Australian Government

Department of Home Affairs

Cyber Security Legislative Reforms – Explanatory Document

Cyber Security (Security Standards for Smart Devices) Rules

© Commonwealth of Australia 2024

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at https://creativecommons.org/licenses/by/4.0/legalcode.

This means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website at https://creativecommons.org/ as is the full legal code for the CC BY 4.0 license at https://creativecommons.org/licenses/by/4.0/legalcode.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of the Prime Minister and Cabinet website— https://www.pmc.gov.au/government/commonwealth-coat-arms.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P-23-02503-c

Contents

Cyber Security (Security Standards for Smart Devices) Rules

Context

Australia's cyber security landscape is evolving quickly, with malicious activities targeting Australia becoming more frequent and sophisticated. The Cyber Security Act is designed to provide a clear legislative framework for broad, whole-of-economy cyber security issues, positioning the Australian Government to respond to new and emerging cyber security threats. The Act is intended to provide additional protections to Australian citizens and businesses, build mitigations for extant cyber risks, and improve the Government's threat picture to inform protections, incident response procedures, and future policy.

To date, Australia's voluntary approach to smart device security is fragmented and insufficient. In 2020, the Government introduced a voluntary Code of Practice: Securing the Internet of Things for Consumers setting out guidance for smart device manufacturers and suppliers aligned to the European Telecommunications Standards Institute (ETSI) standard. A government study of manufacturers' uptake of the Code revealed a low level of adoption across the country. Mandatory standards will uplift the cyber security of smart devices in Australia and ensure that Australians can trust in the security of their digital products.

Scope of devices under the standard

The power within the Act enables the Minister for Cyber Security to prescribe security standards for all, or a subclass of, smart devices, through subordinate legislation, also known as rules. As the initial application of the power, it is intended the rules will detail the technical security standards required for consumer-grade relevant connectable products. Future applications of the rules will be considered as required, for example to address risks with evolving technology.

Products that are included in the scope of the intended security standard are outlined under Division 2. This is covers smart devices that meet the definition of ***relevant connectable product*** as defined in section 13 of the Cyber Security Act and that would be expected to be reasonably acquired by a ***consumer*** per *Australian Consumer Law,* per section 6 of the Rules. The combined definitions means that this set of rules applies only to consumer-grade smart devices unless otherwise exempted from the rules.

The rules provide that the security standard for the specified class i.e. consumer-grade, apply to products that will be acquired in Australia, and the security standard applies to products that are intended by the manufacturer of the product to be acquired for personal, domestic, or household use, per section 8(1)(a). The rules further specify that the acquisition is intended to be in Australia by a ***consumer***, under section 8(2). Where a business acquires a product as a consumer, the business will have the same protections as outlined in the Australian Consumer Law.

The proposed consumer-grade standard will be operational 12 months after it has been made in Rules to allow industry sufficient time to prepare for the new requirements.

Exempt devices

The proposed format of rules takes an exclusion-based approach for the coverage of devices for each specified security standard. Generally, devices will be excluded if: there is existing legislation that can adequately address the cyber security of 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. The list of excluded devices for each standard can be amended to exclude further devices, or scope devices back under the coverage of the standard.

Under section 8(b), the consumer-grade smart device standard excludes the following types of devices:

Desktop computers or laptops, tablets, and smartphones.	Manufacturers of these devices would face unique challenges in complying due to the complex nature of the supply chains of device components. These devices (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 devices, and develop bespoke measures to ensure their security.
Medical devices, otherwise known as therapeutic goods as defined in the *Therapeutic Goods Act 1989.*	Medical devices are typically more strictly regulated and by more established regulatory systems – in Australia, this responsibility sits under the Therapeutic Goods Administration.

Road vehicles and road vehicle components as defined by sections 6 and 7 of *the Road Vehicle Standards Act* 2018 respectively.	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. While road vehicles and road vehicle components are proposed to be exempt from the consumer-grade smart device standard (per draft rules), a new standard for the cyber security of road vehicles could be added under the Cyber Security Act should the existing Road Vehicle Standards Act 2018 not be sufficient.

Statements of compliance

Division 3 of the Rules sets out the minimum details necessary for a statement of compliance for devices that are required to meet the security standard. The statement must be prepared by or on behalf of the manufacturer and must include, at a minimum:

(a) the product type and batch identifier;
(b) the name and address of:
    i. the manufacturer of the product; and
    ii. an authorised representative of the manufacturer; and
    iii. each (if any) of the manufacturer's other authorised representatives that are in Australia;
(c) a declaration that the statement has been prepared by, or on behalf of, the manufacturer of the product;
(d) a declaration that, in the opinion of the manufacturer:
    i. the product has been manufactured in compliance with the requirements of the security standard; and
    ii. the manufacturer has complied with any other obligations relating to the product in the security standard;
(e) the defined support period for the product at the date the statement of compliance is issued;
(f) the signature, name and function of the signatory of the manufacturer;
(g) the place and date of issue of the statement of compliance.

Per section 10 of the Rules, responsible entities, manufacturers and suppliers, must retain the statements of compliance of products in scope under this security standard for a minimum of 10 years.

Notification of recall

Section 20 of the Cyber Security Act establishes that if a manufacturer fails to comply with a recall notice per section 19 of the Cyber Security Act, the Minister may publish a notification that the relevant entity has failed to comply with the notice on a public website.

Per section 11 (b) of the Rules, the public notice will outline actions that a consumer may wish to take If a consumer has already purchased a recalled product. This can include, for example, consider destroying that product or take extra precautions when using the product.

Schedule 1 – Security standards consumer grade relevant connectable products

Passwords

As the initial application of the power, Schedule 1 details the technical security standards required for consumer-grade relevant connectable products. The rules explains any relevant technical definitions related to the security standards.

Under section 2 of Schedule 1, where the hardware or software of a product requires the use of a password, the security standard would require that this password must be:

- unique per product – meaning that universal default passwords (sometimes as simple as “admin” or “default”) that are applied consistently across all units of a product must not be used; or
- defined (or, set) by the user of the product.

Under subsection 3, the Schedule prescribes additional requirements on passwords that are unique per product. These requirements prevent the password from being otherwise easily guessable by someone other than the user of the product. The security standard prohibits passwords, which are unique per product, from being:

- based on incremental counters;
- based on or derived from publicly available information;
- based on or derived from unique product identifiers, such as serial numbers, unless this is done using an encryption method, or keyed hashing algorithm, that is accepted as part of good industry practice; or
- otherwise guessable in a manner unacceptable as part of good industry practice.

Information on how to report security issues must be published

Under section 3, the Schedule prescribes requirements surrounding security issue disclosure mechanisms for the hardware or software of consumer-grade relevant connectable products. Manufacturers are required to publish information regarding these requirements, including:

- at least one point-of-contact to allow a person to report security issues related to the hardware or software of the product to the manufacturer; and
- details of when a person who makes a security issue report will receive an acknowledgement of receipt of the report and status updates regarding the report until the resolution of the reported security issue.

Importantly, the security standard places clear requirements on the way this information must be published to ensure that it is accessible, clear and transparent, and in English. Additionally, the information must be made available without request, free of charge, and without seeking or collecting personal information about the person making the report.

Information on defined support period for security updates must be published

Under section 4, the Schedule prescribes the requirement for manufacturers of consumer-grade relevant connectable products to define and publish a support period for security updates for their products. A security update is the elements of a software update that protect or enhance the security of a product, including addressing security issues that have been discovered by or reported to the manufacturer. Notably, any software update may be entirely, partially, or in no part a security update.

To meet this requirement, a manufacturer is required to first define a support period (with an end date) for which security updates for the product will be provided by, or on behalf of, the manufacturer. This defined support period will then be required to be published in a manner such that it is:

- accessible;
- clear and transparent;
- in English;
- understandable by a reader without prior technical knowledge; and
- made available without request, free of charge, and without seeking or collecting personal information about the reader.

Subsection 4(7) provides additional requirements surrounding the publishing of the defined support period where a manufacturer offers to supply the product on their website, or another 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.

Where any information is published on the website that is intended to inform consumers' decisions to acquire the product, the manufacturer must ensure the defined support period is prominently published with this information. Additionally, in each instance on the website that the main characteristics of the product are published, the manufacturer must ensure the defined support period is published alongside or otherwise given equal prominence to these main characteristics.

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.

Importantly, a person should not be required to unnecessarily navigate within such 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 such a website if information intended to inform consumers' decisions 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 consumers' decisions to acquire the product.

The following is a non-exhaustive list of potential locations on a manufacturer's website (or other website under their control) where information would or would not be considered to be intended to inform consumers' decisions to acquire a product, or may be considered to be the publication of the main characteristic of the product:

Likely intended to inform consumers' decisions to acquire a product, or likely the publication of the main characteristics of 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.

Likely not intended to inform consumers' decisions to acquire a product, or not likely the publication of the main characteristics of the product:

- generic product press releases;
- support articles; and
- information for accessories of the product (for example, the purchase webpage for a smartphone case) – although, if the accessory is itself a consumer-grade smart device, its own defined support period may need to be published as stipulated by this subsection.

The defined support period must not be shortened after it is published by the manufacturer. However, the period would be able to be extended. If extended, the new defined support period is required to be published by, or on behalf of, the manufacturer as soon as practicable in a manner consistent with the publishing of the original defined support period.

Attachment A – Mandatory security standards and industry-led voluntary cyber security labelling scheme for consumer-grade smart devices

Impact Analysis Addendum (OIA23-05842; legacy: 23882)

Part 1: Context and background

Strategic context

The *2023–2030 Australian Cyber Security Strategy* (the Strategy) and associated *2023-2030 Australian Cyber Security Action Plan* (the Action Plan) outlines the pathway to Australia becoming a world leader in cyber security by 2030. As part of the Strategy, the Australian Government announced that it would co-design options to legislate a mandatory cyber security standard for smart devices and develop a voluntary labelling scheme for consumer-grade smart devices.

On 22 November 2023, the Department of Home Affairs published an Impact Analysis on mandatory security standards and industry-led voluntary cyber security labelling scheme for consumer-grade smart devices.

Consultation

An evaluation of the domestic Code of Practice in March 2021 suggested that voluntary, principles-based guidance had a limited impact on business decision-making, with evidence suggesting that low-cost manufacturers were least likely to make more security-conscious design choices

During consultation in 2021, the Australian Government heard feedback from consumer advocate groups and manufacturers suggesting a possible market failure in the smart device market. Feedback strongly suggested that it is reasonable to expect smart device manufacturers to incorporate basic security features into their products given their capability and understanding of the manufacturing process. However, the Australian Government also heard that manufacturers are not sufficiently incentivised to build secure-by-design products. Manufacturers who prioritise cost and time to market over cyber security can attract higher demand as consumers are typically price-sensitive and generally lack the expertise to distinguish products based on security features.

The Australian Government has heard that any regulation on smart devices should only be used as a last resort and must demonstrate a net benefit to society. However, the majority of stakeholders across the nation were supportive of introducing a mandatory standard for smart devices in Australia. There was strong support for Australia adopting international standards because we are a small technology market. Industry stakeholders told us that aligning with international standards would help reduce regulatory burden and lower barriers to entry in the Australian market. There were also views that regulation would need to be future-proofed to adapt to changes in the threat environment and would need to be accompanied by strong enforcement to ensure compliance by industry.

The *Cyber Security Strategy Discussion Paper* sought industry and community views on the adoption of a mandatory product standard for consumer-grade smart devices in Australia. Submissions supported a long-term vision for the Australian cyber security landscape where digital goods and services sold are secure-by-design. Many submissions noted that small businesses and vulnerable communities would be the primary beneficiaries of regulation requiring stronger security standards. By allocating more cyber security risk to manufacturers and other entities better placed to mitigate those risks, we can create a safer digital economy.

The objective of Australia's cyber security standard for consumer-grade smart devices would be to align with international benchmarks, ensure consistency between jurisdictions and minimise regulatory burden on Australian businesses, while also meeting our national security objectives.

Part 2: Additional consultation and impacts on legislative design

The *Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper* (the Consultation Paper) sought additional views from the public and industry on how a mandatory cyber security standard for consumer-grade smart devices could address gaps in Australia's current cyber security

legislative landscape by incorporating basic security features by design and preventing cyber attacks on Australian consumers. The Consultation Paper posed tailored questions to the public and industry on discrete areas of the policy design to refine the agreed conceptual option – as described in the original Impact Analysis – into a pragmatic, co-designed solution to uplift the cyber security of Australians and their technologies.

Responsible entities

The Consultation Paper noted many entities contribute to the supply chain that provides Australian consumers with access to smart devices, including manufacturers, subcontractors, software developers, importers and distributors. The Department of Home Affairs (the Department) sought views on which entities should be covered within the scope of a mandatory security standard.

The majority of stakeholders provided feedback that manufacturers and suppliers of smart devices should be held responsible for compliance with the standard.[1] This would be consistent with the proposed product standard compliance requirements. Some stakeholders suggested that all entities in the supply chain should be held responsible.[2]

The original Impact Analysis assessed that providing a mandatory standard for smart devices would place responsibility for ensuring that products meet baseline cyber security requirements on manufacturers and developers. Under this approach, negative externalities in the smart device market would be mitigated as consumers will be less likely to unknowingly purchase and bear responsibility for the consequences of an insecure smart device. Economic, social and community impacts under these assumptions have been adequately assessed.

In response to the additional feedback received, the mandatory standard will mirror the approach taken for consumer product safety – which places responsibilities of varying levels on vendors, suppliers, importers and manufacturers to comply with standard. This would align with approach taken in the UK's *Product Security and Telecommunications Infrastructure Act 2022* (UK PSTI Act) and associated regulatory regime.

Standards to be adopted in Australia

The Consultation Paper noted adopting the European Telecommunications Standards Institute (ETSI) EN 303 645 standard would bring Australia in line with our international partners, noting recent developments in smart device standards across other jurisdictions. The Department sought views on whether the first three principles of the ETSI EN 303 645 standard would be an appropriate minimum standard to mandate for cyber security of smart devices in the Australian market.

The majority of stakeholders supported mandating the first three principles of the ETSI EN 303 645 standard as a baseline in Australia.[3] This aligns with international approaches and introduces a level of security across smart devices in Australia while limiting negative consequences on market availability, innovation, and competition.

Some stakeholders suggested that higher-risk products should adhere to a higher standard.[4] Some stakeholders suggested a higher standard than the first three principles of the ETSI standard be mandated in Australia, such as the first six principles[5] or the whole ETSI standard.[6] Alternatively, a phased implementation of the whole ETSI standard could be considered.[7]

It was also suggested that the Australian Government consider mutual recognition with comparative standards in international jurisdictions.[8]

A small number of stakeholders did not support mandating the first three principles, as they provided insufficient consumer protection, and noted other standards be considered instead.[9] These alternate

---

[1] For example: CI-ISAC; Origin Energy; Fortinet Australia; Information Technology Industry Council.
[2] Tasmanian Department of Premier and Cabinet; Australian Information Security Association (AISA); KordaMentha; IoT Alliance Australia (IoTAA); Tech Council of Australia.
[3] For example: Fortinet Australia; Standards Australia; BSA Software Alliance; IoTAA.
[4] Australasian Higher Education Cybersecurity Service (AHECS); NSW Government; Australian Digital Health Agency; Therapeutic Goods Administration.
[5] Tasmanian Department of Premier and Cabinet.
[6] Black Ink Legal.
[7] NCC Group; CHOICE.
[8] Splunk.
[9] SA Government; Black Ink Legal; VeroGuard Systems.

standards included the International Standards Organisation (ISO)/International Electrotechnical Commission (IEC)[10] and the National Institute of Standards and Technology (NIST).[11]

The original Impact Analysis assessed that, to ensure international consistency and adoption of best practice, Australia should consider adopting part or all of the ETSI EN 303 645. Modelling conducted by the UK found the probability of attacks on smart devices could be reduced by between 20 and 70 per cent through a standard consisting of the first three principles of ETSI EN 303 645. This modelling aligns with technical advice from the Australian Signals Directorate's Australian Cyber Security Centre that the first three principles of the ETSI standard are the highest priority technical controls. Economic, social and community impacts under these assumptions have been adequately assessed.

In response to the additional feedback received, similar to the UK, Australia will only mandate the first three principles of the ETSI standard. As a small market, Australia benefits from aligning to international best practice, where relevant. Mandating more of the ETSI standard or the whole standard risks Australia being out of step with other markets, thereby disincentivising technology manufacturers from supplying to the Australian market and limiting consumer choice. Additionally, Australia will adopt a mutual recognition scheme for smart devices that comply with other comparable standards.

To ensure the baseline requirements can remain agile and relevant in the ever-changing cyber security landscape, the standard will be stipulated in subordinate instruments to the primary legislation – in the form of rules. The use of rules will ensure that subordinate instruments can be drafted flexibly and made by a delegate, enabling timely amendments in future.

In addition to the technical elements of the standard (initially, the first three elements of the ETSI standard), the subordinate instruments will include the following:

- the scope of devices covered – which will require products to meet the definition of a *consumer good* and *relevant connectable products*; and
- potential penalties for non-compliance.

Smart devices to be regulated

The Consultation Paper noted the UK PSTI Act takes an exception-based approach to defining which smart devices are regulated – that is, broadly capturing products capable of connecting with the internet or a network, from which specific devices can be exempted by prescription in delegated legislation. The Department sought views on the types of devices that should meet a mandatory smart devices standard in the Australian context.

Most stakeholders agreed that the scope of the standard should apply to all smart devices in Australia, subject to exceptions. Feedback included that the definition of the scope of products should be flexible enough to apply to emerging technologies.[12] Stakeholders also suggested that all internet and network-connected devices should be in scope.[13] Some did not support an exception-based approach.[14]

Some stakeholders noted that smart devices that are currently subject to equivalent or higher security requirements should be excluded from this standard.[15]

Some stakeholders suggested that high-risk smart devices or devices that are used for high-risk purposes, should adhere to a stronger standard.[16] However, these devices, such as distributed energy resources, should not necessarily be exempt from the baseline standard.[17]

Some stakeholders suggested that low-risk, low-value, and/or smart devices with a short lifespan could be excluded from the standard as some devices are so non-complex that they may be unable to comply, such as smart plugs and light bulbs.[18]

---

[10] AISA; Australian Information Industry Association (AIIA); the CISO Tribe; VeroGuard Systems.
[11] AISA; DP World; NBN Co.
[12] CYAINSE; CI-ISAC; NSW Government.
[13] Infoblox; Allied Assurance.
[14] NBN Co; SA Government; Security Mark.
[15] Transurban; IoTAA; SA Government; Black Ink Legal.
[16] AHECS; NSW Government; Australian Digital Health Agency; Therapeutic Goods Administration.
[17] Ausgrid; AEMO; EnergyAustralia.
[18] CYAINSE; The Cybersecurity Coalition; AWS; KordaMentha; Communications Alliance.

There was mixed feedback about the inclusion of smart phones, as some stakeholders suggested they should be included,[19] while others noted they are already built to high security standards.[20]

There was mixed feedback on whether industrial, enterprise and/or operational devices should be included. Some noted they should be included,[21] while others said they should be held to a higher standard.[22]

The original Impact Analysis did not look to the scope of devices covered by the standard. However, there was strong support from industry that any standard adopted by Australia should be internationally aligned. Assessment of economic, social and community impacts were prepared in a device-agnostic manner and noted that regulatory costs would be reduce through alignment with international approaches. This analysis of impact remains valid in the context of the additional consultation received.

In response to the additional feedback received, the standard will use a constructed definition of *consumer good* and *relevant connectable products* to determine the scope of the smart devices that will be regulated, providing exclusions as required.

Introduction timeframes

The Consultation Paper noted manufacturers and vendors will require time to adjust to new security requirements for smart devices, as several business processes and practices may need to shift to meet new standards. Conversely, however, the Consultation Paper raised that consumers will continue to face risks as more products are developed and sold prior to commencement of the standard. The Department sought views on an appropriate time period to enable industry to adjust to any new requirements.

Most stakeholders agreed a 12-month implementation timeframe would be sufficient for responsible entities to comply with a new standard.[23] Other suggestions included:

The original Impact Analysis did not look to the specific time implementation period of the standard. However, the assessment of economic, social and community impacts noted, as a mandatory requirement, a standard would have a relatively rapid impact on the market, accounting for the time needed to pass legislation and an appropriate phased introduction for manufacturers and retailers. This analysis of impact remains valid in the context of the additional consultation received.

In response to the additional feedback received, the standard will feature at least a 12-month transition period, which is consistent with domestic precedence and international models.

Monitoring and enforcement

The Consultation Paper noted designing an appropriate regulatory model would be critical to achieving effective compliance with the mandatory standard. The Department sought views on appropriate remediation mechanisms and proportionate penalties for non-compliance.

Only some stakeholders commented on this aspect of the Consultation Paper. Some agreed that the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) would be a suitable framework to monitor compliance and enforcement of the standard.[24] Some called for clarity on how the Regulatory Powers Act would work.[25]

The original Impact Analysis assessed that the use of an existing regulator would maximise regulatory efficiency for government by utilising existing organisational and administrative processes. Economic, social and community impacts under these assumptions have been adequately assessed. Government may choose to establish a new regulatory body that requires additional funding over and above the economic cost modelled in the original Impact Analysis. Careful consideration should be taken and provided as advice in this scenario to ensure the outcomes of the multi-criteria analysis remain valid.

In response to the additional feedback received, the Regulatory Powers Act would provide a suitable monitoring and enforcement framework for the standard. Further engagement is underway across

[19] Tasmanian Department of Premier and Cabinet; Quokka; EnergyAustralia.
[20] NCC Group; Information Technology Industry Council; AIIA; Communications Alliance.
[21] NCC Group; Water Services Sector Group.
[22] Fortinet Australia; Information Technology Industry Council; Ausgrid.
[23] For example: IoTAA; CHOICE; Australian Digital Health Agency; Digital Industry Group Inc (DIGI).
[24] CI-ISAC; NCC Group; Australian Information Security Association.
[25] IoTAA; CHOICE.

Commonwealth entities to determine the most appropriate agency or regulatory models to enforce this standard.

Part 3: Application of security standards to consumer energy resources

The original Impact Analysis considered the costs and benefits of regulatory options for minimum cyber security standards for consumer-grade smart devices and to inform consumers about the cyber security of their devices through a labelling scheme. However, the original Impact Analysis was prepared on the basis that consumer energy resources (CER), particularly rooftop solar photovoltaic (PV) systems and small-scale batteries would be out-of-scope of the proposed regime, given other work underway on CER cyber security.

Due to additional engagement across government and industry on the roadmap for CER cyber security, the Australian Government now proposes to include CER within the initial security standard for consumer-grade smart devices, as an important first step to uplift the security of these devices. This part considers the costs and benefits of this proposal.

Role of consumer energy resources

CER allow customers to have control over how electricity is produced and consumed at their premises. There is a large ecosystem of CER, including smart thermostats, home energy management systems, controllable appliances like air conditioners and pool pumps, and rooftop PV and batteries.

Governments expect that CER will play a large role in Australia's energy transformation. Consumer investments in their own energy resources help avoid the need for investments in grid-scale generation and electricity networks. The Energy Climate and Ministerial Council has set out its ambitions for CER in Australia's energy future through the National CER Roadmap.

CER are already large and important resources in Australia's electricity systems. There are around four million small-scale solar photovoltaic systems installed in Australia.[26] In the National Electricity Market, which spans the east of Australia, rooftop solar alone contributed more electricity to the grid in the first quarter of 2024 (13 per cent) than grid-scale solar, wind, hydroelectric generation or gas.[27]

CER are increasingly being connected to the internet. Inverters for small-scale rooftop solar are leveraging internet technologies to provide benefits to consumers, including remote monitoring and maintenance, and customer engagement through apps. An estimated 35 per cent of the CER fleet will be internet-connected by 2027.[28]

The prevalence of CER is expected to continue to grow into the future, forecast to increase five times to 2050.[29] Under the most likely scenario considered in the Australian Energy Market Operator (AEMO)'s 2024 Integrated System Plan (ISP), 79 per cent of detached homes in the NEM will have rooftop solar by 2050, up from 30 per cent today. This is in addition to battery storage and complementary technologies that are likely to come online over the same timeframe.

Benefit of uplifting cyber security

The cyber security threat environment for CER is similar that described in the original impact analysis. A large number of internet-connected devices creates a large attack surface for malicious actors, ranging from amateurs with different levels of capability to cyber criminals and nation-state actors.

Products and services without built-in security can present vulnerabilities that malicious actors can easily exploit, potentially undermining public trust in innovative technology. Many digital products do not have security standards built in by design or turned on by default. As a result, consumers and businesses can be offered less secure products and services, with insufficient expertise to manage the risk.

The cost of cyber incidents to the economy is significant. It includes ransom payments, lost revenue from business interruption, business recovery costs, lost shareholder value, reputational damage, and costs to the taxpayer from any government support. Beyond the direct economic costs, there are a range of social and psychological impacts that are difficult to quantify.

---

[26] Small-scale installation postcode data | Clean Energy Regulator (cer.gov.au)
[27] AEMO p.7
[28] AEMO, 2024 General Power System Risk Review – Report July 2024, p.119
[29] AEMO p.49

CER presents an additional risk because it is increasingly part of the interconnected energy system. Malicious actions against individual CER systems may impact how those systems operate for individual consumers. For example, if a system is not operating as expected, it may affect electricity supply to a premises and result in financial losses to a consumer from needing to buy electricity from the grid. Malicious actions against large numbers of CER systems have the potential to cause grid instability in local networks or in the wider electricity system.

Stakeholders have noted cyber security concerns with CER. For example, the Cyber Security Cooperative Research Centre has identified the increasing risk of hacking, malware, manipulation and disruption related to internet-connected solar inverters.[30]

The benefit of uplifting cyber security for CER is similar to those considered in the original impact analysis. That is, secure CER devices are key to protecting the security, privacy and safety of individuals and to ensuring a prosperous and secure digital economy. Security uplift in this space also helps prevent compromises of the larger networks that devices are connected to, which could impact energy security and national security.

Proposed change and consultation

Products addressed by this part are those covered by the AS/NZ 4777 *Grid connection of energy systems via inverters* family of standards. Other products like smart thermostats, load control appliances and home energy management systems were expected to be covered under the scope of the original Impact Analysis.

The proposal for mandatory minimum standards, supported by a voluntary labelling scheme, aligns with stakeholder feedback about the need for cyber security uplift for CER. In April 2023, the Department of Climate Change, Energy, the Environment and Water (DCCEEW) commissioned Standards Australia to investigate:

- existing standards for CER cybersecurity.
- international standards that could be adopted or modified for the Australia context.
- Australian-specific standards which may need to be developed to address any gaps.

Standards Australia worked with stakeholders to conduct a gap analysis and standards road-mapping process. A CER Cybersecurity Advisory Group (CERCAG) was established to provide expert input, comprising energy industry representatives, energy market bodies, academia and government.

The group considered that there is a need for standardisation to uplift CER cyber security in Australia. The group recommended that certain standards could be adopted or modified for use in Australia, and that technical specifications should be developed to provide targeted guidance for the Australian CER market.

Analysis of impacts

This addendum impact analysis anticipates that the implementation of the Bill with respect to CER will have an impact consistent with the findings of the Department of Home Affairs' original impact analysis.

The original impact analysis found a combination of mandatory standards and a voluntary labelling scheme yielded the highest benefit. [31] The analysis considered the expected impact on cyber security, regulatory cost to industry, regulatory cost to government, flexibility and responsiveness, and potential for unintended consequences.

The option of combined minimum standards and a voluntary labelling scheme is likely to be equally effective in the context of CER.

Impact category	Expected impact
Cyber security impact	The Department of Climate Change, Energy, the Environment and Water (DCCEEW) conducted desktop research into the cyber security practices of major CER suppliers into Australia. The purpose was to understand compliance levels of Original Equipment Manufacturers (OEMs) with the top three best practice principles of the European Telecommunications Standards Institute (ETSI)

[30] Power Out p.6
[31] The option of 'mandatory standard' alone also achieved the same overall rating score.

	standard EN 303 645, and identify whether OEMs supplied international markets subject to similar regulations. DCCEEW selected ten OEMs that supply batteries into Australia. DCCEEW reviewed their websites and product documentation to determine: ▪ whether they used universal or default passwords ▪ whether they had implemented a mechanism to manage reports of vulnerabilities ▪ whether they kept their software updated. DCCEEW found that: ▪ 50 per cent of the OEMS did appear to describe the use of default or universal passwords in product documentation related to devices, apps, menus or other features ▪ 60 per cent of the OEMS did implement some form of vulnerability management reporting and/or policy on their website ▪ 70 per cent of the OEMS indicated they kept their software updated. From these OEMS, DCCEEW selected five OEMs that also supplied rooftop solar inverters into Australia. DCCEEW applied the same methodology and found similar results: 50 per cent did appear to describe the use of default or universal passwords in product documentation related to devices, apps, menus or other features, 80 per cent did implement some form of vulnerability management reporting and/or policy on their website, and 80 per cent indicated they kept their software updated. From this, smart CER devices appear to have similar vulnerabilities and mitigation strategies as other consumer-grade smart devices. Compromises to these devices would have similar impacts to those considered in the original impact analysis, relating to the security, privacy and safety of individuals and the larger networks to which devices are connected. In addition, compromises to these devices have the potential to cause inconvenience, lost energy supply and financial harm to customers where devices don't operate as intended. The option of combined minimum standards and a voluntary labelling scheme is likely to be equally effective for uplifting cyber security in the context of CER as for other consumer-grade smart devices. Suppliers will need to consider their cyber security posture and adapt their products and businesses practices, if needed, to meet the minimum requirements.
Regulatory costs to industry	DCCEEW considered the regulatory cost to industry of implementing the proposed minimum cyber security requirements. DCCEEW applied the same methodology[32] as the original impact analysis, with desktop research to confirm data inputs. DCCEEW found that: ▪ the anticipated industry turnover for rooftop solar inverters and batteries over the next 10 years is around $43.3 billion ▪ the total cost of compliance with the security standards over 10 years is around $51.7 million

[32] This addendum adopts the same costs of implementation used by the Department of Home Affairs in the original impact analysis. The addendum anticipates that the changes that need to be implemented by CER OEMs to comply with the standard will be similar to those required for other smart devices – for example, updating product and marketing material; updating business practices; implementing password management and vulnerability reporting mechanisms; and providing consumer advice. The addendum anticipates that costs for CER OEMS to implement these changes will be similar to those for other businesses supplying smart devices.

	▪ the total cost of compliance of as a percentage of market turnover over the 10 years is around 0.12 per cent. This is consistent with the share of compliance costs to turnover found in the original impact analysis (0.17 per cent). DCCEEW considered whether smart CER suppliers in Australia also sell into markets with similar regulatory requirements for smart-device cyber security, particularly the United Kingdom (UK). The UK's Product Security and Telecommunications Infrastructure Act 2022 creates similar minimum cyber security requirements for consumer-grade smart devices as those proposed under Australia's Cyber Security Bill 2024. DCCEEW found that all the OEMs examined also supplied products to the UK. Minimum cyber security requirements for CER in Australia are expected to create marginal additional costs for suppliers into Australia, since they should already be implemented, or in the process of being implemented, for other markets. As in the original impact analysis' findings on a voluntary labelling scheme, businesses would only label their smart products if the benefits outweighed the costs.
Regulatory costs to government	The government has already committed to pursuing a combined mandatory standard and voluntary labelling approach for other smart consumer devices. This decision already involves setting up a regulatory and legal apparatus to implement this approach. Extending this approach to CER creates a marginal additional regulatory cost to government.
Flexibility and responsiveness	The same flexibility and responsiveness considered in the original RIS can be expected. The mandatory standards can be adapted if needed to respond to changes to technology or the threat environment. The proposed labelling scheme is voluntary, allowing flexibility for suppliers.
Potential unintended consequences	The original impact analysis considered the potential for unintended consequences of a voluntary labelling scheme. This impact analysis anticipates that the potential for unintended consequences with respect to CER is similar, that is: ▪ ongoing education would be required to ensure effectiveness ▪ businesses would only choose to participate if the benefits outweighed the costs ▪ the Australian Consumer Law would deter manufacturers from making misleading or deceptive claims.

The impact of expanding the scope of consumer-grade smart devices subject to minimum cyber security standards to include CER is consistent with the initial regulation impact assessment prepared for the *Cyber Security Act 2024*. While there is a minor financial impact to be borne by the CER sector, this impact is offset by the significant benefit to consumers and the energy system from increased cyber security protections for this equipment.

Part 4: Conclusion

Conclusion

The additional legislative design and expansion to include CER does not impact the policy position or materially change the impact to industry from the original proposal.

The Australian Government's commitment co-design a voluntary labelling scheme to measure the cyber security of smart devices has not changed. This addendum does not supplement or further contextualise any of the content that was published in the original Impact Analysis regarding this measure.

/