

Simplify your
energy transition



14 February 2025

Australian Government
Department of Home Affairs
cisgcomms@homeaffairs.gov.au

To whom it may concern

Consultation on Subordinate Legislation to the Cyber Security Act and Security of Critical Infrastructure Act 2018 (SOCI Act).

Thank you for the opportunity to respond to the Cyber Security (Security Standards for Smart Devices) Rules 2024 (**draft Rules**).

Intellihub is a digital energy management specialist, providing smart metering devices and services to over 50 energy retailers across Australia and New Zealand. We specialise in providing an ecosystem of products, services, and technologies to deliver asset management, installation, financing, and operations for more than 2.5 million smart meters. Beyond smart meters, our services touch everything from solar to water, virtual power plants to electric vehicle charging. We are proud to be part of Australia's journey towards a more sustainable and efficient way of using energy and other utilities.

Like the Australian Government, we recognise that Australian consumers need confidence in the security of 'smart devices' in their homes. Further, and in our role as an enabler of the future of sustainable energy in Australia, we are also invested in Australia's transition to a net zero economy, and the need to continue to attract investment to aid that transition, for Australia to become a leader in renewable energy, to add value to natural resources, and strengthen Australia's economic security. With this background, and also acknowledging that regulatory certainty is a critical prerequisite for business confidence and investment (especially in the sectors in which we operate), we have set out our comments below.

The Fact Sheet – Security standards for smart devices (fact sheet) describes the draft rules as “being aligned with existing international approaches”, and in particular that these follow closely the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023 (UK) (**UK regulations**) made under the Product Safety and Telecommunications Act 2022 (UK). However, and in contrast with the UK regulations, we note that the draft Rules appear not to have not excluded two classes of relevant connectable devices in the same way in which they are excluded under the equivalent UK regulations:

- Gas and electricity smart meters (to which we would add water smart meters)
- Electric vehicle smart charging points.

The rationale for the proposed difference in approach in Australia (as compared to the UK) – if indeed a difference in approach is intended – is presently not clear to us.

We accept that there could be a view, particularly in the case of smart meters for gas, electricity and water utilities, that an exemption for smart meters is not required on the basis that these items may be considered to be outside the scope of the draft Rules. This would be on the basis that such items are not smart devices that could reasonably be expected to be “acquired in Australia by a consumer”. In other words, and in the Australian context, they are acquired as a wholesale product by energy retailers as part of a bundled service which allows such retailers to bill consumers for their electricity consumption. The challenge is that this conclusion results from an interpretation of the draft Rules on which there may be ambiguity, where there should be certainty.

The fact sheet advises that the “The consumer-grade smart device standard is expected to cover smart devices that



consumers use every day, such as smart TVs, smart watches, home assistants, baby monitors, and **consumer energy resources**.” [emphasis added] A definition for “consumer energy resources” has not been provided.

The Cyber Security Legislative Reforms – Explanatory Document: Cyber Security (Security Standards for Smart Devices) Rules (**explanatory document**) specifically includes a *Part 3: Application of security standards to consumer energy resources*, explaining that the Australian Government now proposes to include consumer energy resources (**CER**) within the initial security standard for consumer-grade smart devices, as an important first step to uplifting the security of these devices given the potential impact malicious activity involving these devices could have on energy supply to Australian homes. The explanatory document refers to CER as including “particularly rooftop solar photovoltaic (PV) systems and small-scale batteries”, and also describes the range of CER in scope as including “those covered by the AS/NZ 4777 Grid connection of energy systems via inverters family of standards” as well as “other products like smart thermostats, load control appliances and home energy management systems”. However, these references are in the context of a discussion of broader regulatory impact, and not a clear position with respect to the application of the draft Rules.

Intellihub considers that the intent of the draft Rules and the regulatory position regarding Intellihub products (including, specifically, smart meters) is presently unclear. Guidance would, in Intellihub’s submission, better support the broader business and investment environment with respect to delivering on net zero expectations.

We are grateful to the Cyber and Infrastructure Security Centre (CISC) and the Department of Home Affairs for considering these issues and their impact on our industry. We look forward to receiving your guidance on the matters above in due course.

We would also be happy to provide further information should this be considered beneficial.

Yours sincerely,

Signed by:

513DQC1BQ984A41C...
Sara Abak

Chief Information Security Officer