



11 August 2026

Electricity Authority Te Mana Hiko
Level 7, Aon Centre
1 Willis Street
Wellington 6011
New Zealand

By email: fsr@ea.govt.nz

Submission: Proposal for Transpower to share common quality information between System Operator and network owner functions

1. Introduction

SMA welcomes the opportunity to provide feedback to the Electricity Authority Consultation Paper on the 'Proposal for Transpower to share common quality information between System Operator and network owner functions'.

SMA is a leading global specialist in photovoltaic (PV) systems and battery energy storage system (BESS) power conversion and control technology. With more than 156 GW of installed inverter capacity across over 190 countries, including more than 468 MW in New Zealand, 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.

Following a recent strategic realignment, SMA's New Zealand business is now fully focused on the large-scale segment, supplying these German-manufactured, cyber-secure inverter solutions to the New Zealand market. This focus reflects the increasing importance of system stability, cybersecurity, and advanced grid-support capabilities in New Zealand'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. Our cyber security credentials are summarised in Attachment 1.

We look forward to working with the Authority as the review of the Transpower proposal progresses. We also look forward to working with the Department of Prime Minister and Cabinet as it progresses its uplift of cyber security for critical infrastructure and we encourage the Authority to ensure that decisions taken in relation to this proposal are consistent with those efforts.

2. Summary

SMA supports the Authority's objective of ensuring that Transpower, in its role as a transmission network owner, has access to the information it requires to plan and operate the transmission network efficiently. SMA does not, however, support the proposal in its current form. In SMA's view, the proposal presents a material risk to the cyber security of New Zealand's critical infrastructure and to the intellectual property (IP) of the manufacturers who supply that infrastructure. SMA considers that this risk is likely to affect the willingness of original equipment manufacturers (OEMs) to invest and participate in the New Zealand market, and that the resulting cost to the New Zealand economy would outweigh the administrative savings identified in the Consultation Paper.

3. What is at risk?

The proposal puts at risk the security of source code and block diagrams of inverters. Access to the source code and block diagrams of SMA's inverters could enable competitors to replicate SMA's products, resulting in the loss of intellectual property of very substantial value. Malicious actors can also use source code and block diagrams to undermine operation of critical infrastructure by changing critical operational parameters. For example, changing settings for fault ride through could enable an external fault (like a failure of a large power station) to trigger wider systemic failure by causing failure of other generators and battery storage to ride through the fault, as required. Large scale battery storage could be damaged or destroyed simply by changing the maximum charging voltage parameter.

As noted in the recent Discussion Document issued by the Department of the Prime Minister and Cabinet¹,

"Cyber risks are generally not well understood or collectively managed to a consistent level across New Zealand's critical infrastructure system."

Systems using SMA inverters in New Zealand will, in most cases, exceed 30 MW and will therefore be considered critical infrastructure. We expect Transpower and EA to understand the need to protect the core control systems for critical infrastructure.

The Department of Prime Minister and Cabinet has demonstrated an understanding of this risk and has acknowledged the reluctance of companies to share information that could be used to harm competitiveness.

SMA considers it essential that the need to protect the core control systems of critical infrastructure is given commensurate weight in the Authority's assessment of this proposal.

4. What does SMA want?

SMA wants to continue to do business in New Zealand with confidence that we are not required to compromise our standards for protection of IP and cyber security as part of the cost of participating in the New Zealand energy transition. For SMA, this means:

- There should be no requirement to share unencrypted models of inverters to any organisation except for Transpower in its role as System Operator,
- There should be a register of all people with access to the relevant IP and the register should be accessible by the owner (e.g. SMA) who is required to share its IP,

¹ Enhancing the cyber security of New Zealand's critical infrastructure system: Digitally resilient critical infrastructure services to power New Zealand's economy and protect our communities

- When models are shared (whether encrypted or unencrypted) there must be a non-disclosure agreement (NDA) directly between the owner of the IP and the person receiving the IP,
- The owner of the IP should have legal recourse if a person to whom IP was provided makes unauthorised use of it.

5. Risks arising from the proposal

SMA is not presently in a position to assess the cyber security maturity of Transpower's transmission network owner function. SMA has not been provided with information sufficient to satisfy itself that Transpower's core information technology (IT) networks afford the level of protection appropriate to material of this sensitivity. SMA would welcome engagement with Transpower and the Authority on this point. The Department of Prime Minister and Cabinet has acknowledged that in New Zealand, "approximately 35 percent of SCADA assets... are at or nearing the end of their life. Such assets tend to be no longer supported by the original supplier, creating vulnerabilities that can be used by malicious actors to access and compromise core IT networks."

New Zealand does not have a centralised or consistent approach to sharing or reporting information related to the cyber security of critical infrastructure. To our knowledge, Transpower has not publicly released the results of a detailed cybersecurity assessment or maturity score. Transpower has not published:

- Its overall cybersecurity maturity rating,
- Assessment scores by domain, or
- Alignment with international standards.

New Zealand does not currently have mandatory cyber security legislation applying to critical infrastructure operators. SMA notes the Department of the Prime Minister and Cabinet's own observation that New Zealand's approach to cyber security remains predominantly voluntary and submits that a voluntary framework is not a sufficient basis on which to broaden access to OEM intellectual property. As acknowledged by the Department of Prime Minister and Cabinet, the National Cyber Security Index ranks New Zealand 49th in the world and the lowest of the Five Eyes partners. New Zealand ranks particularly poorly on factors related to cyber security of critical infrastructure.

Our understanding of the Transpower proposal (see footnote 15², p.16) is that asset owners would be required to provide:

- m1 model in PowerFactory (may be encrypted)
- m2 model in PowerFactory (must be unencrypted)

² Footnote 15 of the Consultation Paper states, "Owners of synchronous generating stations are required to provide both the m1 and m2 models in PowerFactory format. Owners of IBR assets are required to provide both the m1 and m2 models in both PowerFactory and PSCAD formats. Owners of IBR assets are also required to provide the m2 model in Powertech's Transient Security Assessment Tool (TSAT) format. The PowerFactory m2 model provided by owners of IBR assets must be unencrypted. All other models may be provided in encrypted form."

- m1 model in PSCAD (may be encrypted)
- m2 model in PSCAD (may be encrypted)
- m2 model in Powertech's Transient Security Assessment Tool (TSAT) (may be encrypted)

SMA does not support the CACTIS requirement for the sharing of unencrypted models. This proposal puts SMA's IP at risk. It also puts at risk the cyber security of the New Zealand electricity grid and all other electricity grids to which SMA inverters are connected. If participation in the New Zealand market requires acceptance of this level of exposure, SMA will need to reconsider the basis on which it supplies equipment into that market.

5.1 Risks regarding models and best practice solutions

SMA's biggest concern is regarding security around sharing of PSCAD models and the prospect of them being shared with staff and consultants without SMA's knowledge, without any NDA and without any practical possibility of SMA taking legal recourse if the critical IP leaks. The relative ease with which PSCAD models can be reverse engineered means that, in SMA's view, the proposal carries a risk that is disproportionate to the benefits identified. We are less concerned about the prospect of sharing PowerFactory Loadflow modelling or an encrypted TSAT model due to the lower risk of loss of IP through reverse engineering.

Open, encrypted PSCAD models are relatively simple to reverse engineer especially when aided by artificial intelligence (AI). Even with encryption, an open PSCAD model gives access to backward and forward control signals which aids the reverse engineering process. A reverse engineered PSCAD model would enable a competitor to copy SMA's IP and would enable a malicious actor to undermine system security. (e.g. simply by turning off or changing fault ride through settings).

This is not a theoretical concern about how encrypted models might be handled. Clause 4.8 of the CACTIS requires that, where an asset owner provides an encrypted PSCAD or TSAT model, the inputs and outputs of the encrypted model must be made accessible to the System Operator, and the function of the encrypted portion must be explained in the supporting documentation. The CACTIS therefore requires the provision of precisely the input and output visibility, together with a functional description, that materially assists reverse engineering. Encryption under the CACTIS limits inspection of a model; it does not render the model opaque. SMA submits that the Consultation Paper's treatment of encrypted models as carrying a materially lower risk of unconsented disclosure should be revisited in light of clause 4.8.

Best practice approaches to handling encrypted PSCAD models include the following:

- The encrypted PSCAD models are only made available to system operators. They are not required and therefore not made available to network service providers (NSPs), NSPs' consultants, customers or customers' consultants.
- System operators handle the sensitive IP contained in encrypted PSCAD models under a prescribed set of conditions. For example, retaining all PSCAD models on a single laptop, allowing access to no more than two consultants and recording all instances of staff or consultants accessing the critical IP.

6. Responses to the questions raised in the Consultation Paper

Q1. Do you support the Authority's proposal to require the System Operator to provide Transpower, as a transmission network owner, with access to the System Operator's ACS database, subject to appropriate information use and confidentiality requirements? If not, why not?

SMA does not support the proposal in its current form, although its concern with this limb of the proposal is narrower than its concern with the sharing of modelling information. SMA recognises that asset capability statement information is provided to the System Operator by the asset owner, and that it is for the most part not information in which SMA holds intellectual property. SMA has two concerns.

First, an asset capability statement records equipment capability and operational limitations, including matters such as the maximum transient reactive current specified for the purposes of clause 8.25B(1). That information reflects the design and performance envelope of SMA's equipment. It is commercially sensitive, notwithstanding that it is not source-level material of the kind contained in a vendor-specific model.

Second, the Consultation Paper states at paragraph 3.17 that Transpower would be required to treat all asset capability statement information as confidential and to comply with appropriate information handling, use and security requirements. On SMA's reading, the proposed drafting in Appendix A does not achieve this. The confidentiality and storage obligations in proposed clause 3(7)(b) of Technical Code A attach only to information accessed under proposed clause 3(5)(b), being modelling information. Asset capability statement information accessed under proposed clause 3(5)(a) attracts a use restriction only. SMA sets out its comments on the drafting in response to question 10.

If the confidentiality and handling obligations described at paragraph 3.17 were given effect in the drafting and were of the standard set out in SMA's response to question 3, SMA would not oppose Transpower, as a transmission network owner, being given access to the asset capability statement database. SMA's remaining concerns, which relate to modelling information and to the framework as a whole, are set out in response to questions 2, 3, 5 and 6.

Q2. Do you support the Authority's proposal to require the System Operator to share encrypted modelling information with Transpower as a transmission network owner, subject to appropriate information use and confidentiality requirements?

SMA does not support the proposal in its current form. SMA is willing to provide Transpower with information it requires on request and subject to an NDA.

SMA does not support arrangements under which its intellectual property may be accessed without SMA knowing the identity of the recipients and without a non-disclosure agreement in place.

SMA also draws the Authority's attention to clause 4.9 of the CACTIS, which provides that where an original equipment manufacturer deems a model is not to be shared publicly, the asset owner must additionally provide the System Operator with a PowerFactory or Western Electricity Coordinating Council generic model that the System Operator may share publicly. The CACTIS therefore already contains a mechanism for making a usable representation of an asset available to parties other than the System Operator without exposing proprietary detail.

SMA submits that this mechanism, rather than the sharing of vendor-specific models, should be the default position for Transpower in its transmission network owner role. Transpower's stated

need, as described in section 4 of the Consultation Paper, is for network planning, design, protection coordination and asset management. For much of that work the generic model provided under clause 4.9, together with the asset capability statement, is likely to be sufficient. Where a vendor-specific model is demonstrably necessary for a particular study, SMA is willing to provide it on request, subject to a non-disclosure agreement executed directly with SMA. This would meet Transpower's requirements at materially lower risk than a standing entitlement of access.

Q3. Do you support the Authority's proposal to require Transpower's transmission network owner function to meet the same access and storage requirements for encrypted and unencrypted modelling information as apply to the System Operator? If not, why not?

SMA supports the principle of applying consistent obligations to both of Transpower's functions. SMA submits, however, that the obligations in clause 3(2A) of Technical Code A are not adequate for material of this sensitivity, for the reasons set out in SMA's submission of 04 August 2026 on the incorporation of the CACTIS. In particular, the obligation in clause 3(2A)(b) is owed to the party that provided the information, so where the asset owner rather than the OEM provides the models the OEM has no standing to enforce it; there is no requirement for individual confidentiality undertakings from those granted access; clause 3(2A)(c) requires only that systems, policies, procedures and confidentiality obligations be in place to prevent disclosure so far as reasonably possible, which falls short of a flow-down of equivalent obligations to contractors and advisers; there is no register of persons with access, no notification to the owner of the intellectual property, and no requirement to return or destroy the material; and the OEM has no remedy under the Code in the event of a breach. Extending those obligations to a second function does not address the underlying deficiency.

SMA acknowledges, and welcomes, that clause 2(11) of Technical Code A permits an asset owner to discharge its obligation under clause 2(10)(c) by arranging for the original equipment manufacturer to provide modelling information to the System Operator directly. Where that route is used, the OEM is the party that provided the information and the confidentiality obligation in clause 3(2A)(b) is owed to the OEM. SMA regards this as an important protection and asks the Authority to confirm that reading.

More fundamentally, SMA submits that the Code should specify the requirements for handling modelling information, rather than expressing them at a level of generality that leaves the substance to be determined by the party holding the information. There is a marked asymmetry in the framework as it stands. What an OEM must disclose is prescribed with precision: model type, software platform and encryption state are specified in the CACTIS at the level of individual files. What may be done with that material once disclosed is described in three general limbs, being that it is treated as confidential, stored on a secure server, and made available only to persons subject to appropriate systems, policies, procedures and confidentiality obligations. The operative detail, being who may be granted access, on what undertaking, for how long, with what logging, and what becomes of the material when it is no longer required, sits in internal policy. It is not consulted on, is not visible to the owner of the intellectual property and may be varied unilaterally.

SMA submits that requirements of this kind belong in the Code. If they sit in the Code, they are settled through a public process in which OEMs may participate, they are enforceable by the Authority, and they cannot be changed without consultation. SMA suggests the Code specify, at a minimum, that access be limited to named individuals recorded in a register; that each such individual give a personal confidentiality undertaking; that the register be available on request to the owner of the intellectual property in the information; that contractors and advisers be bound by

obligations no less restrictive than those applying to Transpower; that access be logged; and that the material be returned or destroyed once the purpose for which it was provided is spent.

SMA makes a related observation about where the disclosure obligations sit. The requirement that the PowerFactory M2 model be provided in unencrypted form is the most intellectual property sensitive obligation in the framework. It does not appear in the Code. It appears in the CACTIS, which is a system operation document prepared by Transpower as System Operator and which may be amended under clauses 7.13 to 7.22 of the Code. The scope of what must be disclosed is therefore capable of being expanded through a process attracting less statutory scrutiny than that which governs the protections in Technical Code A, and at the instance of a party that benefits from the disclosure. SMA raised this in its submission of 04 August 2026 and repeats it here because the present proposal widens the class of persons within Transpower who may access that material. Where a requirement compels the disclosure of proprietary source-level material, SMA submits that the requirement should sit in the Code.

Q4. Do you support the System Operator to provide Transpower as a transmission network owner with access to equivalence arrangement and dispensation applications and supporting information? If not, why not?

SMA does not object to the sharing of equivalence arrangement and dispensation information that does not contain OEM intellectual property. SMA does not, however, support any arrangement under which its critical intellectual property, including the material contained in PSCAD models, may be disclosed without SMA knowing the identity of the recipients and without a non-disclosure agreement in place.

Q5. Do you agree with the Code amendment proposal's objective? If not, why not?

SMA agrees with the objective of ensuring that Transpower, as a transmission network owner, is able to maintain the integrity, stability and safety of the transmission network. SMA does not agree that the objective, as framed, gives adequate weight to the protection of OEM intellectual property. In SMA's view, the administrative efficiencies identified are outweighed by the risks and potential costs of cyber security breaches and loss of investment.

SMA also considers that the objective, as framed, does not account for the effect of the proposal on the level of cyber security protection applying to intellectual property relating to critical infrastructure. Comparable jurisdictions are strengthening cyber security requirements for critical infrastructure, and SMA submits that New Zealand should not move in the opposite direction.

SMA submits that this is not solely a question of protecting SMA's commercial interests. Intellectual property relating to critical infrastructure raises cyber security and, ultimately, national security considerations. SMA submits that the objective should be framed with those considerations in view, rather than by reference to the integrity of the transmission network alone.

Q6. Do you agree the Code amendment proposal's benefits outweigh its costs? Please provide evidence to support your view.

No. The rationale for the sharing of IP as outlined in the CACTIS is to reduce the cost and administrative burden of the System Operator signing NDAs with OEMs. The net present benefit identified is modest when compared with the loss an OEM would sustain if its intellectual property were disclosed to a competitor. The cost benefit analysis of the CACTIS does not take account of the economic impact if the new regulations deter key OEMs from participating in the New Zealand

market. SMA submits that this is a material risk which warrants express consideration in the Authority's cost-benefit analysis.

The Consultation Paper states that confidentiality and information security obligations on Transpower as a transmission network owner will be strengthened. From an OEM perspective, the displacement of directly negotiated non-disclosure agreements reduces rather than increases the protection available, for the reasons given in response to question 3. SMA is not presently able to assess the assurance given and would welcome further detail on the substance of those obligations, on how compliance with them will be monitored, and on what recourse is available to an OEM in the event of a breach.

SMA is also concerned that a proposal which broadens internal access to intellectual property relating to critical infrastructure may reinforce investor concerns about New Zealand's approach to security and competitiveness, and about its attractiveness as a destination for investment. The Department of the Prime Minister and Cabinet has itself observed that New Zealand's approach is not keeping pace with comparable countries, and that domestic and overseas investors alike need assurance that critical infrastructure is prepared to withstand and recover from cyber incidents. That consideration does not appear in the evaluation of costs and benefits.

In summary, SMA submits that the proposal would reduce the protection afforded to OEM intellectual property, would carry consequential cyber security risk, and may affect New Zealand's attractiveness as an investment destination. The Consultation Paper quantifies the offsetting benefit as a net present benefit of \$85,000 to \$154,000 over fifteen years. SMA submits that this is not a proportionate basis for the change proposed.

SMA requests that the Authority defer further progress on this aspect of the CACTIS until further consideration has been given to the risks and potential costs of OEMs avoiding investment in New Zealand and how IP protections could be strengthened to avoid this scenario while achieving the reform objectives of the Electricity Authority.

Q7. Do you agree the Code amendment proposal is preferable to other options? If you disagree, please explain why and give your preferred option in terms consistent with the Authority's main statutory objective in section 15 of the Act.

No. SMA does not support the Code amendment proposal in its current form. SMA's preferred option is: A register of who has access to SMA IP, including consultants

- For the register to be available to SMA
- NDAs with all people who have access to our data
- A means of recovering IP or recourse if it leaks

SMA would add to the above that the generic model mechanism in clause 4.9 of the CACTIS should be the default basis on which Transpower, as a transmission network owner, is given access to modelling information, with vendor-specific models provided on request and under a non-disclosure agreement where a particular study demonstrably requires them.

Q8. Do you agree with the analysis presented in this Regulatory Statement? If not, why not?

SMA does not agree with the analysis in the Regulatory Statement in one material respect. The evaluation of costs and benefits at Table 1 quantifies the administrative savings available to Transpower and to asset owners but attributes no cost to the increased exposure of OEM

intellectual property, or to the risk that OEMs restrict the models they are prepared to supply into the New Zealand market.

The Authority treats the reduced need for bilateral non-disclosure agreements as a benefit. From an OEM perspective, a non-disclosure agreement is not solely a transaction cost. It is the instrument that gives the intellectual property owner standing, visibility of who holds its information, and a remedy if that information is misused. Removing it does not eliminate the risk; it transfers the risk from Transpower to the OEM. SMA submits that this transfer should be recognised as a cost in the analysis.

SMA notes that the transaction cost saving quantified at paragraphs 6.13 and 6.14 is the saving from not negotiating non-disclosure agreements in respect of unencrypted models. On SMA's reading of the proposed drafting, unencrypted models will continue to be provided by asset owners and OEMs directly to Transpower as a transmission network owner under the transmission agreement, rather than being shared by the System Operator. The costed benefit therefore does not arise from the sharing of encrypted information between Transpower's two functions. It arises from the displacement of bilateral confidentiality arrangements in respect of unencrypted models. SMA develops this point in response to question 10.

Q9. Do you agree the Code amendment proposal complies with section 32(1) of the Act?

SMA does not express a view on whether the Code amendment proposal falls within the Authority's powers under section 32(1) of the Act. SMA notes, however, that the assessment against section 15(1) rests on the proposition that strengthened confidentiality obligations will maintain the trust and confidence of asset owners and OEMs. For the reasons set out above, SMA does not consider that proposition is presently made out, and the efficiency benefits claimed may accordingly be overstated.

Q10. Do you have any comments on the drafting of the proposed Code amendment? Please explain your answer.

SMA has the following comments on the proposed drafting.

(a) The proposed drafting does not extend any confidentiality or storage obligation to asset capability statement information. The obligations in clause 3(2A) of Technical Code A are framed by reference to information provided under clause 2(10)(c), being modelling information. Asset capability statement information is provided under clause 2(2). Proposed clause 3(7)(b) applies the clause 3(2A) obligations only to information accessed under proposed clause 3(5)(b). Asset capability statement information accessed under proposed clause 3(5)(a) therefore attracts only the use restriction in proposed clause 3(7)(a). This does not deliver what paragraph 3.17 of the Consultation Paper describes. Because clause 3(2A) is itself confined to clause 2(10)(c) information, simply cross-referring to it will not close the gap. SMA suggests either that clause 3(2A) be amended so that its scope extends to asset capability statement information, or that a corresponding obligation be drafted for that information.

(b) Proposed clause 3(5)(b) confers access to encrypted modelling information but does not prohibit the provision of unencrypted modelling information by the System Operator to Transpower as a grid owner. Paragraph 4.28 of the Consultation Paper states that unencrypted models would continue to be obtained directly from the asset owner or OEM. Given the sensitivity of the material, SMA submits that this should be stated expressly rather than left to inference, by providing that the system operator must not give Transpower as a grid owner access to unencrypted modelling information.

(c) The term “encrypted modelling information” in proposed clause 3(5)(b) is not defined in the Code. Under clause 4.6 of the CACTIS only the PowerFactory M2 model is required to be unencrypted; whether the remaining models are provided in encrypted form is a matter for the OEM. The scope of proposed clause 3(5)(b) is therefore determined by choices made outside the Code and may vary between assets and over time. SMA suggests the term be defined, and that the definition make clear that a model is not encrypted for the purposes of the clause merely because parts of it are encrypted.

(d) Proposed clause 3(7)(b) applies the clause 3(2A) obligations to Transpower as a grid owner as if those obligations applied to it. Clause 3(2A)(b) requires the information to be treated as confidential to the party that provided it. Where information reaches Transpower as a grid owner under proposed clause 3(5)(b), the party that provided it is the System Operator, which is to say Transpower itself. On that reading the obligation would be owed by Transpower to Transpower, and the benefit that clause 2(11) confers on an OEM that supplies models directly would be lost at the point of transfer. SMA suggests the drafting preserve the identity of the protected party, by providing that Transpower as a grid owner owes the obligation to the same party to whom the system operator owes it under clause 3(2A)(b).

(e) Proposed clause 3(5) operates as a new gateway through clause 3(2). Clause 3(2) provides that information about an asset may be disclosed by the system operator only as expressly provided for in the Code, as required in a grid emergency or for grid security, as required by law, or as otherwise agreed with the relevant asset owners. At present the route to Transpower as a grid owner is clause 3(2)(d), agreement. The proposal converts that consent-based route into a standing statutory entitlement under clause 3(2)(a). SMA submits that the Consultation Paper should be explicit that this is the legal effect of the amendment, and that the consent presently required is being removed rather than streamlined.

(f) Models provided under clause 2(10)(d) appear to fall outside clause 3(2A) altogether. Clause 2(10)(d) requires an asset owner to provide a model that can be used for the network models in clause 8.25A(3)(a). Clause 3(2A) applies only to information provided under clause 2(10)(c). SMA raises this as a gap in the existing framework which the Authority may wish to address while amending clause 3.

(g) Proposed clause 8.54AB confers access to all information held by the system operator on applications for equivalence arrangements and dispensations. Proposed clause 8.54AB(2) restricts the use of that information but imposes no confidentiality obligation, no storage requirement and no control on access, and the obligations in proposed clause 3(7)(b) do not extend to it. Supporting information for a dispensation application may include test results, design detail and modelling material of the same sensitivity as the material dealt with under Technical Code A. SMA suggests that proposed clause 8.54AB apply the same handling obligations, in whatever form those obligations are finally settled.

(h) The reference in proposed clause 8.54AB(1) to all information held by the system operator on an application is unbounded. Paragraph 5.5 of the Consultation Paper describes the purpose more narrowly, being to enable technical input on whether a proposed equivalence arrangement or dispensation would compromise system security or reliability. SMA notes that the outcome of an application is already visible to Transpower as a grid owner: clause 8.54AA requires the system operator to maintain and publish the system operator register, and decisions on equivalence arrangements and dispensations are published in that register under clause 8 of Schedule 8.1. What proposed clause 8.54AB adds is access to the application and its supporting information, which is the material most likely to contain OEM intellectual property. SMA suggests the

entitlement be confined to information necessary for the assessment contemplated by proposed clause 8.54AB(2).

(i) SMA suggests the Code require the System Operator and Transpower as a grid owner to maintain a register of persons granted access to modelling information, and to make that register available on request to the owner of the intellectual property in that information, together with the further handling requirements set out in SMA's response to question 3.

**Q11. Do you see any unintended consequences in making the proposed Code amendment?
Please explain your answer?**

Yes. SMA anticipates that the proposal may weaken cyber security protections in practice and could result in the loss of SMA's critical intellectual property to a competitor.

A further consequence, which SMA considers the Authority should weigh, is that OEMs may respond by limiting the models they are prepared to supply into the New Zealand market, or by declining to supply at all. That outcome would reduce the quality and completeness of modelling information available to both the System Operator and Transpower, which is the opposite of the effect the proposal is intended to achieve.

Submitted by:

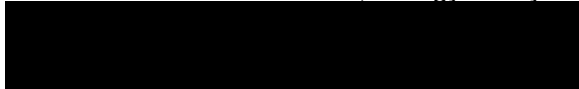
SMA Australia Pty Ltd
Level 8, 76 Berry Street
North Sydney NSW 2060
Australia

By its Authorised Representative:

A handwritten signature in blue ink, appearing to read 'J Alexander', with a horizontal line drawn underneath it.

John Alexander
Managing Director
SMA Australia Pty Ltd

Contact: Darren Gladman, Energy Policy & Regulatory Affairs



Attachment 1 – SMA's Cyber Security Credentials

As an EU-headquartered company, SMA aims for the highest standards of cyber security. We meet and aim to exceed all cyber security standards in the countries in which we operate.

We meet the EU's NIS2 Directive which establishes a comprehensive cybersecurity framework for critical infrastructure in the EU and applies to inverter OEMs such as SMA. NIS2 requires a risk-based approach to cybersecurity that covers asset management, secure system design, supply chain security, incident detection and reporting, vulnerability management, business continuity, and recovery planning. Operators must implement technical and organisational controls to protect operational technology (OT), communications networks, and cloud-connected services from cyber threats.

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.

We have undertaken assessment against the Australian Energy Sector Cyber Security Framework (AESCSF) since 2024. The AESCSF assessment (managed by Deloitte and overseen by the Australian Energy Market Operator (AEMO) confirmed that we met SP-1 level standards using the 'Lite' framework, achieving a rating of 100% across all applicable domains. In 2026 SMA undertook the full assessment under the AESCSF. The results, benchmarking and how the results can be described to the market were confirmed by Deloitte and are summarised in Figures 1 to 3, below.

Maturity Indicator Level (MIL) scores



We can say that overall SMA scored:

100% at MIL-1

99% at MIL-2

98% at MIL-3

Figure 1 – SMA's 2026 Maturity Indicator Level (MIL) scores

Security Profile (SP) scores



We can say that overall SMA scored:

99% at SP-1

100% at SP-2

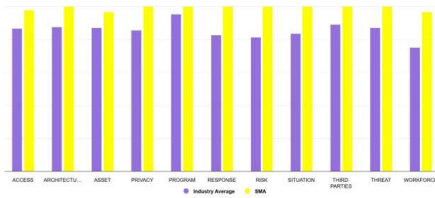
97% at SP-3

SMA Solar Technology

4

Figure 2 – SMA's 2026 Security Profile (SP) scores

Comparison to average



This compares SMA to the "industry average" of 'non-market participants'

SMA is encouraging Deloitte and AEMO to benchmark inverter OEMs for a more meaningful comparison

SMA Solar Technology

6

Figure 3 – Benchmarking of SMA against industry average of the five 'non market participants' who completed the 2026 AESCSF assessment