights under the new framework.

Excluded Devices
Some smart devices will be exempt from the standard due to:

- Existing legislation that already addresses cybersecurity risks.
- Government-led initiatives to develop specialized security frameworks.
- Technical complexity that requires tailored security measures.

Conclusion

The introduction of security standards for smart devices is a critical step in strengthening cybersecurity across connected products in Australia. By holding manufacturers accountable and ensuring robust security practices, these regulations will protect consumers, businesses, and national infrastructure from cyber threats.

For more details or to participate in the consultation process, please visit the official Cyber Security Authority website.

Legal Disclaimer

The information provided in this document has been carefully compiled to ensure accuracy. However, we assume no liability for any errors, omissions, or timeliness of the content.