EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs and the Minister for Cyber Security

Cyber Security Act 2024

Cyber Security (Security Standards for Smart Devices) Rules 2025

Legislative Authority

The *Cyber Security (Security Standards for Smart Devices) Rules 2025* (the Rules) are made under sections 14, 16 and 20 of the *Cyber Security Act 2024* (the Act).

Purpose and background

Part 2 of the Act provides the power for the Minister to prescribe rules to establish mandatory security standards for products that can directly or indirectly connect to the internet ('relevant connectable products') that will be acquired in Australia in specified circumstances. To be subject to a security standard, products must be in the specified class of products and be acquired in the circumstances specified by the Rules, unless they are exempt.

Part 2 of the Act places obligations on manufacturers of products that are subject to a security standard to manufacture the products in compliance with the security standard and to comply with any other obligations relating to the product that are set out in the security standard. Suppliers of products subject to a security standard must not supply the product if they are aware the product is not compliant with the relevant security standard. Suppliers must also supply the product in Australia with a statement of compliance prepared by the manufacturer, which is a statement that, among other things, provides that the product is compliant with a relevant security standard.

The primary purpose of the Rules are to establish security standards for consumer grade products under section 14 of the Act of Division 2 of Part 2 of the Act, which will apply to the specified class of products, unless exempted, that are intended to manufactured to be used, or are of a kind likely to be used, for personal, domestic or household consumption, per Australian Consumer Law. In addition, the security standards will only apply to products that could reasonably be expected to be acquired in Australia by a consumer. The security standards will apply to products that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources.

The security standards in Schedule 1, Part 1 of the Rules closely follows 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)*. Accordingly, the security standards will impose the following obligations relating to these products:

- **Password requirements** – requirements on manufacturers to manufacture products so all consumer smart device passwords need to be unique per product or defined by the user;

- **Publication requirements for reporting security issues** – requirements for manufacturers to publish details on how security issues are to be reported, which will allow security researchers and others to report issues, with status updates on the resolution of these issues.

- **Defined support period publication** – requirements for manufacturers and suppliers to publish details about the defined support period, which is the period in which security updates will be provided by, or on behalf of, the manufacturer.

In addition to the establishment of the security standards for consumer grade products, the Rules also specify, for the purpose of section 16 of Division 2 of Part 2 of the Act, requirements relating to statements of compliance for products that are subject to the security standards. The Rules specify what information the statements of compliance must contain, including details about the manufacturer of the product and a statement whether, in the opinion of the manufacturer of the product, the product is compliant with the security standards. The instrument also specifies other requirements relating to statements of compliance, including the period for which a supplier or manufacturer must retain them.

Sections 17, 18 and 19 of Division 2 of Part 2 of the Act outline a series of enforcement notices and detail within that may be issued to a responsible entity if there is reasonable suspicion of non-compliance with the Rules. These are compliance notices (section 17), stop notices (section 18), and recall notices (section 19). Subsections 17(2)(h), 18(2)(h), and 19(2)(h), specify rules made under this Part of the Act may contain other matters that can be set out in these enforcement notices. The enforcement notices for these Rules do not require further detail in addition to those set out in the Act. However, future rules for smart devices may set out other matters in relation to enforcement notices.

The final purpose of these Rules is to specify, for the purpose of section 20 of Division 2 of Part 2 of the Act, other matters that may be published by the Minister on the public notification of failure to comply with a recall notice. The Rules specify that in addition to the matters contained in the Act, the Minister may also specify details of the recall notice and actions consumers are recommended to take in response to the notice.

Part 1 of the Rules will commence the day after the Rules are registered. Part 2 and Schedule 1 of the Rules commence 12 months after registration.

Consultation

The Rules are made by the Minister for Cyber Security in accordance with the requirements of subsection 87(3) of the Act. This subsection specifies, the Minister, before making or amending rules under the Act, must publish a notice that:

- sets out the draft rules or amendments, and

- invites persons to make submissions to the Minister about the draft rules within a period not shorter than 28 days.

The Minister must also consider any submissions received during the period specified in the notice.

In accordance with these requirements, the draft Rules were published on the Department's website on 16 December 2024 and closed for submissions on 14 February 2025. 18 submissions were received in relation to these Rules.

Common themes of stakeholder feedback included:

- that a longer transition or implementation period was needed than the proposed 12 months. This recommendation was considered and on balance, it was decided that 12 months is a sufficient period given, in particular, similar regulations in the UK also had a 12 month transition period that ended in April 2024. Manufacturers with products in the UK market are already required to meet similar requirements if they are operating across these jurisdictions.

- that the retention period for statements of compliance should be reduced from the proposed 10 years to five years. This recommendation has been incorporated and this is now reflected in the Rules. This suggestion is consistent with the average lifespan of a relevant connectable product and reduces administrative burden on industry.

- that guidance should be provided to manufacturers and suppliers in the lead up to the Rules being enforced. This is consistent with the Department's intent to provide communication and guidance materials over the transition period.

The Department engaged industry stakeholders from across all sectors in a consultation process to design the instrument and primary legislation. On 19 December 2023, the Minister released the Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper. Consultation remained open until 1 March 2024. The Department received over 130 written submissions and the feedback focused on ensuring the measures achieve their intended outcomes.

Consultation on options to secure smart devices was also included as part of broad industry consultation on the development of the 2023-2030 Australian Cyber Security Strategy (the Strategy). The Australian Government launched consultation on the Strategy on 27 February 2023 and closed consultation on 15 April 2023.

In these circumstances, the Minister was satisfied that appropriate consultation was undertaken, in accordance with section 17 of the *Legislation Act 2003* because:

- persons and industry organisations likely to be affected by the Rules had an adequate opportunity to comment on the draft Rules; and

- extensive industry consultation was undertaken on the primary legislation and smart device standards policy more broadly.

Impact analysis statements were prepared by the Department of Home Affairs and published by the Office of Impact Analysis at **Attachment C and D**. Impact analysis was originally conducted in relation to this measure during the development of the Strategy, and showed that introducing the combination of a mandatory product standard and a voluntary labelling scheme for smart devices would be the best option to ensure that smart devices sold in the Australian market are secure, while also empowering consumers to make informed decisions. This position was supported by stakeholder consultation.

Following publication, the Department of Home Affairs, in collaboration with the Department of Climate Change, Energy, the Environment and Water (DCCEEW), prepared an addendum to the original impact analysis relating to the inclusion of consumer energy resources (CER) within the scope of these reforms. Since consumer energy resources (CERs) were not within the methodological scope of the original impact analysis, DCCEEW provided an equivalent impact analysis for the application of these policy decisions to CERs. This analysis came to the same conclusions regarding CERs as the original impact analysis provided for other consumer grade smart devices.

Other matters

The Rules are a legislative instrument for the purposes of the *Legislation Act 2003* and are subject to disallowance.

Details of the Rules are set out in **Attachment A**.

A Statement of Compatibility with Human Rights provides that the Rules are compatible with human rights as they do not raise any human rights. The Statement is included at **Attachment B**.

ATTACHMENT A

Details of the *Cyber Security (Security Standards for Smart Devices) Rules 2025*

Part 1 Preliminary

Section 1 Name

This section provides that the name of the instrument is the *Cyber Security (Security Standards for Smart Devices) Rules* 2025 (the Rules).

Section 2 Commencement

Section 2 provides for the commencement provisions of the Rules.

Subsection 2(1) provides that each provision of Rules specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table.

The effect of column 2 is that Part 1 of the Rules, and anything else not covered in the table, will commence the day after the Rules are registered.

Part 2 and Schedule 1 of the Rules commence 12 months after registration.

A note at the foot of the table explains that the table relates only to the provisions of the Rules as originally enacted. The table will not be amended to deal with any later amendments of the Rules.

Subsection 2(2) provides that any information in column 3 of the table is not part of the Rules. Information may be inserted in this column, or information in it may be edited, in any published version of the Rules.

Section 3 Authority

This section provides that the Rules are made under the *Cyber Security Act 2024* (the Act).

Section 4 Definitions

This section sets out definitions of terms used in the Rules.

The note in section 4 provides that a number of the expressions used in the Rules, including manufacturer, relevant connectable product and supplier, are defined in the Act.

The reference to ***Act*** in the Rules is the *Cyber Security Act 2024*.

Consumer is defined in section 6 of the Rules. Section 6 provides that a person has acquired goods as a consumer if the person would be taken to have acquired the goods as a consumer under section 3 of the Australian Consumer Law (ACL).

Defined support period has the meaning given by subclause 4(3) of Schedule 1. Subclause 4(3) of Schedule 1 defines a defined support period to mean the period, expressed as a period of time with an end date, for which the security updates will be provided by, or on behalf of the manufacturer of the product.

Part 2 Security standards for smart devices

Division 1 - Preliminary

Section 5 Simplified outline of this Part

This section provides a simplified outline for the operation of the Rules.

The simplified outline provides guidance to the reader about the rule-making power in Part 2 of the Act relating to security standards. The simplified outline provides that rules may provide mandatory security standards for products that connect directly or indirectly to the internet (relevant connectable products) that are acquired in Australia in specified circumstances.

The simplified outline makes clear that Schedule 1 establishes a security standard for consumer grade relevant connectable products (unless exempted) that will be acquired in Australia by a consumer, which is the specified circumstance for the purpose of subsection 16(1) of the Act.

The simplified outline further provides that sections 15 and 16 of the Act impose obligations for:

- manufacturers to manufacture products in compliance with a security standard if they are aware, or could reasonably be expected to be aware, that the product will be acquired in Australia in a specified circumstance;
- manufacturer to comply with any other obligations relating to the product in the security standard, including obligations to publish information about the product;
- suppliers to not supply non-compliant products in Australia if the supplier is aware, or could reasonably be expected to be aware, that the products will be acquired in Australia in a specified circumstance; and
- suppliers to supply the product in Australia accompanied by a statement of compliance.

Simplified outlines are included to assist readers to understand the substantive provisions. The outline for the Rules is not intended to be comprehensive, and readers should rely on the substantive provisions.

Section 6 Meaning of consumer

This section defines the meaning of 'consumer' for the Rules. This section provides that a person has acquired particular goods as a consumer if the person would be taken to have acquired the goods as a consumer under section 3 of the ACL.

Section 3 of the ACL provides that a person is taken to have acquired particular goods as a consumer, provided no exception in subsection 3(2) applies, if:

- the amount paid or payable for the goods (as determined under section 3) did not exceed $40,000, or a greater amount if prescribed. At the time of the registration of the Rules, $100,000 has been prescribed for the purpose of determining if goods have been acquired as a consumer; or
- the goods were of a kind ordinarily acquired for personal, domestic or household use and consumption (regardless of cost); or
- the goods consisted of a vehicle or trailer acquired to be used primarily used in the transport of goods on public roads (regardless of cost).

Division 2 - Security standards for relevant connectable products

Section 7 Purpose of this Division

This section provides that for the purposes of subsection 14(1) of the Act, this Division provides security standards for specified classes of relevant connectable products that will be acquired in Australia in specified circumstances.

Section 8 Security standards for consumer grade relevant connectable products

This section outlines, for the purposes of subsection 14(1) of the Act, the specified class of relevant connectable products and the specified circumstance they will be acquired in Australia. In order to be subject to the security standard in Part 1 of Schedule 1, a relevant connectable product must belong to the specified class and be acquired by a consumer in the specified circumstance as prescribed in this section.

The Act enables security standards to be made for relevant connectable products. While these are commonly referred to as 'smart devices', a product is typically a combination of the device (hardware and internal software) and its device external software (companion application or app).

Subsection 8(1)(a) provides that the security standard in Part 1 of Schedule 1 applies to the specified class of relevant connectable products that are intended by the manufacturer to be used, or of a kind likely to be used, for personal, domestic or household consumption.

However, under subsection 8(1)(b) certain relevant connectable products that may otherwise be within the specified class are exempted from being subject to the security standard in Part 1 of Schedule 1. The ability to exempt these items in this way is enabled under subsection 13(2) of the Act. The products exempted are:

- a desktop computer or a laptop;
- a tablet computer;
- a smartphone;
- therapeutic goods within the meaning of the *Therapeutic Goods Act 1989*;
- a road vehicle within the meaning of the *Road Vehicle Standards Act 2018;* and
- a road vehicle component within the meaning of the *Road Vehicle Standards Act 2018*.

Particular products have been exempted on the basis of existing regulatory frameworks which cover them. For example, the regulation of vehicles are covered by the powers in the *Road Vehicle Standards Act 2018* that enables the Minister for Transport to determine standards for road vehicles or road vehicle components. Similarly, medical devices are typically more strictly regulated by more established regulatory systems – in Australia, this responsibility sits under the Therapeutic Goods Administration.

Other products, including desktop computers, tablets and smart phones, have been exempted due to the difficulty manufacturers of these products would face in complying due to the complex nature of the supply chains of product components. These products (other than smart phones) have also been excluded from similar international regulatory frameworks such as in the UK. With evolving technical advice and support from industry, government can explore the specific cyber security challenges in complex products, and develop bespoke measures to ensure their security.

For additional clarity, examples of specific products that may or may not be within scope of this standard, and some relevant considerations from the ACL, include:

- smart meters – these products are not considered within the scope of this standard as the primary purpose of a smart meter is to be supplied, installed and used by an electricity retailer. Smart meters are not ordinarily acquired, purchased, or installed by a consumer in Australia;
- point of sale or contactless payment products – these products (provided they cost less than the threshold outlined under the ACL) can be considered within the scope of this standard on the basis that they meet at least one of the conditions of business consumer guarantees:
    - it costs less than $100,000 including GST;
    - it is a product or service commonly bought for personal, domestic or household use; and
    - the good is a vehicle or trailer that is used mainly to transport goods on public roads.

While there are some exclusions for business products outlined under ACL, contactless payment devices do not fit these conditions so are considered in scope under these Rules. These conditions include where a product is intended for resupply, use or transformation in production and

manufacturing, or to repair or treat other goods. These considerations are relevant to whether or not the contact payment devices meet the definition of a kind acquired by a consumer under the ACL, which is a requirement for the purpose of enlivening the security standard in Schedule 1.

Subsection 8(2) provides that the specified circumstance in which these goods will be acquired in Australia for the purpose of enlivening the security standard in Part 1 of Schedule 1, is if the goods are acquired by a consumer (as defined in section 6 of the Rules).

The scope of this standard is being applied to consumer grade relevant connectable products to improve security for as much of the economy as possible. Evidence suggests that even though manufacturers and suppliers have been provided with voluntary guidance to raise the cyber security baseline of smart devices, market failures persist among responsible entities to take steps to proactively protect consumers from basic vulnerabilities. The security measures set out in Schedule 1 achieve a balance of enhanced cyber security protections for consumers, while maintaining a relatively low level of burden on industry.

Division 3 – Statements of compliance

Section 9 Requirements for statement of compliance

This section provides, for the purpose of subsection 16(5) of the Act, the requirements for a statement of compliance with the security standard in Part 1 of Schedule 1 (consumer grade relevant connectable products). Subsection 16(5) of the Act provides that Rules may specify requirements for statements of compliance prepared under subsections 16(1) and 16(2) of the Act. Statements of compliance must meet any requirements specified in Rules in order for a manufacturer to meet their statement of compliance obligations.

Subsection 9(2) provides that the statements of compliance prepared under subsection 16(1) of the Act must be prepared by, or on behalf of, the manufacturer of the product.

Subsection 9(3) specifies what information the statement of compliance for the security standard in Part 1 of Schedule 1 must include to be compliant. The following is specified:

- the product type and batch number (an identifier for a specific group of products manufactured or processed together);
- the name and address of the manufacturer, an authorised representative of the manufacturer and each (if any) of the manufacturers authorised representatives 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 security standard and that 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; and
- the place and date of issue of the statement of compliance.

The information in a statement of compliance is required to differentiate between products that may appear to be similar, for example two products with different manufacturing dates may have different security updates installed by default. The statement of compliance also verifies that, to the knowledge of the manufacturer, a product meets the security standard specified in the Rules. Details of the manufacturer will provide the regulator with a point of contact if there are concerns with the statement of compliance.

Statements of compliance are not required to be provided with the product at point of sale. The statement of compliance is for the use of the regulator to ensure the responsible entity has met their obligations under the Act and Rules. However, responsible entities may provide or publish statements of compliance with their product if they wish to do so.

Responsible entities operating across other jurisdictions with similar compliance frameworks for consumer grade smart devices can provide the same information for the purpose of the statement of compliance. For example, products supplied to the UK market under the *Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023* can provide the same statement of compliance for the Australian market, as long as all the requirements set out in this section are met.

Section 10 Retention period for statement of compliance

This section provides that for the purposes of subsections 16(2) and 16(4) of the Act, the retention period for statements of compliance with the security standard in Part 1 of Schedule 1 is five years. The obligation to retain statements of compliance for this period applies to both manufacturers and suppliers.

Division 4 – Notification of failure to comply with recall notice

Section 11 Matters to be published with notification of failure to comply with recall notice

This section provides, for the purposes of paragraph 20(e) of the Act, other matters that may be published with the notification of failure to comply with recall notice on the Department's website, or in another way that the Minister considers appropriate. Section 20 of the Act specifies what information the Minister may publish where an entity has failed to comply with a recall notice, including the identity of the entity, details of the product and details of and risks posed by the non-compliance. Section 19 of the Act deals with recall notices.

Paragraph 11(a) of the Rules specifies that the Minister may also publish the details of the recall notice given to the entity under section 19 of the Act in the notification of failure to comply with recall notice.

Paragraph 11(b) of the Rules specifies the Minister may also publish actions consumers are recommended to consider taking regarding continued product use in the notification of failure to comply with recall notice. This paragraph provides examples of actions consumers may take that may be included on the notice for this purpose, including destroying the product or taking extra precautions when using the product.

Schedule 1 – Security standards

Part 1 Security standard for consumer grade relevant connectable products

The note under Part 1 of the Rules directs the reader to section 8 of the Rules. Section 8 of the Rules provides the class of relevant connectable products that the security standard within this part applies to, and the products that are exempt from the security standard. Section 8 also provides the specified circumstance in which the security standard is to comply (if the products will be acquired in Australia by a consumer).

Clause 1 Definitions

This clause sets out the definition of terms used in the security standard in Part 1 of Schedule 1.

Application programming interface key means a string of characters used to identify and authenticate a particular user, product, or application so that it can access the application programming interface.

Cryptographic key means data used to encrypt and decrypt data. For clarity, this could include a key or code.

Factory default state means the state of the product after factory reset or after final production or assembly.

Good industry practice means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced cryptographer, engaged in the same type of activity.

Hardware is defined to mean a physical electronic information system, or parts thereof, capable of processing, storing or transmitting digital data.

Incremental counter means a method of password generation in which multiple passwords are the same save for a small amount of characters which change per password to make them unique. The definition provides example of passwords based on incremental counters includes "password1" and "password2".

Keyed hashing algorithm means an algorithm that uses a data input and a secret key to produce a value which cannot be guessed or reproduced without knowledge of both the data input and the secret key.

Manufacturer's intended purpose of a product is defined to mean the use for which the product is intended according to the data provided by the manufacturer, including on the label, in the instructions for use, or in promotional or sales materials or statements. Importantly, the manufacturer's intended purpose remains consistent even if a user does not use that purpose.

Password is defined to not include a cryptographic key, a personal identification number used for pairing in communication protocols which do not form part of the internet protocol suite, or an application programming interface key.

Secret key means a cryptographic key intended to be known only by the person who encrypted or authorised the encrypting of the data, and any person authorised by the person.

The definition of ***security update*** provides that this term is defined in subclause 4(2) of Part 1 of Schedule 1.

Unique per product means unique for each individual product of a given product class or type (that is, alternatively, each individual unit of the product).

Clause 2 Requirements in relation to passwords

This clause contains security requirements relating to the passwords for relevant connectable products subject to this security standard if the product has password functionality.

Subclause 2(1) provides that these requirements apply in relation to passwords being used in relation to those aspects of relevant connectable products as specified in this subclause:

- Hardware for the product when the product is not in the factory default state;
- Preinstalled software for the product when the product is not in the factory default state at the point the product is supplied to a consumer; or
- Software that is not preinstalled at the point it is supplier to a consumer, but which must be installed on the product for all the manufacturer's intended purposes of the products that use hardware, preinstalled software or installable software. For example, this would cover a software update installed after sale that requires additional applications of passwords to fulfil the manufacturer's intended purpose of the product.

Subclause 2(2) specifies that the passwords must be unique per product, subject to subclause 2(3) (see paragraph below), or defined by the user of the product. The definition of password in clause 1 of the Schedule excludes particular things from being considered a password for this purpose of this clause.

For the purpose of paragraph 2(a), subclause 2(3) provides that passwords which are unique per product must not be:

- Based on incremental counters;
- Based on or derived from publicly available information;
- Based on or derived from unique product identifiers. For this purpose, the Rules provides that unique product identifiers include serial numbers, unless this is done using an encryption method, or key hashing algorithms that is accepted as part of good industry practice; or
- Otherwise guessable in a manner unacceptable as part of good industry practice.

The intention of subclause 2(3) is to ensure that manufacturers prescribing default passwords covered by this clause employ all parts of good industry practice (as defined in clause 1 of the Schedule 1) to ensure these passwords are not unacceptably guessable by any party (noting a user would not be guessing a password that is known to them).

Clause 3 Requirements relating to reports of security issues

This clause contains requirements for manufacturers of a relevant connectable products subject to this security standard to publish details on how security issues are to be reported.

Subclause 3(1) provides that the manufacturer must publish details about how a person would report security issues in relation to any of the following aspects of the relevant connectable products listed in this subclause. For this purpose, subclause 3(1) specifies the following aspects of relevant connectable products:

- the hardware of the product;
- software which is preinstalled on the product at the point in which the product is supplied to a consumer;
- software which must be installed on the product for all the manufacturer's intended purposes of the product that use hardware, preinstalled software, installable software; and
- software used for, or in connection with, any of the manufacturer's intended purposes of the product.

Subclause 3(2)(a) specifies the information that the manufacturer must publish in relation to reporting security issues for the things specified in subclause 3(1). It specifies that the manufacturer must publish at least one point of contact to allow a person to report the security issue to the manufacturer.

Subclause 3(2)(b) further specifies that when a person makes a report about a security issue, the manufacturer must ensure the person receives an acknowledgment of the receipt of the report and status updates until the resolution of the reported security issues.

Subclause 3(3) specifies particular requirements that information published under subclause 3(2) must meet. In addition to the information published being accessible, clear and transparent, the information must be made available to a person without prior request for this information being made, in English, free of charge and without requesting the personal information about the person making the report. For example, a manufacturer may choose to publish the details for their point of contact readily in plain English on their website.

Paragraph 3(3)(d) prevents the manufacturer from requesting the provision of personal information for a person to access the information required to be published under subclause 3(2). However, it should be noted that through responding to a person's report of a security issues the manufacturer may request the provision of reasonable contact information, such as an email address (which may include or itself be considered personal information) about the person making the security issue report, for the purposes of satisfying the provision of acknowledgement and status updates required under paragraph 3(2)(b). Any collection, use or disclosure of personal information by the manufacturer would still be subject to the applicable privacy law, such as the *Privacy Act 1988*.

Clause 4 Requirements relating to defined support periods and security updates

This clause contains requirements for manufacturers of relevant connectable products subject to this security standard to publish details on the defined support period for security updates.

Subclause 4(1) provides the manufacturer must publish the defined support period for security updates for the product in respect of the following:

- hardware of the product capable of receiving security updates;
- preinstalled software on the product (at the point where it is supplied to a consumer) that is capable of receiving security updates;
- software that is capable of receiving security updates, which must be installed on the product for all the manufacturer's intended purposes of the product that use hardware, preinstalled software, installable software; and
- software developed by or on behalf of any manufacturer of a product that is capable of receiving security updates and used for, or in connection with, any of the manufacturer's intended purposes of the product.

Subclause 4(2) defines what a security update is. It provides that a security update is a software update that protects or enhances the security of the product, including a software update that addresses a security issue which has been discovered or reported to the manufacturer.

Subclause 4(3) defines that a defined support period is the period, expressed as a period of time with an end date, for which the security updates will be provided by, or on behalf of, the manufacturer of the product. The defined support period should include a fixed end date, rather than an end to the period of time. For example, "no later than 30 June 2027".

For the purposes of subclause 4(3), the manufacturer must provide an available security update to a product, while the product is within its defined support period, as far as practicable and in line with good industry practice.

Subclause 4(4) provides that a manufacturer must not shorten the defined support period once it is published, though it may be extended. Accordingly, subclause 4(5) provides that if a manufacturer extends the defined support period, the new defined support period must be published by, or on behalf of, the manufacturer as soon as is practicable.

Subclause 4(6) provides requirements for the publication of the defined support period under subclause 4(1) or the publication of an extension to a defined support period under subclause 4(5). It provides that the information published relating to the defined support period must be accessible, clear and transparent and made available to a person:

- free of charge in English;
- without a prior request for such information being made;
- without requesting the personal information about the person who accesses the information; and
- in a way that is understandable by a reader without prior technical knowledge.

Subclause 4(7) provides requirements for the publication of the defined support period in the circumstance a manufacturer of a relevant connectable product offers to supply the product on its website, or another website under its control. Supply is a defined term in section 8 of the Act and has the same meaning as in the ACL.

In the circumstance where the manufacturer supplies the product on its website, or another website under its control, subclause 4(7) provides that the manufacturer has two additional requirements. The first is that the defined support period, or any extension to a defined support period, is prominently published with other information on the website that is intended to inform consumers' decisions to acquire the product. This applies in each instance on the website that information is published that is intended to inform consumer decision to acquire the product.

The second requirement is that for each instance on the website that the main characteristics of the product are published, that the defined support period, or any extension to a defined support period, is published alongside or otherwise given equal prominence to the publication of the main characteristics of the product.

The defined support period must be published in any location on the website where either of these criteria are met. This may mean the manufacturer will be required to publish the defined support period in multiple locations on their website, or other website under their control.

The intention of this requirement is to ensure that a person contemplating the purchase of a product can easily find the defined support period while examining information about the product, and subsequently be able to consider the defined support period in their purchasing decision.

Importantly, a person should not be required to unnecessarily navigate a website to discover the location of the defined support period. Further, the discovery of the defined support period should not rely on a person's knowledge of the existence of the Act, its Rules or this Schedule. For example, the defined support period should not only be published in the statement of compliance or in a regulatory section of a website if the information intended to inform a consumer's decision to acquire the product or the main characteristics of the product are published elsewhere on the website).

The publication of the main characteristics of the product refers to the publishing of a sufficient collection of information about the product with the intention of a person being able to obtain a holistic understanding of the product's features, benefits and intended functions.

Correspondingly, product information published on a website is not always intended to inform consumer decisions to acquire the product.

Product information webpages (where information such as product characteristics, functions, features, benefits, and technical specifications are published), product purchase webpages, and product comparison webpages are examples of locations on a manufacturer's website (or other websites under their control) where information that would inform a consumer's decision to acquire a product, or the main characteristics of the product, is likely to be found.

Generic product press releases, support articles, and information for accessories of the product (for example, the purchase webpage for a smartphone case) are examples of locations that are not likely to contain information that would be intended to inform a consumer's decision to acquire a product, or contain the main characteristics of the product. It should be noted that some accessories will amount to consumer grade relevant connectable products in their own right, and therefore require their own defined support periods to be published.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Cyber Security (Security Standards for Smart Devices) Rules 2025

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Overview of the Disallowable Legislative Instrument

Australia's cyber security landscape is evolving, with malicious activities targeting Australia becoming more frequent and sophisticated. The *Cyber Security Act 2024* (the Act) provides a clear legislative framework for whole-of-economy cyber security issues. The Act was introduced to provide additional protections to Australian citizens and businesses; improve the security of our increasingly interconnected devices; build mitigations for existing cyber risks; and improve the Government's threat picture to inform protections, incident response procedures and future policy.

Under Part 2 of the Act, the relevant Minister may prescribe security standards for all, or a range of, smart devices, defined as relevant connectable products.

The *Cyber Security (Security Standards for Smart Devices) Rules 2025* (Disallowable Legislative Instrument) establish the security standards for consumer-grade relevant connectable products. Responsible entities (manufacturers and suppliers) of products subject to the security standards must comply with the standards.

The primary purpose of the Disallowable Legislative Instrument is to establish security standards for consumer grade products under section 14 of the Act, which will apply to the specified class of products, unless exempted, that are intended by the manufactured to be used, or are of a kind likely to be used, for personal, domestic or household consumption. In addition, the security standards will only apply to products that could reasonably be expected to be acquired in Australia by a consumer. The security standards will apply to products that consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and consumer energy resources.

In addition to the establishment of the security standards for consumer grade products, the instrument also specifies, for the purpose of section 16 of the Act, requirements relating to statements of compliance for products that are subject to the security standards. The Disallowable Legislative Instrument specifies what information the statements of compliance must contain, including details about the manufacturer of the product and a statement whether, in the opinion of the manufacturer of the product, the product is compliant with the security standards. It also specifies other requirements

relating to statements of compliance, including the period that a supplier or manufacturer must retain them.

The final purpose of the Disallowable Legislative Instrument is to specify, for the purpose of section 20 of the Act, other matters that may be published by the Minister on the notification of failure to comply with recall notice register. The Disallowable Legislative Instrument specifies that in addition to the matters contained in the Act, the Minister may also specify details of the recall notice and actions consumers are recommended to take in response to the notice.

Human rights implications

This Disallowable Legislative Instrument may engage the following right:

- the prohibition on interference with privacy in Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR)

Article 17(1) of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy.

Interferences with privacy may be permissible, where they are authorised by law and not arbitrary. In General Comment 16, the United Nations Human Rights Committee (UNHRC) argued that the introduction of the concept of arbitrariness in Article 17 "is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be in any event, reasonable in the particular circumstances." The UNHRC further clarified that "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[1]

The Act imposes an obligation on manufacturers of relevant connectable products to respectively manufacture and supply products with a statement of compliance with a security standard. The Disallowable Legislative Instrument prescribes requirements for what a statement of compliance must contain and includes the name and address of the manufacturer of the product; and an authorised representative of the manufacturer; and each (if any) of the manufacturer's other authorised representatives that are in Australia. The statement of compliance must also include the signature, name and function of the signatory of the manufacturer. A statement of compliance must be supplied with a relevant connectable product and will also be available on the manufacturer's website.

In most cases, the entity identified on the statement of compliance will be a manufacturer or a supplier with business details. However, in the rare occurrence that an entity is a sole trader, their personal information may be published in the statement of compliance. Further, the signatory of a manufacturer would also have their personal information published in the statement of compliance. To the extent that an individual is a sole trader or a signatory of a manufacturer and their personal information (name and address) is disclosed in a statement of compliance, the right to privacy will be limited.

Limiting the right to privacy is reasonable and necessary to ensure entities are appropriately accountable for guaranteeing compliance with security standards for relevant connectable products, which are designed for everyday use by Australian consumers. It is also reasonable and necessary to provide sufficient information and corporate authorisation to relevant parties of the compliance of the particular product with a given security standard. This measure is proportionate to achieving the

[1] *Toonen v Australia*, Communication No. 488/1992, para. 8.3; see also communications Nos. 903/1999, para 7.3, and 1482/2006, paras. 10.1 and 10.2.

legitimate objective of protecting public order and the rights and freedoms of others, by ensuring that the public can be made aware of a device's compliance with security standards prescribed under the Act. The security standards seek to improve the cyber security of relevant connectable products and protect Australians from pertinent cyber-attacks and breaches of their personal information.

The Act also establishes a regulatory framework that includes a series of enforcement notices for relevant entities. The final type of notice under this framework is a recall notice under section 19 of the Act, issued when a responsible entity has repeatedly failed to comply with the relevant security standard prescribed for the specific smart device, or actions taken to remediate the issue have proven unsuccessful. Failure to comply with a recall notice could be published on the Department's website or in any other way the Minister considers appropriate. A notice can include relevant information such as details of the manufacturer and/or supplier of the smart device so acquirers of the device can easily identify if they have been affected by a product recall.

Pursuant to section 20 of the Act, the Disallowable Legislative Instrument prescribes matters that may be published with a notification of failure to comply with recall notice. Section 11(a) of the Disallowable Legislative Instrument provides that details of the recall notice given to the entity under section 19 of the Act may be published for this purpose. This includes information that discloses the identity of the entity. In most cases, the entity will be a manufacturer or a supplier with business details. However, in the rare occurrence that an entity is a sole trader, their personal information may be published to inform acquirers of a device that the device does not meet the security standard prescribed. In these instances, the Department of Home Affairs will carefully consider and balance publication of personal information, to ensure available information is proportionate to the risks that non-compliant smart devices pose to the Australian public.

To the extent that an individual is a sole trader and their name is disclosed in a published recall notice, the right to privacy will be limited. Limiting the right to privacy is reasonable, necessary and proportionate to provide sufficient information to owners of affected devices that do not meet relevant security standards to be able to identify those devices and inform them of the manufacturers or suppliers of those devices, enabling owners to take appropriate remedial action. This measure is aimed at the legitimate objective of protecting public order and the rights and freedoms of others, by ensuring that the public can be made aware of devices which do not comply with security standards. Non-compliance with a security standard may potentially expose a person to cyber security-related breaches, including criminal actors gaining access to their personal information.

The proposed rules in the Disallowable Legislative Instrument establish the minimum security standards and scope for consumer-grade smart devices, which are reasonable, necessary and proportionate to achieving the legitimate objective of protecting the Australian community from cyber security related breaches.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights because to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

The Honourable Tony Burke MP
Minister for Home Affairs and Minister for Cyber Security