SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

SMA feedback on the proposed amendments to the Ministerial Directions Powers

SMA-Australia welcomes the opportunity to provide feedback to the Department of Home Affairs (DHA) Consultation Paper on the proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure (SOCI) Act 2018. 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) systems and battery energy storage system (BESS) power conversion and control technology. With more than 144 GW of installed inverter capacity across over 190 countries, including more than 10 GW in Australia, SMA plays a significant role in enabling the global energy transition.

Headquartered in Germany, SMA manufactures its large-scale inverter portfolio entirely in Germany, ensuring high standards of quality, cybersecurity, and supply chain transparency in line with European regulatory frameworks.

Australia is one of SMA's top three global markets, alongside the European Union (EU) and the United States (US). SMA Australia Pty Ltd plays a key role in supporting the development of utility-scale solar and battery storage projects across the country. Following a recent strategic realignment, the Australian business is now fully focused on the large-scale segment, supplying these German-manufactured, cyber-secure inverter solutions to the Australian market. This focus reflects the increasing importance of system stability, cybersecurity, and advanced grid-support capabilities in Australia's evolving energy system.

SMA Solar Technology AG, the Group's parent company, is publicly listed on the Frankfurt Stock Exchange (Prime Standard) and is part of the SDAX index. Ownership and governance are subject to German and EU regulatory frameworks, ensuring strong oversight, transparency, and risk management. These are further supported by robust corporate governance practices, including supplier due diligence, sanctions screening, and risk-based supplier assessments.

SMA is strongly committed to cybersecurity and plays an active role in the development and implementation of industry standards to support secure, resilient energy infrastructure. We support the proposed amendments to the Ministerial Directions Powers outlined in the Consultation Paper.

In SMA's view most of the proposed Ministerial Directions Powers, if exercised, would result in raising standards to a level that we believe is a fair and reasonable given that the objective is to protect national security. The electricity system is critical infrastructure. Companies involved in critical

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

infrastructure should accept that a degree of regulatory oversight and, potentially, Ministerial direction is part of the cost of doing business.

SMA supports moves to strengthen data sovereignty. Australian facilities should be controlled from Australia. Australian data should be domiciled onshore and subject to Australian laws.

Sensitive data (such as details regarding cyber security) should not be freely available to board members who are linked to a foreign state-owned enterprise that is subject to extrajudicial direction under foreign intelligence or national security laws. The proposed Conditions Powers are a proportionate response to this risk. Additional governance or oversight requirements could be imposed on the subsidiary company, SMA Australia. However, governance changes at the SMA Solar Technology AG level would need to be carefully considered to avoid creating issues with governance and legal requirements of EU and German laws that apply to SMA as a publicly listed company.

We support the proposed powers to restrict the use of high-risk vendors, products or services.

We support the proposed amendments to enable delayed disclosure. SMA would need to consider the interaction with EU and German laws. We are a publicly listed company headquartered in Germany and governed in accordance with EU and German law.

We support the proposal to increase the penalties for non-compliance. However, we do not think the value proposed is sufficient to act as an effective deterrent.

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

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Responses to the questions raised in the Consultation Paper

Consultation Question – Measure 1

Scenario:

A major data storage/processing provider that services multiple critical infrastructure assets utilises an offshore managed service provider with links to a foreign state-owned enterprise. The Government has worked with the entity to improve and increase security around access controls and personnel hazards, but engagement stalls and privileged access pathways remain exposed. Based on whole-of-government advice, the Minister has determined the residual national security risk remains unacceptable. The Minister directs the provider to migrate privileged access functions back to Australia within a defined period and implement independent assurance of identity and access management. The direction follows extensive unsuccessful attempts to negotiate voluntary mitigation steps.

What this could look like for your organisation:

A Ministerial direction could require you to relocate high-risk system access functions to a secure Australian-based operating environment, strengthen identity and access management controls, and increase transparency over subcontracting arrangements and personnel security assurance measures. The direction would set outcomes and milestones, but allow flexibility in how you meet them, maintaining continuity of operations while reducing national security risk.

Questions:

How this compares to what you do now

Q1. How closely does the scenario align with how similar risks or dependencies are managed within your organisation? If not, what key differences would apply?

SMA uses data storage/processing providers based in the European Union (EU) and the United States (US). We are also planning to migrate Australian data and access controls to a service provider owned by a US technology company (e.g. Microsoft Azure) with servers and other infrastructure in Australia. We simply would not use the services of a data storage/processing provider that utilises an offshore managed service provider with links to a foreign state-owned enterprise.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

The location of computer servers that control and monitor Australia's fleet of inverter-based resources 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. In SMA's case, our subsidiary operations located outside of Germany comply with the regulations and norms of the country in which the subsidiary is located, or the EU or Germany, whichever is strictest.

Options and feasibility

Q2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches (e.g., guidance, independent assurance, contractual undertakings) could reasonably achieve a similar outcome in your context? Briefly rate feasibility and expected effectiveness.

In the scenario under consideration the Ministerial direction follows "extensive unsuccessful attempts to negotiate voluntary mitigation steps". In this scenario, it is difficult to see how more guidance documents and encouragement of voluntary action would succeed.

Implementation steps and timeframes

Q3. What internal steps and approvals would be needed to implement a direction of this kind (e.g., architectural changes, data/operational technology (OT) segregation, replacement of physical components, supplier re-papering, governance)?

If this situation arose, SMA would act on efforts by the Department of Home Affairs (DHA) to negotiate voluntary mitigation steps. We would accelerate our plans to migrate Australian data and access controls to a US service provider using a data centre in Australia.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Q4. What is a realistic implementation timeline by milestone (e.g., design, procurement, migration, cut-over) while maintaining service continuity? Identify the top three schedule drivers (e.g., change windows, supplier lead times).

Due to competing priorities, we have not yet had the opportunity to plan or receive estimates of the time required and the cost to migrate Australian data and access controls to a service provider owned by a US technology company with servers and other infrastructure in Australia.

Benefits and risk-reduction

Q5. What operational or risk-reduction benefits would you expect from implementing the direction (e.g., reduced likelihood of privileged compromise, improved mean time to detect/contain, fewer exception pathways)? Please indicate any available internal metrics (even if approximate).

The reasons why SMA is planning to migrate Australian data and access controls to a US service provider using a data centre in Australia include enhanced business continuity due to less reliance on communications links with the EU, and contribution to Australia's national security.

Costs and constraints

Q6. What one-off activities would drive effort/cost (e.g., migration, tooling uplift, legal re-papering)? What ongoing activities would persist (e.g., monitoring, periodic assurance)? (You may provide numbers separately if you prefer.)

Due to competing priorities, we have not yet had the opportunity to plan or receive estimates of the time required and the cost to migrate Australian data and access controls to a service provider owned by a US technology company with servers and other infrastructure in Australia.

Q7. Are there operational, contractual or technical impediments that would materially affect how you could comply (e.g., vendor lock-in clauses, specialised OT equipment, data residency constraints)?

We are not aware of any significant barriers to our plans to migrate Australian data and access controls to a US service provider using a data centre in Australia. Preliminary discussions with prospective service providers indicate that this will be a relatively simple exercise.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Board, governance and legal interfaces

Q8. What board-level processes or approvals would you expect to trigger (e.g., risk acceptance thresholds, major capex approval, change of risk appetite)?

Our plans to migrate Australian data and access controls to a US service provider using a data centre in Australia are not expected to require board-level approval. The expenditure will need to be approved, but this can be done from Australia without board approval.

Q9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act that would need to be managed to comply with a direction (such as continuous disclosure, related-party approvals, conflicts management, or director duty considerations)? What guidance from Government would assist your board/company secretary to document compliance?

We do not anticipate that our plans to migrate Australian data and access controls to a US service provider using a data centre in Australia would require any legal or compliance interfaces under the Corporations Act. We expect it to be a routine investment decision.

Market, customers and cumulative effects

Q10. Would compliance have any material impacts on customers, prices, or service quality during transition? Are there cumulative burden issues when combined with other obligations (e.g., CIRMP, privacy, sectoral rules)?

There should be no material impact on customers provided the migration is well planned and managed. There would be a cost, but it would be relatively minor when amortised across the business. We plan to use the migration and the benefits for business continuity, cyber security and national security as a component in our marketing strategies.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Evaluation and support

Q11. What success indicators (e.g., control maturity, reduction in privileged access exceptions, incident metrics) would show the direction achieved its objective in your context? What support or guidance from Government would help (e.g., reference architectures, assurance templates)?

The main objectives of SMA's plan to migrate Australian data and access controls to a US service provider using a data centre in Australia are improved business continuity, contribution to cyber security of the electricity system and to Australia's national security.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Consultation Question – Measure 2

Scenario:

A major cloud services provider that is a critical infrastructure entity under the SOCI Act enters a commercial arrangement with a foreign venture capital fund. Under the agreement, the fund receives a board observer right with access to relevant committee papers. In accordance with SOCI Act Part 2A, the Board is required to approve the entity's Critical Infrastructure Risk Management Program (CIRMP), which contains detailed cross-domain vulnerabilities (physical, cyber, personnel, and supply chain), security architecture diagrams, incident response dependencies, and prioritised remediation plans.

The fund is linked to a foreign state-owned enterprise that is subject to extrajudicial direction under foreign intelligence or national security laws. Government engagement seeks to limit access to security-sensitive materials, but the provider declines, citing investor rights and contractual undertakings. The national security risk remains unresolved.

The foreign-affiliated observer obtains access to the full CIRMP documentation and exfiltrates content. Because foreign compulsion laws can require individuals to cooperate with foreign intelligence agencies, the sensitive material (an aggregated, high-value map of the entity's weaknesses) is at real risk of use for espionage, sabotage, coercion, or targeting (including impacts that could degrade grid reliability, cloud availability, or national security functions). The risk persists even where there is no compromise of IT systems, as the access is legitimate from a corporate governance perspective.

What this could look like for your organisation:

If a board observer or investor representative continued to access sensitive strategic or cyber security information despite unresolved FOCI concerns, the Minister could impose governance-related conditions requiring:

- limited access to defined categories of material (e.g., classified CIRMP annexes only on a need-to-know basis)
- restructured committee participation, including a security-cleared Security Risk Committee independent of foreign-affiliated directors/observers
- independent oversight, including external assurance of CIRMP handling and insider-risk controls, and/or
- ring-fencing of critical systems and data, including prohibitions on offshore access, support, or administration.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Questions:

How this compares to what you do now

Q1. How closely does the scenario align with how similar governance or control risks would manifest in your organisation? If not, what key differences would apply?

SMA would not accept a major investment from a foreign venture capital fund linked to a foreign state-owned enterprise that is subject to extrajudicial direction under foreign intelligence or national security laws.

Options and feasibility

Q2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome in your context (e.g., revised observer protocols, targeted NDAs, committee charter changes, information segregation, independent assurance)? Briefly rate feasibility and expected effectiveness.

The proposed governance-related conditions are reasonable. SMA is a foreign-owned company, headquartered in Germany and publicly listed on the Frankfurt Stock Exchange (Prime Standard) and is part of the SDAX index. We understand and accept that insofar as we supply products that are part of critical infrastructure, accepting regulatory oversight is an expected and reasonable aspect of doing business. The risk-based approach proposed in the Consultation Paper is broadly consistent with the regulatory direction we are seeing in the EU.

SMA Australia is a subsidiary or SMA Solar Technology AG. We would suggest that DHA could impose additional governance or oversight requirements at the SMA Australia subsidiary level. Imposing governance changes at the SMA Solar Technology AG level would need to be carefully considered to avoid creating issues with governance and legal requirements of EU and German laws that apply to SMA as a publicly listed company.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Implementation steps and timeframes

Q3. What internal steps and approvals would be needed to implement governance-focused conditions (e.g., board/committee resolutions, constitution or shareholder agreement changes, access control changes, security vetting for defined roles, independent audit engagement)?

To answer this question, we would need to understand the details of the proposed governance-related changes. It is difficult to provide a detailed answer to a hypothetical scenario that could involve a range of governance-related changes. Broadly, we would need to ensure that any changes are in accordance with governance and legal requirements of EU and German laws that apply to SMA as a publicly listed company.

Q4. What is a realistic timeline by milestone (e.g., design of safeguards, approvals, contracting, rollout) while maintaining continuity of operations? Identify the top three schedule drivers (e.g., shareholder approvals, meeting cycles, vetting lead times).

This question is difficult to answer in the abstract, given that the proposed powers could enable the Minister to direct a range of governance changes. We would need further details of the proposed hypothetical scenarios and additional time to provide a more meaningful response.

Benefits and risk-reduction

Q5. What governance or risk-reduction benefits would you expect from implementing the conditions (e.g., reduced likelihood of undue influence over security-sensitive decisions, lower exposure of sensitive materials, improved audit findings)? Please indicate any available internal metrics (even if approximate).

In this hypothetical scenario, other benefits to SMA would include enhanced protection of competitively sensitive data.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Costs and constraints

Q6. What one-off activities would drive effort/cost (e.g., legal re-papering, charter/constitution changes, access model redesign, onboarding independent directors/committee members, vetting)? What ongoing activities would persist (e.g., additional committee oversight, periodic independent assurance, access monitoring)? (You may provide numbers separately if you prefer.)

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 a company headquartered in Germany, SMA would need to comply with German and EU laws. There could be costs involved in requirements for legal advice, especially if there was a real or perceived conflict between the Ministerial Direction and EU laws. This seems highly unlikely.

Q7. Are there operational, contractual or technical impediments that would materially affect how you could comply (e.g., investor rights clauses, listing rule obligations for committees, identity/access tooling limits)?

This question is difficult to answer in the abstract, given that the proposed powers could enable the Minister to direct a range of governance changes. Broadly, we would need to ensure that any changes are in accordance with governance and legal requirements of EU and German laws that apply to SMA as a publicly listed company.

Board, governance and legal interfaces

Q8. What board-level processes or approvals would you expect to trigger (e.g., committee restructuring, conflicts management protocols, risk appetite changes)?

This question is difficult to answer in the abstract, given that the proposed powers could enable the Minister to direct a range of governance changes. Broadly, we would need to ensure that any changes are in accordance with governance and legal requirements of EU and German laws that apply to SMA as a publicly listed company.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Q9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with conditions (such as director duties, related-party considerations, changes to constitutions, or disclosure obligations)? What guidance from Government would assist your board/company secretary to document compliance?

This question is difficult to answer in the abstract, given that the proposed powers could enable the Minister to direct a range of governance changes.

Market, customers and cumulative effects

Q10. Would compliance have any material impacts on customers, prices, service quality or investor relations during transition? Are there cumulative burden issues when combined with other obligations (e.g., existing FATA conditions, CIRMP, Protective Security Policy Framework (PSPF), sectoral rules)?

No, we would not anticipate any material impact on customers, prices, or service quality. The hypothetical scenario assumes there is a major investment from a foreign venture capital fund linked to a foreign state-owned enterprise. Presumably, relations with that investor would change under this scenario.

Evaluation and support

Q11. What success indicators (e.g., reduction in access to sensitive materials by observer roles, improved independence in security-sensitive decisions, audit outcomes) would show the conditions achieved their objective in your context? What support or guidance from Government would help (e.g., template conditions, model committee charters, sample access matrices, assurance templates)?

Benefits of the governance changes in this hypothetical scenario would include better protection of competitively sensitive data, and less influence by the foreign venture capital fund linked to a foreign state-owned enterprise.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Consultation Question – Measure 3

Scenario:

It is identified within a specific sector that a widely deployed brand of network switches and routers includes an undocumented remote access capability that routes traffic through infrastructure located in a foreign jurisdiction subject to national security laws that are hostile towards Australia's interests. The vendor refuses to allow independent verification of the firmware and does not provide a credible technical explanation for the remote function. Government issues security guidance and engages with the sector to encourage transitioning away from the equipment, but uptake remains inconsistent due to vendor lock-in, limited alternative supply, and commercial upgrade cycles. Security advice concludes that entity-level risk management cannot reliably mitigate the exposure, and the risk is systemic across the sector.

What this could look like for your organisation:

If specified high-risk equipment posed a persistent access risk that could not be mitigated by individual entities, a Ministerial direction could restrict further procurement or deployment of the equipment across the sector, with a phased transition plan and reasonable timeframes to avoid service disruption. Where immediate removal is not possible, compensating controls (e.g., segmentation, enhanced logging/monitoring, code-integrity assurance, SBOM/supplier assurance, uplifted access controls, independent verification and audit) may be required during transition.

How this compares to what you do now

Q1. How would a vendor-specific restriction of this kind interact with your current technology stack, procurement cycles, network/OT architecture, and operational processes? Are there key differences from the scenario that would affect implementation?

SMA assesses foreign ownership, control and influence (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.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

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.

Options and feasibility

Q2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome in your context (e.g., strengthened sector guidance, an industry code with independent audit, Government procurement restrictions only, enhanced vendor due-diligence/assurance)? Briefly rate feasibility and expected effectiveness.

SMA is very active in detecting and eliminating FOCI risks. Advice on ownership of suppliers could assist companies like SMA that have already voluntarily adopted a program of FOCI risk management.

An industry code and Government procurement restrictions could assist but are unlikely to be an effective substitute for Government directions in the hypothetical sicario being considered.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Implementation steps and timeframes

Q3. What internal steps and approvals would be required to comply (e.g., asset inventory and criticality mapping, replacement program planning, network redesign/segmentation, firmware validation, contract variations or re-tenders, outage/change windows, customer communications)?

SMA already maintains a comprehensive register of IT and OT assets.

In the hypothetical scenario, the time required for remediation would depend on the extent of the problem, whether it can be addressed by firmware or requires hardware replacement, and supply chain and logistical issues.

Q4. What is a realistic timeline by milestone (e.g., design/validation, procurement, lab and integration testing, staged deployment, decommissioning) that maintains service availability and resilience? Identify the top three schedule drivers (e.g., supply constraints, interoperability testing, regulatory dependencies).

This question is difficult to answer in the abstract. To provide a meaningful answer, we would need more details about the proposed scenario, the extent of the problem, whether it can be addressed by firmware or requires hardware replacement, and supply chain and logistical issues.

Benefits and risk-reduction

Q5. What security or resilience benefits would you expect (e.g., reduction in privileged/remote access pathways, lower probability of systemic compromise, improved detectability/forensics, reduced attack surface across interdependent assets, reduced mean-time-to-detect anomalies due to standardised telemetry)? Please indicate any available internal metrics (even if approximate).

In the hypothetical scenario, replacing the compromised routers would be necessary to ensure the security of the infrastructure.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Costs and constraints

Q6. What one-off activities would drive effort/cost (e.g., equipment replacement or remediation, redesign and testing, contract modifications, data migration, workforce upskilling)? What ongoing activities would persist (e.g., compensating controls, enhanced monitoring/telemetry, periodic independent assurance)? (You may provide numbers separately if you prefer.)

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

A Corrective Action Plan would be created to mitigate issues arising from identification of a vendor of concern. SMA's overall procurement strategy considers the need to avoid excessive strategic dependence on suppliers that may be geo-politically or environmentally sensitive.

If hardware needed to be replaced across SMA inverter fleet, labour and travel would likely be the most significant drivers of effort and cost.

Q7. Are there operational, contractual, supply-chain or technical impediments that could materially affect your ability to comply (e.g., vendor lock-in, limited comparable technologies, third-party dependencies, integration with legacy OT)?

No. SMA already undertakes annual risk analysis (Tier 1). This includes assessment of "high risk" suppliers with respect to environmental social and governance (ESG) issues. Monitoring is undertaken using different risk monitoring systems. The overall procurement strategy considers the need to avoid excessive strategic dependence on suppliers that may be geo-politically or environmentally sensitive.

Board, governance and legal interfaces

Q8. What board-level processes or approvals would you expect to trigger (e.g., major capex approvals, risk appetite changes, write-down decisions, customer notification strategies)?

In a scenario where hardware needs to be changed for every SMA inverter in the field, there would be a need for approval for major capex, notification to the market and customer notification.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Q9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with a vendor-restriction direction — such as continuous disclosure, asset impairment disclosures, or directors' duty considerations in balancing transition risk and service continuity? What guidance from Government would assist your board/company secretary to document compliance?

This question is difficult to answer in the abstract. We would need to understand the extent and cost of the direction to provide a more meaningful answer.

Market, customers and cumulative effects

Q10. What are the likely market and competition implications (e.g., near-term vendor concentration, price effects, supply constraints, interoperability impacts) during transition? Would compliance have material impacts on customers, prices or service quality? Are there cumulative burden issues alongside other obligations (e.g., CIRMP, privacy, sectoral rules)?

If hardware needed to be replaced then depending on the hardware in question, there might be vendor concentration and supply constraints.

Evaluation and support

Q11. What success indicators would demonstrate the direction achieved its objective in your context (e.g., % removal or remediation by milestone, reduction in high-risk remote access paths, incident/near-miss trends, independent verification results)? What support or guidance from Government would help (e.g., reference architectures, interoperability/segmentation patterns, minimum telemetry/assurance requirements, SBOM formats, model contract clauses)?

In this scenario the benefits speak for themselves. Success would mean elimination of remote access capability that routes traffic through infrastructure located in a foreign jurisdiction subject to national security laws that are hostile towards Australia's interests.

There could also be interim milestones, such as the percentage of equipment relaced.

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

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

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 the Australian Energy Market Operator (AEMO), and their recommendation was to avoid Kaspersky, TikTok and Deepseek.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Consultation Question – Measure 4

Scenario:

A publicly listed operator and SOCI Act-captured entity that hosts cloud and colocation services for government agencies, financial institutions, and large corporates, detects a potential cyber intrusion within its privileged access management systems. The affected environment supports identity and access functions for numerous tenants, including several operators of critical infrastructure assets.

The company investigates the potential compromise which reveals that the intrusion bears hallmarks of a highly capable state-backed threat actor, including advanced tradecraft designed to move laterally across client environments without immediate detection. It engages the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) for technical advice and support.

While the entity has contained the attacker's initial foothold, evidence is identified suggesting that the malicious actor has attempted to harvest authentication tokens used by several interconnected tenants, including operators in the aviation, banking, and energy sectors. Preliminary advice indicates a real possibility that premature public disclosure such as through the entity's continuous disclosure obligations could, among other things:

- Alert the threat actor their activities are known, thereby accelerating their activities before remediation can be completed.
- Encourage opportunistic attackers to exploit similar identity related vulnerabilities shared across other Australian data storage and processing assets, including those used by the Government and critical infrastructure.
- Disrupt migration efforts underway with ASD and making detection of the actor's activities against other entities more difficult.

Following the initial period of analysis, the entity determines it would need to make a public disclosure in accordance with the Corporations Act and ASX Listing Rules. Government advises that a premature public announcement could create material national security and systemic economic risks, including potential unauthorised access to sensitive government workloads and cascading disruptions across multiple industries relying on hosted systems.

Under the proposed options, ASIC or the Minister for Home Affairs could delay the entity's disclosure obligations for a limited period, for example, 30 days. This temporary delay would enable:

- Completion of cross-tenant remediation and token revocation.
- Hardening of identity infrastructure across other data centre operators facing related vulnerabilities.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

- Coordination with impacted aviation, banking and energy operators to ensure continuity of essential services.
- Preparation of a controlled, accurate public communication once systemic risks were mitigated.

Q1. Is a delayed disclosure power necessary in high-risk cyber incidents, and what types of disclosure obligations (under the Corporations Act or otherwise) should it cover?

Delayed disclosure is reasonable in the scenario where disclosure without delay would compromise national security.

Q2. In the above scenario, would section 111AT (Option 1) be sufficient to prevent an entity disclosing the cyber incident or would the entity require a direction under SOCI (Option 2) to prevent disclosure? Why?

We have not had the opportunity to seek legal advice on this.

Q3. Are there any non-legislative disclosure obligations (e.g., contractual requirements during capital raisings or major transactions) that could prevent or undermine a delayed Corporations Act disclosure?

We would need to consider the interaction with EU and German laws. The company is headquartered in Germany and is governed in accordance with EU and German law as a publicly listed company.

Q4. Who should hold the power to delay disclosure (ASIC, the Minister for Home Affairs, or both)?

The Minister for Home Affairs.

Q5. What criteria should govern when a delay can be issued?

It should be governed by the opinion of the Minister for Home Affairs that without a delay, national security could be compromised.

Q6. What safeguards, time limits, and oversight mechanisms are needed while still enabling effective risk management?

An appropriate safeguard would be for the Minister to take advice from ASIC to enable an appropriate balance of maintaining transparency in the market while preserving national security.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Q7. What operational or compliance impacts might arise during a delay?

SMA would need to seek legal advice on the interaction with EU disclosure requirements. We have not yet done so.

Q8. What guidance, tools, or support would entities need to meet their obligations under this power, and how should the market be informed once a delay is lifted?

It would be helpful to have legal guidance on the responsibilities of multinational companies if the Australian legal requirement is contrary to the legal requirement in the country of its head office.

Q9. Are there relevant international practices that should inform the model, and what unintended consequences should be considered?

We recommend DHA consider how the proposed requirement would interact with laws of relevant countries, such as the EU, USA, China, and other companies active in the Australian energy market with head offices overseas.

SMA Australia Pty. Ltd.
ABN: 44 127 198 761
Level 8, 76 Berry Street
North Sydney NSW 2060
Tel.: +61 1800 SMA AUS

Consultation Question – Measure 5

Scenario:

Q1. Does the proposed increase in the maximum civil penalty (from 250 to 2,000 penalty units) provide an effective deterrent to non-compliance with Ministerial directions under Part 3 of the SOCI Act? Why or why not?

No. The proposed penalty is $660,000. That is not a deterrent. It's a cost of doing business.

Q2. What level of penalty would you consider proportionate to the seriousness of failing to comply with a direction issued to manage a material national security risk?

A more appropriate penalty for failing to manage a material national security risk would be 20,000 penalty points or the value of a year's revenue for the company, whichever is larger.

Q3. Are there alternative mechanisms, in addition to or instead of increased penalties, that could more effectively encourage timely and complete compliance with Ministerial directions?

Yes. Directors could face custodial sentences.

Q4. What guidance or support would assist your organisation to understand and meet compliance expectations under an updated penalty framework?

It should be sufficient for DHA (on behalf of the Minister) to provide clear directions, with explanations if necessary.

Q5. Do you foresee any unintended consequences of increasing the maximum penalty to 2,000 penalty units (e.g., operational, financial or implementation impacts)? If so, please describe.

No.