SMA Feedback on the proposed amendments to the CIRMP Rules

SMA-Australia welcomes the opportunity to provide feedback to the Department of Home Affairs (DHA) Consultation Paper on the proposed amendments to enhance the Critical Infrastructure Risk Management Program (CIRMP) Rules. The proposed amendments will make a valuable contribution to enhancing the cyber security of Australia's critical infrastructure. We welcome DHA's initiatives to improve Australia's cyber security posture.

SMA is a leading global specialist in photovoltaic (PV) system and battery energy storage system (BESS) power conversion and control technology. Our product range spans the home rooftop sector, commercial and industrial (C&I) applications, and large grid-scale applications. Our PV solar 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 GW in more than 190 countries and more than 10 GW inverter capacity in Australia. We are headquartered in Germany, with employees in 19 countries.

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 AG is publicly traded with a diversified shareholder base. Ownership is governed by German and European Union (EU) investment regulations. Risks of foreign control or undue influence are further mitigated through SMA's corporate governance structures, as well as through supplier due diligence, sanctions screening and risk-based supplier assessments.

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 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.

In our submission we focus on cyber security in the renewable energy sector. In future, 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.

There is an urgent need to modernise the legislation, regulations and CIRMP Rules to bring standards and approaches to cyber security for the energy system into the 21st century. Already, it is a regular occurrence for more than half of Australia's electricity to be sourced from renewable sources and the market share for renewable energy will continue to grow. Nevertheless, the legislation and regulations for energy sector cyber security have not been updated to account for the structural changes that have occurred. We know the access to data and control available to inverter original equipment manufacturers (OEMs). We know how that control and data access is regulated in Australia. The know that the regulations are inadequate. Guidelines for the application of the Australian Energy Sector Cyber Security Framework (AESCSF) to the renewable energy generation and storage supply chain would make the current framework clearer and more effective.

Cyber security regulations can be uplifted at minimal or no cost to responsible suppliers. Companies like SMA that take cyber security seriously already exceed the requirements proposed in the Consultation Paper.

We look forward to working with DHA as the review of the CIRMP Rules progresses.

Responses to the policy design questions raised in the Consultation Paper

All-hazard 1 – Consideration of specified risk advice

Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation?

Yes. The proposed critical asset classes for the energy sector are:

- Energy market operator asset
- Electricity asset
- Gas asset
- Liquid fuel asset

Greater specificity within asset classes (possibly sub-classes) would assist industry to understand roles and responsibilities.

In 2024 SMA AU undertook a self-assessment against the AESCSF for the first time. It was unclear which aspects of the AESCSF should apply to SMA, as an inverter OEM, and which parts of the AESCSF should apply to other parts of the supply chain. To address this, SMA AU commissioned an independent cyber security consultant to:

- develop guidelines for the application of the AESCSF to inverter OEMs, 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. We shared these guidelines with the Australian Energy Market Operator (AEMO) and other relevant regulators and policy makers.

It would be very helpful if DHA and AEMO could provide guidelines for application of the AESCSF to the electricity supply chain. This could involve defining cyber security roles and responsibilities for:

- Owners of electricity generation and storage facilities,
- Engineering, procurement and construction (EPC) companies,
- Inverter OEMs,
- Aggregators and virtual power plant (VPP) operators,

- Asset managers and operation and maintenance (O&M) providers, and
- Other third-party services providers.

Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?

There is significant room for improvement of enforcement mechanisms. Existing engagement mechanisms could be used to improve enforcement.

For example, the Security of Critical Infrastructure (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 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 room for improvement in this 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 1: 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 2: Alternatively, require generators and TNSPs to report on whether and how they are passing through their cyber obligations to their supply chain.

The cyber security risks in the renewable energy sector differ from legacy generators and warrant careful consideration. 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.

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, 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

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

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

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 3: 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 4: 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

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

Recommendation 6: 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 7: 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.

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)

Table 2 (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 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.

Table 2 – Assessment of cyber security risks and regulatory gaps in Australia

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 TNSPs pass through cyber security requirements directly to inverter OEMs and sometimes the 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 8: 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 9: 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 10: 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.

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 11: 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 12: 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.

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 13: 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 14: 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.

All-hazard 2 – All-hazard material risk

Are there any specific material risks, like those arising from FOCI, that your organisation minimises or eliminates in their CIRMP?

Does your organisation currently consider FOCI risks in their CIRMP?

Yes. SMA assesses FOCI risks and minimizes and eliminates them wherever we can. Overall, the Chinese supply base has no or very limited importance for the SMA large-scale division. Some of our suppliers manufacture in mainland China and other countries, however we generally purchase from suppliers whose head office is outside of China even if some of their manufacturing is within China.

We are very cautious about the origin of certain critical devices, any associated FOCI risk and the location of their head office. The approach taken for the critical items:

- We ensure that all important power electronics devices (such as insulated gate bipolar transistors and chokes) are produced outside of China by companies whose head office is not in China.
- We have a dual source strategy for fans. All mechanical parts and assemblies are sourced from Eastern Europe and the EU.
- Although battery cells are usually manufactured in either China or South Korea, the complete battery units are manufactured and assembled outside of China.
- Standard / catalogue electronic parts are generally bought directly from the manufacturer or their distributor, or in some cases from brokers.

- Supply chain issues are covered by SMA's contracts.

We ensure that none of the programmable or intelligent components in SMA's medium voltage power station (MVPS) used in the MVPS single-point-of-entry communication board are manufactured in China.

All MVPS communication (incoming and outgoing traffic) is centralised. Our communication board (known as the SC50COM) is the single-point-of-entry for network communication to and from the MVPS. The SC50COM is fully controlled by SMA. Hardware and software are manufactured by SMA. The board is programmed at SMA. No intelligent components on the communication board are manufactured in China. This security architecture effectively prevents access by hostile actors to other components of the MVPS.

Cyber 1 – Cyber security framework uplift

Where applicable, what maturity/profile does your organisation seek to achieve?

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.

As outlined above, in 2024 SMA AU undertook a self-assessment against the AESCSF and commissioned an independent cyber security consultant to develop guidelines for the application of the AESCSF to inverter OEMs and apply the guidelines to assess the cyber security of SMA in its role of inverter manufacturer and supplier to the Australian market.

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. 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 (below) shows the dashboard summary of the Deloitte / AEMO assessment results for the SMA AU large-scale division.

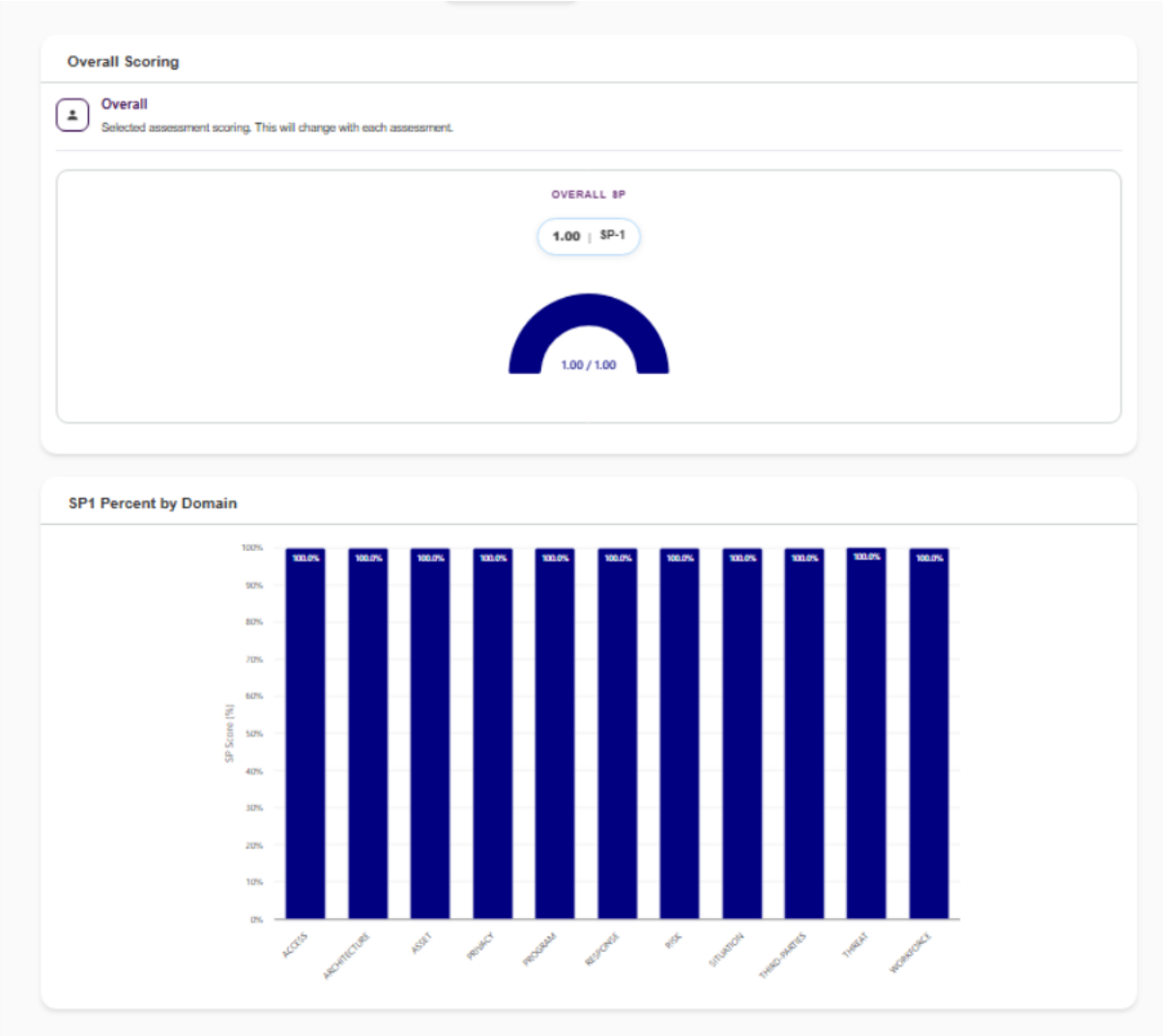

Figure 1: Deloitte / AEMO AESCSF assessment for SMA Australia large-scale division, 2025

SMA AU is currently preparing for the next AEMO assessment. We intend to undertake the full assessment process, so that we can be rated at the more stringent Security Profile 2 (SP-2) or Security Profile 3 (SP-3) levels of the AESCSF.

How does your organisation invest in security beyond achieving minimum cyber framework compliance?

Cyber security rules in the EU are stricter than Australia. Even if SMA were to only invest in minimum cyber security compliance in the EU, we would be beyond minimum compliance in Australia. However, in the EU SMA invests to remain ahead of minimum compliance requirements.

Does your organization face challenges in obtaining the necessary investment in security to reach compliance, or (where necessary) go beyond the minimum cyber framework?

SMA AG invests to maintain, and preferably stay ahead of, compliance with minimum cyber frameworks in the EU. This means that we also stay ahead of Australian cyber security requirements because the EU is more advanced than Australia in regulation of cyber security.

Cyber 2 – Critical systems network integration

What current measures does your organization implement to segregate their critical systems from all other internet facing and less secure systems?

Physically or logically segregated systems are used to isolate and run software that is required for business operations that incur higher risk for the organization.

We do not operate wireless networks that allow access to private aspects of our infrastructure. Wi-fi networks that allow guests to access the Internet do not have access to any private aspects of our infrastructure.

Does your organization mandate security awareness training for users with access to critical systems?

Yes. Cyber security awareness training is mandatory for all SMA AU staff and contractors, not just those with access to critical systems. In 2025 the completion rate for the mandatory cyber security training was 100%. We also conduct regular

and more detailed cyber security training workshops for users with access to critical systems.

What measures does your organization undertake to log who has access and can make changes to your critical systems?

SMA undertakes a range of measures including:

- We have a security operations centre (SOC) which monitors and responds to cyber threats.
- We have security information and event management (SIEM) software to collect, analyse and correlate security data across the organization.
- We regularly review log files for signs of intrusion.
- We have signature- and/or anomaly-based intrusion detection systems (IDS) and intrusion prevention systems (IPS) in place, and sensors are in place at strategic points throughout the network.
- We use anti-malware software. All workstations and servers have malware protection.
- We apply security patches to devices on our network on a regular basis.
- We have anti-spam and anti-phishing protection in place on our email service.

Cyber 3 – Multi factor authentication (MFA)

What type of systems in your organization are currently protected by MFA?

Multi-factor authentication (MFA) is used across the business.

Are there systems or circumstances in which MFA is not reasonably practicable to use? If so, what other compensating controls are, or could be implemented?

MFA is generally practicable. In some situations, security controls are determined by our customers (e.g. for remote VPN access for diagnostics and maintenance). MFA is practicable in these circumstances, however it might not be SMA's decision whether to implement it.

Supply chain 1 – Supply chain vulnerability mapping

To what level of upstream and downstream detail does your organization currently map its supply chain?

SMA maps its upstream and downstream supply chain to Tier 1. Beyond Tier 1, supply chains are mapped for availability purposes and for compliance with quality and sustainability standards. For example, for some electronics suppliers there is mapping to Tier 2 for assurance of deliverability and compliance with requested standards.

Does your organization keep a list or record of alternative approved suppliers?

Yes. A second-source strategy is applied for relevant SMA-specific parts. To ensure deliverability, a second source is generally considered in the awarding process. General specific standard (catalogue) parts are not affected by this strategy.

Does your organization have real-time access to data surrounding supplier availability?

A Vendor Managed Inventory is maintained for a limited number of strategically relevant parts. Availability is regularly assessed with suppliers to support flexibility and material availability.

Supply chain 2 – Vendors of concern

How does your organization currently map vendors of concern in your supply chain?

Annual risk analysis (Tier 1) includes assessment of "high risk" suppliers with respect to environmental social and governance (ESG) issues. Monitoring is undertaken using different risk monitoring systems. Quality-related risks are monitored by supplier quality managers.

What current security measures are put in place if a vendor of concern is identified?

A Corrective Action Plan is created to mitigate issues arising from identification of a vendor of concern. Failure mode and effects analysis is applied for quality-related issues. The overall procurement strategy considers the need to avoid

excessive strategic dependence on suppliers that may be geo-politically or environmentally sensitive.

Does the wider government provide adequate material to support you to identify a vendor of concern and mitigate their potential impact?

SMA AU would welcome advice from the wider government regarding vendors of concern and how to mitigate their potential impact. In 2025 SMA AU was accepted into the Australian Signals Directorate (ASD) Cyber Security Partnership Program, which is a useful source of advice regarding cyber security risks. It would be useful to have access to a government list of vendors of concern, but we are not aware of such a list. We have sought advice from AEMO, and their recommendation was to avoid Kaspersky, TikTok and Deepseek.

Are there other options to reduce the FOCI risk posed by vendors of concern, either in addition to or instead of the proposed approach?

SMA AU welcomes the proposal to require responsible entities to develop and maintain a system to manage risks posed by vendors of concern that expressly consider the risks of foreign ownership, control and influence (FOCI). However, it is unclear how companies are expected to implement this procedure and whether they would face legal and other risks if they were to do so transparently.

We recommend that government procurement processes should address FOCI risks transparently so that the approach and conclusions used by government agencies can also be adopted by companies.

Personnel 1 – Personnel Security Hazards

Does your organization have a personnel security plan, or equivalent in place?

Yes. SMA AU has a personnel security plan in place. It can be made available to DHA, on request.

Would a personnel security plan requirement improve security posture or duplicate existing controls?

SMA AU would support a personnel security plan requirement. We already have a personnel security plan in place so we expect that we could satisfy such a requirement relatively easily.

Does your organization currently use background checking as a security control?

Yes. SMA AU undertakes AusCheck background checks for all new employees and in 2025 we undertook AusCheck background checks for existing employees.

How many AusCheck background checks do you anticipate undertaking each year?

In 2025 SMA AU undertook 61 AusCheck background checks. In 2026, AusCheck background checks will be conducted for all new employees.

What challenges do you foresee for your organization to implement a personnel security plan?

SMA AU has a personnel security plan which is implemented and regularly reviewed. We do not foresee significant new challenges arising from a requirement to develop and implement a personnel security plan.

Physical and natural hazards

Does your organization have a broader physical security plan?

Yes.

What type of physical security measure would be beneficial?

SMA Australia has in place a range of physical security measures, summarized in our physical security plan. The physical security plan can be made available to DHA, on request.

Would a mandated physical security measure be beneficial and how could it be effectively applied to your asset?

SMA AU would support a physical security plan requirement. We already have a physical security plan in place so we expect that we could satisfy such a requirement relatively easily.

Are there additional material risks that your organization considers could be included for physical or natural hazards?

SMA Australia's physical security plan has broad scope. The physical security plan can be made available to DHA, on request.