SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

SMA Australia's Feedback on the Horizon 2 Policy Discussion Paper of the 2023-2030 Australian Cyber Security Strategy

Table of Contents

1. Introduction and scope of our submission
2. Who is SMA?
3. SMA's cyber security and privacy protection credentials
    3.1 Australian Energy Sector Cyber Security Framework
    3.2 ISO 27001
    3.3 EN 303 645
    3.4 IEC 62443
4. Challenges for cyber security in the renewable energy sector
    4.1 Understanding risk thresholds for inverter fleets in Australia's grids
    4.2 Issues arising from the location of servers
    4.3 Gaps in the policy and regulatory framework for cyber security
5. Summary of recommendations
6. Responses to questions raised in the policy discussion paper

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

1. Introduction and scope of our submission

SMA-Australia welcomes the opportunity to provide feedback to the Department of Home Affairs (DHA) Policy Discussion Paper on Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

SMA welcomes DHA's initiatives to improve Australia's cyber security posture. In our submission we focus on cyber security in the renewable energy sector. We believe there is scope for significant improvement in cyber security policy, regulation, verification of compliance, enforcement and awareness in Australia's renewable energy sector.

2. Who is SMA?

SMA is a leading global specialist in inverters for solar photovoltaic (PV) and battery energy storage systems (BESS). Our product range spans the residential rooftop sector, commercial and industrial (C&I) applications, and large grid-scale applications. Our inverter and battery storage products are complemented by components for energy management, system monitoring, and data analysis. SMA has a global inverter capacity of 144 gigawatts (GW) in more than 190 countries and more than 9 GW inverter capacity in Australia. Our annual production is about 40 GW. We are headquartered in Germany, with employees in 20 countries. We are one of the world's leading manufacturers of grid forming inverters.

SMA's multi-award-winning technology is protected by more than 1,600 patents and utility models. Since 2008, the Group's parent company, SMA Solar Technology Aktiengesellschaft (SMA AG), has been listed on the Prime Standard of the Frankfurt Stock Exchange (S92) and is listed in the Small-Cap-duetsche Aktienindex (SDAX index).

SMA Australia Pty Ltd (SMA AU) is a subsidiary of SMA AG and has been in operation since 2007. SMA AU as a supplier plays a key role in the development of Australian solar PV and battery storage projects and is actively supported by SMA AG who identify Australia as one of the top three global markets, along with the European Union (EU) and the United States of America (USA).

SMA is committed to cyber security. We play an active role in development and implementation of cyber security policies, regulations and standards in the EU and elsewhere.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

3. SMA's cyber security and privacy protection credentials

As an EU-headquartered company, SMA aspires to highest standards for cyber security and privacy of customers' personal data, including our customers' personal energy data. We meet and aim to exceed all cyber security and privacy standards in the countries in which we operate. Our subsidiary offices adhere to the standards of the EU General Data Protection Regulation (GDPR), unless local legislation requires us to do otherwise.

3.1 Australian Energy Sector Cyber Security Framework

In 2024 SMA Australia commissioned an independent cyber security consultant to:

- develop guidelines for the application of the Australian Energy Sector Cyber Security Framework (AESCSF) to inverter manufacturers, and
- apply the guidelines to assess the cyber security of SMA in its role of inverter manufacturer and supplier to the Australian market.

Our cyber security consultant developed guidelines for interpretation and application of the AESCSF maturity model which was shared with the Australian Energy Market Operator (AEMO) and other relevant regulators and policy makers.

Our consultant and the SMA AG cyber security team applied the guidelines to undertake a self-assessment against the domains applicable to SMA in its role as a power conversion equipment (PCE) and plant control product original equipment manufacturer (OEM). The assessment examined a total of 86 controls and anti-patterns for SP1 level assessment against the scopes which SMA performs, and the implicit or explicit risks they could expose to a site operator.

The result of the consultant's assessment in 2024 confirmed that SMA meets the Security Profile 1 (SP-1) level standards under the AESCSF across all applicable domains.

In 2025 AEMO opened its annual AESCSF assessment process and SMA was among the first inverter OEMs in Australia to participate in the assessment. The assessment process was managed by Deloitte and commissioned and overseen by AEMO.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

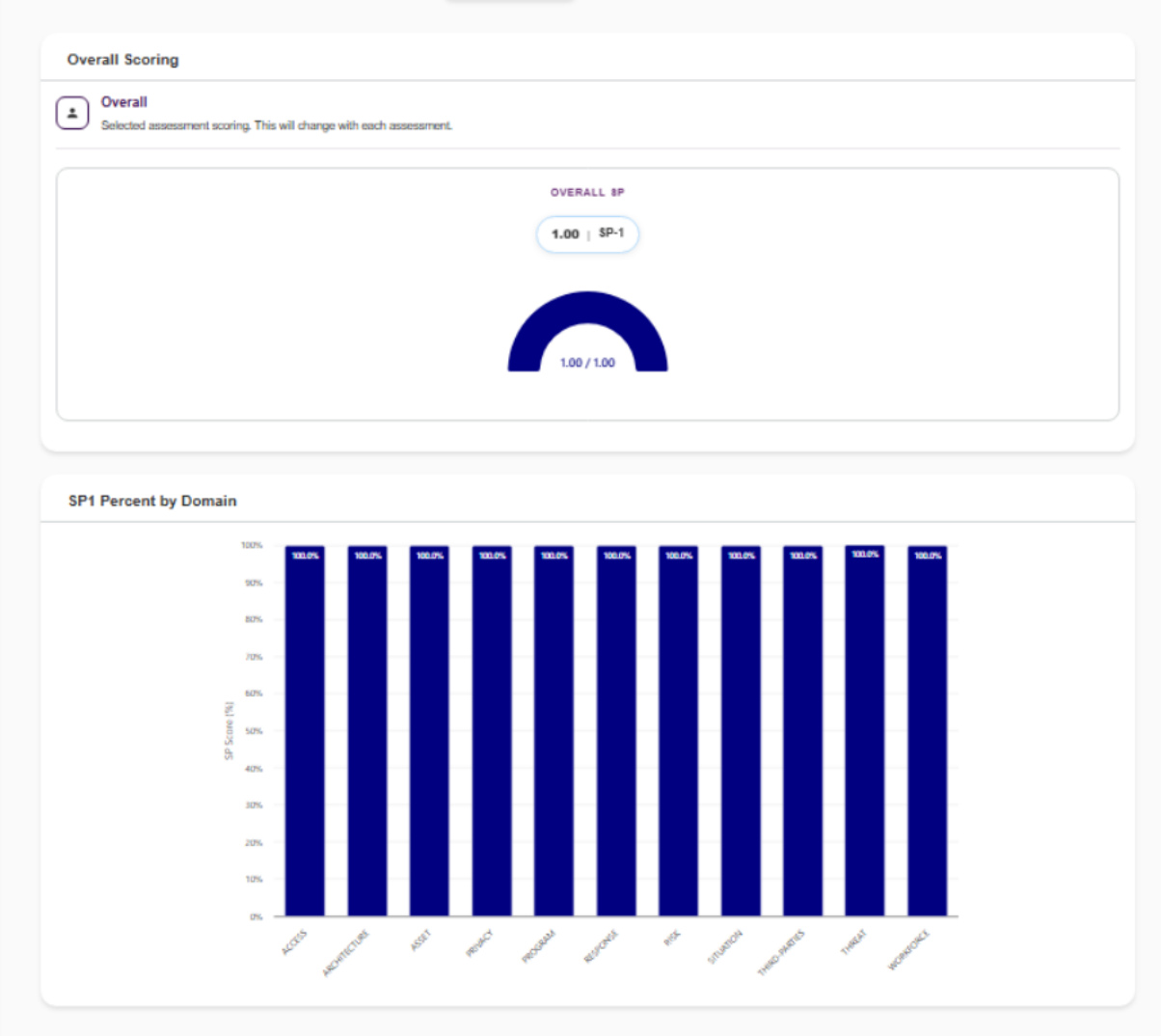

Figure 1: Deloitte / AEMO AESCSF assessment for SMA Australia large-scale division, 2025

In June 2025, Deloitte and AEMO assessment confirmed that SMA AU's large-scale division meets the SP-1 level standards under the AESCSF 'Lite' framework, achieving a rating of 100% across all applicable domains. Figure 1 (above) shows the dashboard summary of the Deloitte / AEMO assessment results for the SMA AU large-scale division.

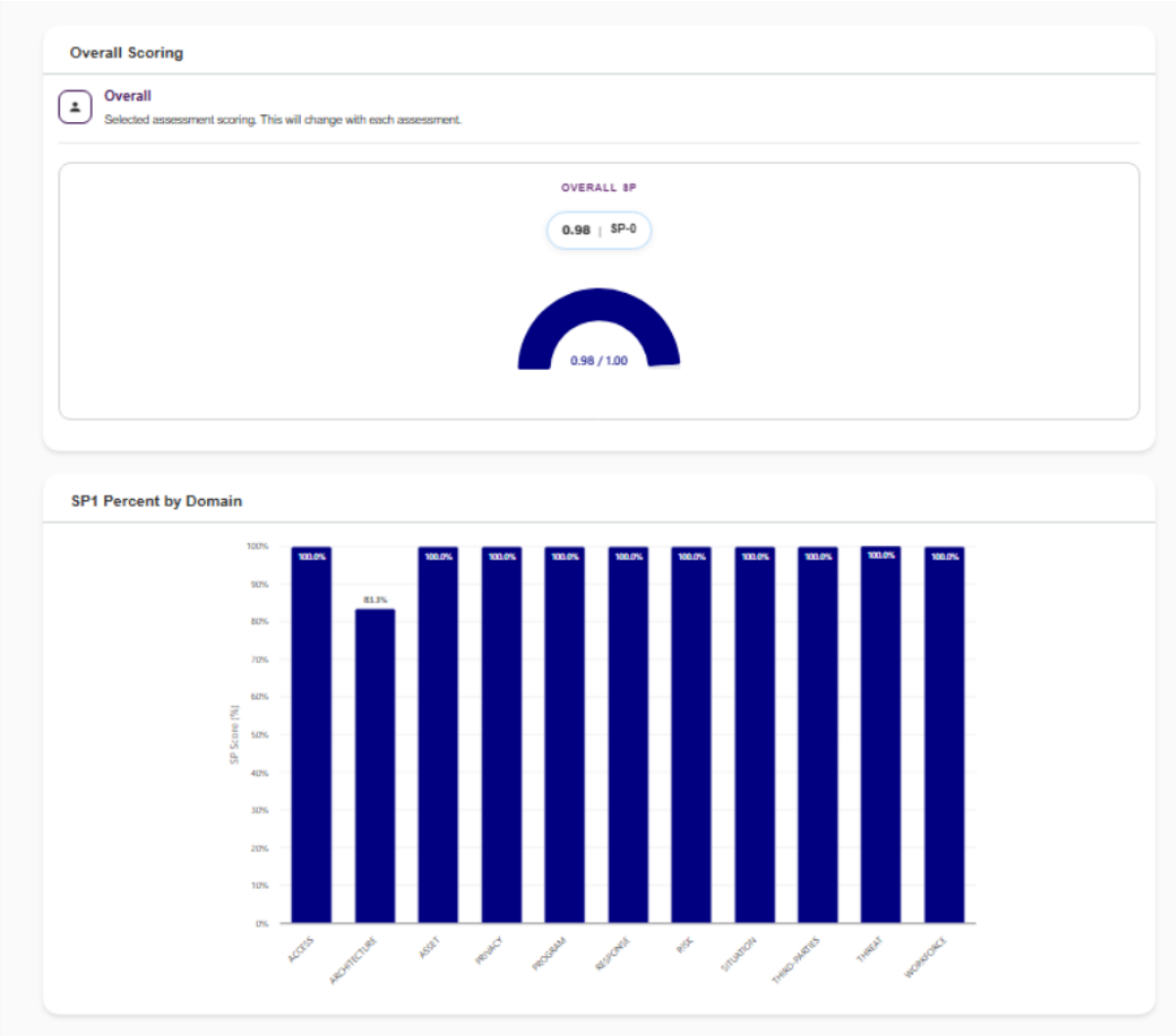

Figure 2: Deloitte / AEMO AESCSF assessment for SMA Australia home and business division, 2025

The Deloitte and AEMO AESCSF assessment confirmed that SMA AU's home and business division meets the SP-1 level standards under the AESCSF 'Lite' framework, achieving a rating of 98% across all applicable domains. Figure 2 (above) shows the dashboard summary of the Deloitte / AEMO assessment results for the SMA AU home and business division.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

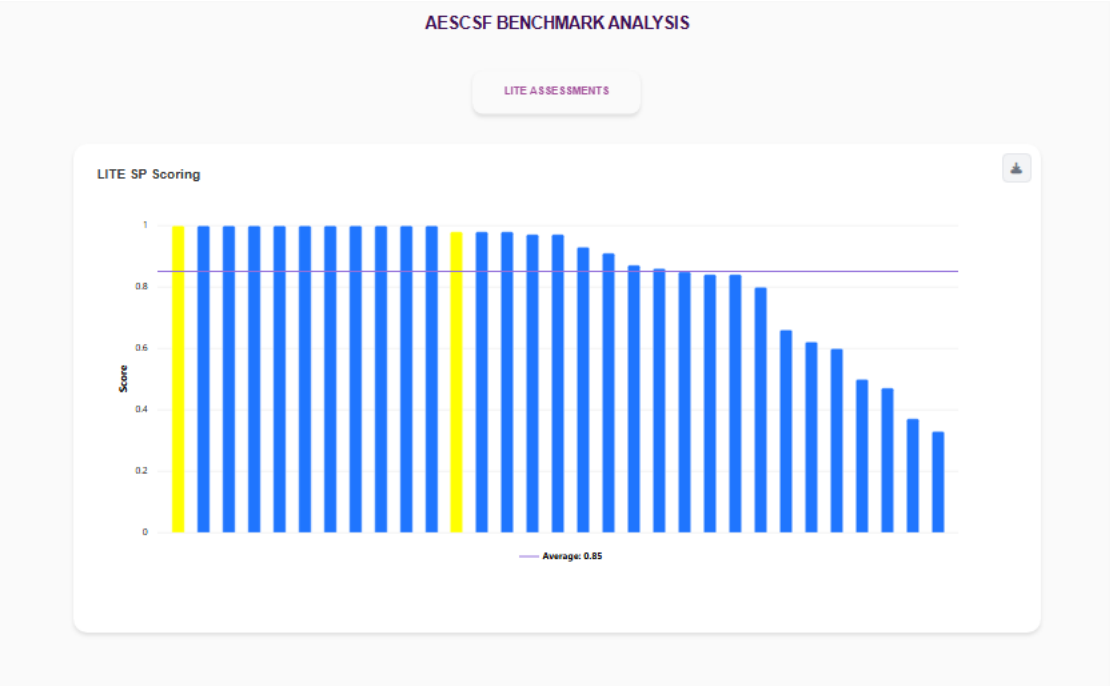

Figure 3 (above) shows the dashboard summary of the Deloitte / AEMO AESCSF benchmark analysis for SMA AU. The yellow bar on the left-hand side represents SMA AU's large-scale division and the yellow bar in the middle represents SMA AU's home and business division.

SMA AU is currently preparing for the next AEMO assessment, in which we will undertake assessment against the more stringent Security Profile 2 (SP-2) level of the AESCSF.

3.2 ISO 27001

ISO 27001 is the leading international standard dedicated to information security, setting the benchmark for organisations worldwide. The ISO 27001 framework outlines stringent requirements for establishing, implementing, operating, and continuously improving an Information Security Management System (ISMS). The ISMS's key objective is to ensure the confidentiality, integrity and availability of data and information is maintained. The three security objectives are:

- Confidentiality – ensuring information is accessible only to authorised individuals
- Integrity - protecting the accuracy and completeness of information and processing methods
- Availability – ensuring that authorised users have access to information and systems when needed

Since August 2024, the SMA Sunny Portal Information Security Management System has been certified as compliant to ISO 27001:2022. Every year, we undergo rigorous independent audits to verify that we continue to maintain the highest standards of cyber security to protect

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

our customers' data from cyber criminals. The 2024 certificate is available here - Microsoft Word - ebb_3830390_3671466989_1.docx (sma.de) We are awaiting receipt of the certificate for the 2025 audit.

3.3 EN 303 645

SMA's home and business range of inverters has been certified to EN 303 645 since 1 August 2025. EN 303 645 is the leading cyber security standard for consumer Internet of Things (IoT) devices. Certification to EN 303 645 demonstrates that we satisfy the Cyber Security Act's three Ministerial rules, which are provisions of EN 303 645.

3.4 IEC 62443

As an inverter OEM, SMA is regularly audited against (but not yet fully certified to) the applicable parts of IEC 62443, namely:

- IEC 62443-4-1 (requirements for the secure development processes of products),
- IEC 62443-4-2 (requirements for products), and
- parts of IEC 62443-3-x.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

4. Challenges for cyber security in the renewable energy sector

In Australia, there is significant room for improvement in the regulation of cyber security in the renewable energy sector. The major areas for improvement are:

- Understanding the risk thresholds for inverter fleets in the Australian context,
- Understanding and addressing the risks of remote control and monitoring by overseas servers,
- Ensuring that parts of the sector that are not covered by cyber security legislation or regulations are brought into the regulatory framework, and
- Ensuring that cyber security regulations, where they exist, are adequately enforced.

4.1 Understanding risk thresholds for inverter fleets in Australia's grids

A recent report[1] written by DNV and published by Solar Power Europe assessed the cyber security risk of solar and battery inverters in terms of:

- Device-level security for individual inverters,
- Portal security for aggregators, virtual power plants (VPPs) and OEM portals,
- Enterprise security, and
- Intentional misuse in cooperation with a nation-state.

Table 1 (below) summarises DNV's assessment of the gaps in regulation of cyber security in the EU electricity system.

Party	Residential, C&I	Utility scale
Inverter manufacturer	Yes. Little or no regulation	No access after commissioning
Plant owner	Limited end user functions	Yes and regulated
EPC (installer)	Limited to own installations	No access after commissioning
VPP, aggregator	Yes. Little or not regulation	Yes. Little or no regulation
Networks	Yes and regulated	Yes and regulated
O&M operator, asset manager	Limited to own installations	Yes, but limited by operator
Other third-party service	Yes. Little or no regulation	Generally no direct access

Table 1 – Assessment of cyber security risks and regulatory gaps in the EU, based on 2025 assessment by DNV

[1] DNV (2025), Solutions for PV Cyber Risks to Grid Stability, published by Solar Power Europe and available here

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

The report concluded that remote access and control by inverter OEMs and VPP operators remains a significant and largely unaddressed risk. The report found that the ability to remotely control more than 3 GW of inverters (in total) would be sufficient to cause a blackout in the EU. It estimated that there are twelve companies with a fleet of remotely controllable inverters with capacity exceeding 3 GW. It would be insightful to undertake a similar assessment in the context of Australia's grids.

Recommendation 1: Assess the capacity of the inverter fleet in the Australian grids that, if remotely operated by a malicious actor, could be used to cause a blackout.

Recommendation 2: Assess how many inverter OEMs already have an inverter fleet large enough to cause a blackout if they are operated by a malicious actor.

4.2 Issues arising from the location of servers

The location of computer servers that control and monitor Australia's fleet of inverter-based resources (IBRs) matters. When those computer servers are located overseas, they are more susceptible to interruption either by malicious actors or by unplanned disruptions. It is unclear whether the legislation of the overseas country in which the servers are located would take precedence over Australian legislation, if the two legislative frameworks were in conflict. In addition to national security and cyber security concerns, there are also privacy concerns when personal data is held overseas. It is unclear what protections are afforded to customers' personal data, including their personal energy data, when the data is stored and managed overseas.

Recommendation 3: Assess the risks of continuing to allow Australia's inverter fleet to be monitored and controlled by overseas servers.

Recommendation 4: Assess the costs and benefits of requiring use of onshore computer servers for the control and monitoring of Australia's inverter-based electricity generators.

Recommendation 5: Clarify whose legislation determines how customers' personal energy data can be used and passed on where the data is stored on servers in the People's Republic of China (PRC), the USA, the EU, and elsewhere.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

4.3 Gaps in the policy and regulatory framework for cyber security

In the context of Australia's regulatory frameworks for cyber security in the electricity sector, the areas for consideration can be categorised as follows:

- Large scale generators and batteries above 30 MW
- Large-scale – aggregated assets
- Medium scale generators and batteries, smaller than 30MW and larger than IoT devices
- VPPs, aggregators, and OEM portals for small-scale and C&I assets
- IoT devices, including internet-connected consumer and distributed energy resources (CER and DER)

Figure 5 (below) is a summary of SMA's assessment of gaps in the policy and regulatory framework for cyber security of renewable generators and batteries in Australia's electricity system.

Generator class	Policy gap?	Regulatory / enforcement gap?
Large-scale – single plant above 30 MW	No gap. Covered by the Security of Critical Infrastructure (SOCI) Act.	Enforcement depends on industry and is variable. Room for improvement.
Large-scale – aggregated assets	No policy or legislation	Unregulated
Medium-scale – C&I assets less than 30MW, larger than IoT	No policy or legislation	Unregulated
VPP, aggregator, OEM portal for small-scale and C&I assets	No policy or legislation	Unregulated
IoT devices	No gap. Covered by Cyber Security Act.	No framework for enforcement currently exists.

Figure 5 – Assessment of cyber security risks and regulatory gaps in Australia

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

Large scale generators and batteries above 30 MW

The SOCI Act requires cyber security assessment for generation and storage assets larger than 30 MW. SMA's experience is that sometimes generators or transmission network service providers (TNSPs) pass through cyber security requirements directly to inverter OEMs and sometimes the engineering, procurement and construction (EPC) contractor passes through the requirement to the inverter OEM. However, the extent to which the cyber security requirements are passed through the supply chain is variable. There is significant room for improvement in the approach to ensuring cyber security in generators' supply chains. One way to achieve this would be to amend the SOCI Act to place the cyber security obligation directly on the inverter OEM. Alternatively, a suitable organisation (such as AEMO), could request generators to demonstrate the steps they have taken to ensure the cyber security of their supply chain.

Recommendation 6: Consider amending the SOCI Act to capture the generators' supply chain directly, so that enforcement is not dependent on action by generators or TNSPs.

Recommendation 7: Alternatively, require generators and TNSPs to report on whether and how they are passing through their cyber obligations to their supply chain.

Large-scale – aggregated assets

Fleets of aggregated assets are not covered by the SOCI Act, even if the fleet capacity exceeds 30 MW. The consequences of a cyber security breach for a fleet of aggregated assets exceeding 30 MW are no less impactful than a cyber security breach of a single asset exceeding 30 MW. The risk of a cyber security breach for a fleet of aggregated assets is larger than the risk for a single asset due to the larger attack surface. The SOCI Act should be amended to address this loophole.

Recommendation 8: Amend the SOCI Act to clarify that the 30 MW threshold applies to fleets of aggregated resources that exceed 30 MW, even if no individual generator or battery in the fleet exceeds 30 MW.

Medium scale generators and batteries

The Cyber Security Act applies to IoT devices. There is no upper threshold specified in the Act. It seems reasonable to infer that it applies up to the system size where distribution network services providers (DNSPs) require use of supervisory control and data acquisition (SCADA) systems instead of reliance on the public internet. The threshold for SCADA in Australia varies by DNSP, from 200kW up to about 1.5 MW.

This means that there is no legislation and no cyber security policy governing medium-scale inverter-based generation and storage in the 200 kW to 30 MW size range. This is the system size that is most often used in C&I applications.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

This gap could be addressed by reducing the threshold in the SOCI Act below 30 MW. The new threshold should be determined by the point at which inverters are no longer controlled over the public internet and are required by DNSPs to use SCADA systems. The threshold under the SOCI Act could be reduced as low as 200 kW to ensure that there are no gaps in the coverage of cyber security legislation.

Recommendation 9: Reduce the threshold in the SOCI Act to below 30MW. The new threshold should be determined by the threshold above which generation and storage systems must use SCADA rather than relying on public internet.

VPPs, aggregators and OEM portals for small-scale assets

There are no cyber security requirements for VPPs or OEM portals. The Cyber Security Act applies product-level cyber security rules to small-scale, internet-connected assets but there are no obligations for the associated information security management system.

Recommendation 10: Mandate standards for VPPs and OEM portals. Consider ISO 27001 as a starting point.

Internet-connected CER

The Cyber Security Act states that after March 2026, manufacturers are expected to have a self-declared Statement of Compliance for products supplied to Australian consumers. However, there are no requirements on manufacturers to verify that they have a Statement of Compliance, and no one has responsibility under the Act for determining the validity of the self-declaration.

If the government is serious about the cyber security of IoT devices, it must move beyond encouraging voluntary self-declarations by manufacturers. An enforceable framework is required.

Experience has demonstrated that rebate eligibility requirements under the Small-scale Renewable Energy Scheme (SRES) are a highly effective means of enforcing CER product standards. The Clean Energy Council (CEC) product approval process has been very effective as a routine compliance mechanism. This approach should be adopted for the Ministerial Rules under the Cyber Security Act.

The Ministerial Rules under the Cyber Security Act encourage voluntary action to satisfy three provisions of the EN 303 645 standard. They are:

- No default passwords,
- A means to manage reports of vulnerabilities, and
- Provision of information regarding how long a device is likely to be supported.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

There are many other provisions of the EN 303 645 standard that should be mandated and enforced under the Cyber Security Act. They include provisions to:

- Securely store sensitive security parameters,
- Communicate securely,
- Minimise exposed attack surfaces,
- Ensure software integrity,
- Ensure that personal data is secure,
- Make systems resilient to outages,
- Examine system telemetry data,
- Make it easy for users to delete user data,
- Make installation and maintenance of devices easy, and
- Validate input data.

SMA's IoT product range has been independently certified to the entire EN 303 645 standard. To protect consumers' privacy and the cyber security of Australia's energy systems, all inverter OEMs supplying the Australian market should be required to satisfy all EN 303 645, not just three provisions of the standard.

Recommendation 11: Develop and implement a routine compliance mechanism for the product-level cyber security requirements of the Cyber Security Act, such as requiring them as an eligibility requirement for rebates under the SRES.

Recommendation 12: Consider strengthening the Cyber Security Act and broadening its requirements, so that inverter OEMs are required to demonstrate that their products have been independently certified to all EN 303 645 – not just three provisions of the standard.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

5. Summary of recommendations

Understanding risk thresholds for inverter fleets in Australia's grids

1: Assess the capacity of the inverter fleet in the Australian grids that, if remotely operated by a malicious actor, could be used to cause a blackout.

2: Assess how many inverter OEMs already have an inverter fleet large enough to cause a blackout if they are operated by a malicious actor.

Issues arising from the location of servers

3: Assess the risks of continuing to allow Australia's inverter fleet to be monitored and controlled by overseas servers.

4: Assess the costs and benefits of requiring use of onshore computer servers for the control and monitoring of Australia's inverter-based electricity generators.

5: Clarify whose legislation determines how customers' personal energy data can be used and passed on where the data is stored on servers in the PRC, the USA, the EU, and elsewhere.

Regulation of large scale (above 30 MW)

6: Consider amending the SOCI Act to capture the generators' supply chain directly, so that enforcement is not dependent on action by generators or TNSPs.

7: Alternatively, require generators and TNSPs to report on whether and how they are passing through their cyber obligations to their supply chain.

Large-scale – aggregated assets

8: Amend the SOCI Act to clarify that the 30 MW threshold applies to fleets of aggregated resources that exceed 30 MW, even if no individual generator or battery in the fleet exceeds 30 MW.

Medium scale generators and batteries

9: Reduce the threshold in the SOCI Act below 30MW. The new threshold should be determined by the threshold above which generation and storage systems must use SCADA rather than relying on public internet.

Aggregators, VPPs and OEM portals

10: Mandate standards for VPPs and OEM portals. Consider ISO 27001 as a starting point.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

Internet-connected CER

11: Develop and implement a routine compliance mechanism for the product-level cyber security requirements of the Cyber Security Act, such as requiring them as an eligibility requirement for rebates under the SRES.

12: Consider strengthening the Cyber Security Act and broadening its requirements, so that inverter OEMs are required to demonstrate that their products have been independently certified to all EN 303 645 – not just three provisions of the standard.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

6. Responses to Questions Raised in the Policy Discussion Paper

In this submission, we have not responded to every question raised in the Consultation Paper. We have limited our responses to our areas of expertise.

1. What trends or technology developments will shape the outlook over the next few years and what other strategic factors should the Government be exploring for cyber security under Horizon 2?

Over coming years and decades, Australia's energy systems will increasingly be dominated by electricity generation from renewable sources. There are many gaps in cyber security policy, regulation and enforcement in Australia's renewable energy sector. Now is an opportune time to begin addressing these gaps. The problem of poor cyber security in legacy electricity generation systems will become larger and more difficult to address the longer we wait to act.

Jurisdictional governments are currently implementing various versions of an Emergency Backstop Mechanism. The existence of the Emergency Backstop Mechanism will add to the cyber security risk and makes even more important and urgent the task of ensuring all inverter size classes, aggregators and OEM platforms are covered by legislation and that they rules under the legislation are effectively enforced.

2. Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

The regulatory framework for Australia's electricity system is complicated by complex governance and confusion over the division of Federal and state responsibilities. Fortunately, this does not yet appear to be the case in regulation of cyber security. To our knowledge, state and territory governments are standing aside and allowing the Australian government and national agencies such as AEMO to take responsibility for the cyber security of energy. This is a welcome development. We encourage DHA and other Australian government agencies to continue leading in this area and not to delegate its cyber security responsibilities to lower levels of government.

3. Does the high-level Model resonate, and do you have any suggestions for its refinement?

The Model is a useful starting point. It could be refined by addressing questions such as:

- Are there gaps in cyber security policies and legislation which leave unaddressed significant parts of the industry in question?
- Are there regulations or other mandatory requirements (such as standards) to put the policies and legislative provisions into effect?
- Is there a process for verifying whether regulations or other mandatory requirements have been adhered to?

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

- Is enforcement action taken if regulations and other mandatory requirements are not satisfied?
- Is the enforcement action effective?
- Is there transparent public reporting of the success of the regulator or other agency responsible for enforcement of regulations?
- Is the enforcement of regulations leading to the successful delivery of the desired high-level outcomes?

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

Yes. There should be publicly available information to enable consumers and businesses to know which companies and products are compliant with cyber security regulations. In the case of renewable energy, the public reporting could include:

- What are the cyber security regulations or other mandatory requirements (such as standards) that apply to residential, C&I and utility-scale electricity generation and storage?
- Which products and companies have demonstrated compliance with the cyber security requirements applicable to them?
- Which companies or products, if any, have had enforcement action taken against them?
- What options are available to consumers and businesses who own equipment that does not meet the applicable cyber security regulations?

This information should be published by an independent organisation. It should not be left to self-assessment and marketing by manufacturers.

5. What could the government do to better target and consolidate its cyber awareness message?

We urge the government to consider better targeting its cyber awareness messaging to industry using industry-specific campaigns.

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience?

There is insufficient information regarding cyber security standards and compliance available to guide small to medium scale businesses (SMBs) and not-for-profits (NFPs) to guide their procurement decisions. For example, SMBs are significant purchasers of solar PV systems and batteries. These systems are covered by the Cyber Security Act 2024. From 2026, Ministerial rules under the Cyber Security Act will encourage inverter OEMs to voluntarily self-assess against three provisions of the EN 303 645 standard for cyber security of consumer IoT

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

devices. SMBs and NFPs are not well placed to undertake their own research into the cyber security standards of the products they purchase. A 'white list' or other third party, trusted source of information would assist Australian businesses and NFPs to evaluate the cyber security credentials of the products they buy and the companies with which they collaborate. We are hopeful that the IoT Alliance Australia can help to address this gap with its proposed Labelling Scheme for Smart Devices.

There could be a role for government or organisations funded by government grants to educate businesses and consumers about the value of certification to standards for information security management systems, such as AS ISO/IEC 27001, why it would be desirable for them to obtain this certification and why they should expect certification to standards like AS ISO/IEC 27001 from their information security management business partners.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting / endorsing SMB tailored standards?

SMBs and NFPs should be provided with free online resources suitable for staff training. Online cyber security training should be a standard part of all professional development for all employees who use computers or any internet-connected resources as part of their work.

To assist SMBs and NFPs with the selection of cyber secure IoT devices:

- the Ministerial rules under the Cyber Security Act 2024 could be enforced, and
- compliance with the Ministerial rules under the Cyber Security Act 2024 could be publicised, possibly by IoT Alliance Australia.

SMBs in the energy sector should be encouraged to participate in the AEMO AESCSF annual assessment.

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

We are aware of the mandatory reporting obligation that was introduced in the Cyber Security Act 2024, the Ransomware Playbook and other material published on cyber.gov.au. How the ransomware threat is evolving or changing is not SMA's area of expertise.

13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?

Governments could support training of staff by making available free online courses that educate people in the basics of avoiding phishing and other common methods used by cyber criminals.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

14. Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

Yes. SMA is headquartered in Germany. Our subsidiary offices adhere to the standards of the EU GDPR, unless local legislation requires us to do otherwise. The GDPR provides the world's best protection for data privacy. This includes personal energy data such as data regarding electricity consumption. This data is the basis of energy portals, which are supplied by most inverter OEMs along with their inverters. The legislation governing the privacy of personal energy data collected using inverter OEM portals is, we understand, determined by where the company is headquartered and where the data is stored. In the case of inverter OEMs that are headquartered and store their data in the USA, the privacy regulations are set at the state level and vary significantly from one state to another. In the case of inverter OEMs that are headquartered and store their data in the Peoples Republic of China (PRC), there are few, if any, protections for privacy of personal data.

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

There are very few cyber security regulations covering the renewable energy sector in Australia.

The most common enquiries that SMA receives regarding regulation of cyber security arise from obligations under the SOCI Act. We regularly receive requests from generators or their EPC contractors regarding our cyber security credentials, especially whether we have undertaken the AEMO annual AESCSF assessment.

There are several cyber security standards to which SMA and our products are certified, but these are not currently required by regulation. For example, SMA's information security management system is certified to ISO 27001. Our inverter product range for the home and business sector is certified to the EN 303 645 standard for consumer IoT cyber security. It is disappointing that there is no enforcement mechanism in place for the Ministerial rules under the Cyber Security Act and that they will rely on corporate goodwill and voluntary action for their success.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

No. There are very few cyber security compliance requirements that place any obligation on renewable energy generators. The SOCI Act applies to generators larger than 30MW and some, although not all, generators and EPC contractors ask for SMA's AESCSF cyber security credentials. Apart from that, we are not aware of any other rules or mandatory standards for cyber security of generation or storage of renewable energy.

18. What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?

Australia should draw on international cyber security standards wherever possible. For CER, the Ministerial rules under the Cyber Security Act will require IoT devices to satisfy three provisions of EN 303 645 from 2026. Those three provisions are:

- No universal default passwords,
- A means to manage reports of vulnerabilities, and
- Provision of information regarding how long a device is likely to be supported.

There are other requirements in EN 303 645 that all CER should be required to demonstrate. SMA urges the Government to amend the Cyber Security Act to require IoT devices to meet all EN 303 645, not just the three provisions currently in the Cyber Security Act. Inverters OEMs have had plenty of time to prepare. AS ETSI EN 303 645:2023 was directly adopted as an Australian standard in 2023.

OEM portals and VPP platforms should be required to meet ISMS cyber security standards such as ISO 27001.

19. How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?

The rooftop solar and battery sector in Australia is highly competitive and price driven. Improving cyber security costs money. So long as cyber security requirements remain voluntary, cyber secure products will be at a competitive disadvantage to products without cyber security features.

The Clean Energy Regulator has successfully implemented a model to ensure that all inverters purchased by Australian homes and businesses meet the AS 4777.2 product standard. The government should consider using this model for uplifting the cyber security of consumer

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

energy resources. The Clean Energy Regulator ensures that all inverters installed in Australia comply with AS 4777.2 using the following approach:

- Inverter OEMs must demonstrate compliance with AS 4777.2 for their product to be eligible for rebates under the SRES.
- OEMs obtain AS 4777.2 certification for their products from accredited test laboratories.
- The Clean Energy Regulator contracts the role of verifying compliance and publishing a 'white list' of compliant products. Currently, the CEC is responsible for verifying certification and publishing results.
- Agents who administer SRES rebate claims are responsible for verifying that the inverters used in systems for which a rebate is claimed appear on the CEC inverter list.

This system could very easily be adopted for demonstrating compliance with the Australian adoption of the international standard - AS ETSI EN 3030 645:2023. This is true, whether the compliance is with all the standard or only the provisions that currently are mentioned in the Ministerial rules under the Cyber Security Act. This approach will be far more effective than relying on the education of consumers. It would ensure that all installed inverters meet the mandated standards and would not assume that consumers are well-informed about cyber security standards and will take the initiative to demand certain standards in the products they purchase.

AS ETSI EN 3030 645:2023 is a product standard, suitable for application to inverters. However, a more significant threat to cyber security and privacy of personal energy data arises when internet-connected systems utilise OEM portals. SMA's energy data portal (known as 'Sunny Portal') and the systems associated with it are certified to ISO 27001. The government should consider mandating ISO 27001 for all energy data portals supplied by inverter OEMs. Platforms for VPPs should also be required to be certified to ISO 27001.

20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

Understanding of the risk of foreign ownership and control of technology vendors would be improved by an assessment of the technology, grid vulnerability, corporate ownership and control of fleets of inverter-based generation and storage assets. This assessment could include questions such as:

- What capacity of inverter fleet, if remotely controlled by a malicious actor, could cause a blackout on Australia's grids?
- How many OEMs already have an inverters fleet of that size in Australia?
- Where do those OEMs locate the computer servers that monitor and control their fleets?

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

- Who owns those OEMs and where are they headquartered?
- Which legislation applies to those inverter OEMs, the operation of their fleets and their use of data, including personal data?

Only responsible vendors will take on voluntary guidance. The government needs to be willing to regulate. It will be insufficient to rely on industry guidance, consumer education and voluntary activities.

21. How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?

It would be helpful for the government to start by clarifying the legal framework for the storage and use of personal data, including personal energy data. For example, most inverter OEMs gather their customers' personal energy data using data portals. The data collected is generally stored on computer servers in the country in which the inverter OEM is headquartered. In this situation, it is unclear whether the storage and use of the customer data is governed by Australian legislation, or the laws of the country in which the data is stored, or both. If both, it is unclear what is required when the foreign laws and Australian laws do not align. This is a significant issue for the use of customers' personal data. In the EU, the general principle is that customers should determine how their personal data is used. In some states in the USA, the law gives corporations leeway to use customers' personal data for the benefit of shareholders. In the PRC, the law gives the PRC leeway to use customers' personal data for the benefit of the PRC. It is unclear how the privacy of Australians is protected when their data is held overseas.

22. Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?

Protection of critical intellectual property (IP) is a challenge in the Australian electricity system. For an OEM like SMA whose inverters have advanced capabilities, our most critical IP is source code and block diagrams that enable those advanced capabilities. We understand that AEMO requires access to some critical IP especially to reassure itself that it is well prepared in the event of insolvency by a major OEM. However, we are very concerned that some network service providers (NSPs) are demanding access to OEMs' critical IP as a condition of network connection. AEMO has demonstrated high levels of security in the way it handles critical IP, but the same cannot be said for NSPs.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

Providing guidance will not be sufficient. The government should regulate to require minimum standards. It is impractical to expect consumers to educate themselves about which are the most relevant cyber security standards, and which products or companies meet those standards. The government should consider publishing a 'white list' of compliant products in various categories, or outsource that role to independent organisations. Adherence to the 'white list' could be driven as a requirement of regulations, or as a condition of grid connection approval or by making it an eligibility requirement of rebates. Consumer energy resources would be an ideal place to begin. The system already exists to ensure compliance of inverters with relevant Australian standards. It would be a very simple matter to extend the coverage to include product-level cyber security standards, like AS ETSI EN 3030 645:2023.

24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

Government subsidies are currently encouraging Australian homes and businesses to purchase and install energy products with no cyber security certification or other protections. The Australian Government should make cyber security a condition of eligibility for its solar PV and battery subsidies.

Some Australian jurisdictional governments (e.g. Western Australia) are mandating VPP participation as a condition of eligibility for solar and battery rebates. There are no mandatory cyber security requirements for VPPs in Australia. All VPP operators should be required to be certified to ISO 27001.

25. Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?

It would be helpful to know more about what is possible and permissible.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

30. Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

In the energy sector, the roles and responsibilities of AEMO and industry are clear. What remains unclear is responsibility for policies to ensure cyber security preparedness (including cyber security standards for products and platforms) and which government agency, if any, has responsibility for enforcement.

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

The government should mandate requirements through regulation (or as eligibility criteria for government rebates) and should impose penalties on companies that do not meet the requirements.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

Yes, that would be beneficial. SMA's vulnerability reports are published and are available here - https://www.sma.de/en/cybersecurity/security-notifications

33. How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

From SMA's perspective, the obligations under the SOCI Act are proportionate and well-understood. The failure is in enforcement. It has been left to industry to enforce standards on its supply chain. In a highly cost-competitive industry, there is constant pressure to use the cheapest supplier. There is no pressure from regulators to use suppliers with appropriate cyber security credentials.

34. Are there significant cyber security risks that are not adequately addressed under the current framework?

Yes. As outlined in our submission there are significant gaps in legislation and policies for cyber security. Even where there is legislation, enforcement is inadequate or non-existent.

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

The regulatory burden of cyber security for the renewable energy sector is very small. The risk is significant. Relying on voluntary action is wishful thinking. More and better regulation for cyber security is warranted and needed.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

36. What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?

As outlined in our submission, critical infrastructure owners and operators are expected to be responsible for assessing the cyber security credentials of their supply chain. In our experience some do – many do not. By allowing cyber security provisions to remain voluntary, companies that take cyber security seriously are at a competitive disadvantage to those who do not. Cyber security is a public good. It is insufficient for the government to encourage companies to do the right thing. The government needs to be willing to regulate and enforce the regulations.

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

The Australian Government can support private sector partners to uplift cyber security by:

- Mandating requirements in regulations,
- Enforcing regulations and acting against companies that do not meet regulations,
- Mandating cyber security requirements as eligibility criteria for rebates such as the SRES and other financial support mechanisms controlled by the Australian Government, such as the Capacity Investment Scheme (CIS).

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

The AESCSF is being used by generators that fall under the SOCI Act, and some of them are passing that requirement through to their supply chain.

46. Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

A good starting point would be to ensure that companies with the ability to control and monitor fleets of inverter-based generators and storage locate their computer servers in Australia and are unequivocally bound by Australian legislation, not the legislation of the country where their head office is located.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
[redacted]

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

The government should:

- Review and amend cyber security legislation to address gaps and ensure that the entire renewable energy industry is covered,
- Develop regulations to require compliance with cyber security standards,
- Clarify that for energy assets in Australia it is the Australian legislation that should have primacy, even if the data is stored overseas or if the computer servers controlling the inverter fleet are overseas,
- Consider regulating to mandate use of onshore computer servers for monitoring and controlling inverter fleets, and
- Develop mechanisms for enforcement that do not rely on goodwill by industry and voluntary action by consumers.

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment

International standards that should be adopted in Australian legislation and enforced through regulations (or as eligibility criteria for government rebates) include:

- EN 303 645,
- IEC 27001, and
- IEC 62443.