Developing Horizon 2 of the 2023-2030 Australian Cybersecurity Strategy

29th August 2025

Australian Government
Department of Home Affairs

Lodged electronically

SolarEdge Technologies is a global frontrunner in smart energy solutions, particularly renowned for revolutionising how solar power is harvested and managed with its direct current (DC)-optimised inverter systems. Since its foundation in 2006, the company has shipped over 57 GW of systems and monitors more than 4.3 million solar installations across 145 countries, demonstrating its considerable global reach and technological leadership. SolarEdge's design, pairing optimisers with a string inverter, boosts energy yield, enhancing output by 2%–15% in all settings and delivers up to 50 extra days of energy per year. Its broad, diversified product line (including inverters, power optimisers, monitoring platforms, electric vehicle charging, and battery storage) further underpins its strong market position and appeal to a wide range of energy stakeholders across both residential and commercial distributed markets.

Introductory remarks

With the primary focus of SolarEdge Technologies being in the residential CER space, it is very clear to us, based on our international businesses and large scale activities, that cybersecurity requirements in Australia are lagging behind the rest of the world which is exposing vulnerabilities and risks, both at DER/CER level, but given the volume of the DER/CER installations in Australia it also poses significant system security risks for the energy sector.

SolarEdge Technologies has built its product, including vendor selection processes and system-level integration, with cybersecurity at the core. As such, SolarEdge welcomes the opportunity to respond to the consultation on developing Horizon 2 of the 2023-2030 Australian Cybersecurity Strategy.

Feedback on Consultation Questions

2. Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

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

Implementation: there are clear overarching objectives already detailed, but without clearly defined mechanisms for application, especially at a product and governance level, the 'Embed' element of cyber security messaging, standards, capability and efforts will be hard to apply.

Considering specifically the rapid growth of the DER/CER sector, and all of the millions of access points and regions of system critical infrastructure, there needs to be a lot more safeguards around products being installed as well as information networks accessing devices and controlling them.

There needs to be a clear governance structure around rules and regulations as this is a fundamental requirement for domestic, as well as international, cyber regulatory alignment.

Currently. Although cyber regulation and policy exist, it is very hard to find out what requirements should be applied and how meeting requirements are enforced or reported.

There needs to be much clearer information defining industry-specific requirements, specifically the DER/CER space and have a body in place to administer and enforce the requirements.

2.2 Collaborating across all levels of Australian Government

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

There needs to be a national set of Device, Data, Network, Visibility and Control standards and procedures for the DER/CER industry implementations and managed under a robust governance framework.

Systems like the AESCSF could be enhanced with more evidence and compliance-based mechanisms, as this is a very good evaluation tool, but with conformance structured around self-declaration, it misses accountability and enforcement capabilities.

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cybersecurity outcomes

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

The high-level model (Figure 5. Cybersecurity Policy Evaluation Model) is based on new technology being developed, which in itself poses a significant risk, as the majority of threats from a cyber perspective originate from existing technology.

The high-level model should be amended to include existing technology; this will help to highlight existing gaps that need to be addressed as well as existing technology already capable of complying and contributing to a new cyber framework.

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

A simple process for the DER/CER sector would be to use the current Clean Energy Council (CEC) list of approved inverters to ascertain the OEMs that currently have, and have historically been important and have installed devices in Australia.

Using the fundamental requirements of the 'Cybersecurity (Security Standards for Smart Devices)' it will be possible to see what gaps currently exist with the installed fleet of products, as well as what products that have previously been installed be able to comply.

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

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

Currently, the messaging feels appropriate at a very high level.

However, industry-specific awareness, such as within the DER/CER region, there is a complete lack of any education for Australian consumers when it comes to product selection, installation and best practices.

In fairness, this is probably also due to a lack of any meaningful regulation, standards required for compliance, benchmarking and governance.

6. What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cybersecurity expertise?

No comment.

7. How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?

One simple process would be to ensure that any devices that could potentially be accessed and pose a cyber risk be clearly identifiable.

It's good practice to educate and encourage SMBs and NFPs to uptake existing cyber resources, but the resources lack detailed information of products or services that have native Cyber Resilience. Ideally, a good outcome would be to have both hardware and software to be ranked and listed so that entities can see what intrinsic levels of in-built safety exist within the products, a bit like a cyber star rating, or the 'U.S. Cyber Trust Mark', which is a cybersecurity certification and labelling program. (Expected timeline for the official release: 2025)

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

As mentioned in Q7. Ideally, a good outcome would be to have both hardware and software to be ranked and listed so that entities can see what intrinsic levels of in-built safety exist within the products, a bit like a cyber star rating to sit on top of safe practices.

9. What existing or developing cybersecurity standards, could be used to assist cyber uplift for SMBs and NFP's?

Ensure that products and services can meet the following:

- *ETSI 303-645*
- *The radio equipment directive 2014/53/EU*
- UK PSTI

In addition,

- The 'Cyber Resilience Act' which is an EU wide legislation for the cybersecurity of IoT and connected devices (effective from 2026-2027)
- The 'NIS 2 Directive', again, an EU wide directive for achieving a high level of cybersecurity across the EU (effective October 2024).
- UL 2941, which is a dedicated international standard for the cybersecurity of Smart Inverters and Distributed Energy Resources (Expected timeline for the official release of the standard: 2025)

10. What are the unique challenges that NFP entities face for cybersecurity compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?

It comes down to financial resources to implement data hosting in facilities certified to ISO 27001, etc. There is also a lack of resources to use 3rd party specialist consultants to review current practices and help recommend mechanisms to uplift security levels.

To achieve these recommendations, there needs to be financial support packages for consultation and implementation of mechanisms to improve cyber-secure systems and infrastructure for NFPs.

11. Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?

They are expensive and often contain get-out clauses that put the onus of responsibility back on the small entity, making them non-viable products.

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

SolarEdge has a good understanding of the threat of ransomware; the threats are becoming more sophisticated and common.

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

Offer a dedicated support package for businesses, this should include the full spectrum of support once a demand has been received, to settling the demand and then supporting with an investigation for accountability and also identifying the means of the attack.

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

The DER/CER globally experiences cyber-attacks on a very regular basis. For a detailed breakdown of the extent and methods, please refer to the DERSec Solar Vulnerabilities report of 2024:

- https://dersec.io/reports/DERSec-Solar-Vulnerability-Summary-v2.0-Final.pdf

Additionally, the DNV report of 2025 on 'Solar sector proposes solutions to mitigate critical cybersecurity risks' also helps to articulate the challenges and proposed solutions.

- https://api.solarpowereurope.org/uploads/SPE_2025_Solutions_for_PV_Cyber_Risks_to_Grid_Stability_032dc2ae5a.pdf?updated_at=2025-04-29T07:11:32.315Z

15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? and

The Government should consider adopting a legal structure, such as in Denmark, that gives everybody the right to their own body, facial features and voice to counter Deepfakes as an addition to identity crime prevention. Denmark's law is structured to give individuals complete control, similar to copyright, over their own image, including their face, voice and body.

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

The 'Australian Cyber Security Legislation', but it needs to cover a lot more ground.

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

Globally yes, within Australia no….

3.2 Shield 2: Safe technology

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

- *ETSI 303-645*
- *The radio equipment directive 2014/53/EU*
- UK PSTI
- The EU 'Cyber Resilience Act'
- The EU 'NIS 2 Directive'
- UL 2941
- Having data hosting in facilities certified to ISO 27001

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

A good way to highlight risk is to have both hardware and software listed and ranked so that entities can see what intrinsic levels of in-built safety exist within the products, a bit like a cyber star rating, or the 'U.S. Cyber Trust Mark', which is a cybersecurity certification and labelling program.

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

SolarEdge already employs a strict vendor vetting process for hardware components (HBOM). We have end-to-end software development in EU and Israel both for inverter and Local Controllers. We employ security analysis of any 3rd party code as well as secure manufacturing site controls.

At an organisation level we have cyber awareness training, secure coding training, a vulnerability disclosure program (Bug Bounty), a business continuity plan as well as a cyber insurance policy.

From a technical perspective, we have a Technical Director for Product Cybersecurity, a dedicated secure development lifecycle (SDL) team, a vulnerability researchers & In-house "Red Team" as well as an incident Response Team (IRT).

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

SolarEdge considers that in the DER/CER space, data access and transfer across the economy is already well understood by industry.

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

Mandate much stricter minimum product and system requirements as well as a governance structure around enforcement.

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

To start with, define both 'safe and responsible'. Currently, there is no effective way to assess emerging technologies' risk factors. For this, there will need to be product, system, infrastructure, reporting and vulnerability assessments defined and mandated.

3.3 Shield 3: World-class threat sharing and blocking

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

Proactivity is motivated by incentives. Alternatively, proactivity is motivated by a requirement to comply within a ranking system, where the highest-ranked levels of industry can become favoured or mandated.

25. Does the government need to scope and define what Australia's proactive cybersecurity posture should look like for industry?

The scope should fall into four key components:

Device Security
Data Security
Network Security
Visibility and Control

When considering the DER/CER segment, from SolarEdge's perspective, these components can be described as follows:

Device Security

Securing devices from unauthorised access is crucial for ensuring seamless functionality and continuous operation of a PV system.

This is achieved by combining several security measures tailored to the unique security needs of each PV system and its components. SolarEdge implements unique device passwords and restricts remote access only to pre-authorised users.

Remote access is role-based and granted to specific users for a limited duration after completing multi-factor authentication (MFA*).

Additional device security measures include detection and prevention of run-time anomalies by an embedded security agent, built-in casual Wi-Fi scanning protections, static code analysis and 3rd party penetration testing.

All SolarEdge inverters receive over-the-air security updates, ensuring customers have secure access to software and firmware updates.

Data Security

To protect data generated by a PV system, the remit extends beyond physical device security.

Connected SolarEdge inverters for example, do not store sensitive information in them and can be fully wiped of configuration data in a factory reset.

SolarEdge stores system-generated data on-premises at a dedicated SolarEdge-operated data centre in Germany.

We implement a comprehensive backup cycle to protect our customers' data and store it with multiple redundancies.

Best practice encryption and authentication are in place for a system to access the server.

SolarEdge is fully compliant with the requirements of the GDPR.

Network Security

Any basic PV system requires internet connectivity to provide performance monitoring.

This potential vulnerability becomes more acute when an advanced energy optimisation system is integrated in the organisation's IT network. An attacker accessing the PV system could potentially infiltrate the company's IT network.

To protect both the PV system and the company's IT network, SolarEdge limits access to the PV system through a single point of entry, via the SolarEdge Local Controller, or via the Inverter in smaller installations.

All communications passing through the gateway are inspected and analysed, and a masking feature enhances protection by making it inaccessible, even if an intrusion attempt is made within the same LAN.

To further mitigate risk, the gateway's communication with our servers can be set up via a separate cellular-based connection or a dedicated VLAN.

A relay protection device can be added to provide physical circuit protection.

Visibility & Control

In addition to ongoing, proactive monitoring, SolarEdge's security methodology empowers the customer's IT and security teams to monitor their energy assets in real-time.

All communications between the gateway and the SolarEdge server are encrypted and channelled through a single port (443), which can be whitelisted by the IT department.

If IT monitoring and switch-off capability is desired, the system can also be set up under a dedicated VLAN.

SolarEdge devices contain an extra security feature, designed to block any remote action on the inverter, unless temporary access is granted by someone physically present at the device.

SolarEdge devices also collect robust security logs on failed log-in attempts, system crashes and general system performance.

Data analysed at SolarEdge's SOC (Security Operations Centre) can be made available to customer IT teams.

26. How could government further support industry to block threats at scale?

Implement data handling and access controls based on existing, robust international standards.

27. How could the use of safe browsing and deceptive warning pages be amplified?

There needs to be more focus on handheld devices, such as smartphones and the remote use of 3rd parties to spy on users, either via gathering metadata, the use of the camera or the microphone. The threat is to consumers is not so much about their browsing habits, it comes from the default functions of tracking apps.

The use of safe browsing and deceptive warning pages should not be amplified; they need to be added to, to include deletion of browser data and cookies.

28. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

There needs to be more work done to identify threat and scam routes, especially through misleading advertising on social media platforms. Building on the HCSN Pilot, this level of data access and information misuse could easily be replicated across many sectors.

29. How can we better align and operationalise intelligence sharing for cybersecurity and scams prevention?

There needs to be a coordinated intelligence sharing platform across all industries to help identify risk and share threats as well as support with prevention activities/education.

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

To have a robust 'early warning system' and a clearly defined support process post-attack.

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

Mandate the requirement.

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

Yes.

3.4 Shield 4: Protected critical infrastructure

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

The SOCI Act, at a high level, it is fit for purpose; however, the definition of critical infrastructure needs to be addressed as it does not effectively encapsulate the DER/CER industry, which has more digital connection points into the energy system than any other industry segment.

For example, the Act states that an asset is a critical electricity asset if it is:

(a) a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules; or

(b) an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with subsection.

In principle, when a DNSP (Distribution Network Service Provider) operates a CER flexible export, Dynamic Operating Envelope, or Emergency Backstop Mechanism, they will be coordinating the generation output of CER devices via a network well in excess of 100,000 customers; however, obligations under the Act are as yet not being adhered to in full.

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

Not that SolarEdge can identify.

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

SolarEdge considers that they are.

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

Entities managing the aggregation of assets and vulnerabilities should be assessed against the AESCSF. This will help critical infrastructure owners and operators to identify gaps and mature their cyber and operational resilience practices.

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

There needs to be a simple, clear articulation to private sector partners of the obligations, duties and responsibilities once they have been defined, as well as implementation deadlines. Publicity around changes and requirements can be coordinated through the Technical regulator, as part of DCCEEW's National CER Roadmap

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

From a DER/CER view point, they are not, as mostly the industry does not see itself as critical infrastructure, although, as per the SOCI Act, aggregated fleets of DER/CER would form a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules.

3.5 Shield 5: Sovereign capabilities

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

The government's role would be to fund education, training and research.

The actual roles and requirements will be defined by the industry.

Research needs to be forward-looking, especially considering the impact of quantum computers and their potential decryption capabilities.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

Risk-based initiatives from industry to address potential threats and liabilities. So, a response to the changing threat levels rather than a proactive approach.

41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

Industries with transferrable skill sets would be IT support, telecommunications, finance, and government.
A workforce to provide transferable skills would be those including problem-solving, analytical thinking, communication, and attention to detail as these are crucial for a cybersecurity career.

Industries with Transferable Skills

- IT Support & Technical Fields: Roles in IT helpdesk, system administration, and software development provide hands-on experience with technical systems and problem-solving, directly applicable to cybersecurity functions.
- Finance & Banking: This sector requires a high degree of analytical thinking and attention to detail, especially concerning financial data and security, which aligns with the needs of risk assessment and threat detection in cybersecurity.
- Telecommunications: Experience with network infrastructure, data flow, and complex communication systems is a strong asset for understanding and defending networks.
- Government & Law Enforcement: Professionals in these sectors often have experience with regulatory compliance, security protocols, and critical data handling, making them a good fit for roles in national cybersecurity initiatives.
- Consulting: Strong communication, problem-solving, and strategic thinking skills developed in consulting are valuable for advising organisations on cybersecurity best practices and strategy.

Key Transferable Skills

- Problem-Solving: The ability to identify issues, analyse complex situations, and develop effective solutions is critical in cybersecurity.
- Analytical & Critical Thinking: Essential for analysing security threats, evaluating vulnerabilities, and making informed decisions about protective measures.

- Communication: Clear and concise communication is vital for explaining technical risks and solutions to both technical and non-technical stakeholders.
- Attention to Detail: Meticulous observation is required to detect subtle security anomalies and ensure the accuracy of security systems.
- Adaptability: The dynamic nature of cybersecurity requires a willingness to learn new technologies and adapt to evolving threat landscapes.
- Teamwork & Collaboration: Cybersecurity is a team effort; professionals must collaborate effectively with colleagues, other departments, and external partners.

By focusing on developing these non-technical and foundational technical skills, individuals from various industries can pivot their careers into a growing cybersecurity workforce.

42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?

Industry, academia, think tanks and government would best work together by analysing future threats from future technology. This way, collaboration can funnel into strategy both from a readiness perspective but also from a technology development one as well.

43. How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?

As identified, often academic cyber-related projects come from individual institutions and enterprises, and are often limited to short-term projects and grants. To address this, there should be an umbrella functioning and development pool, potentially funnelled through an entity like ARENA that has an overarching objective to connect investment, knowledge and people to deliver cyber innovation.

44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

The development of Australian technology should be the highest priority for sovereign capability. All other areas required for growth and development can be replicated and transferred overseas.

Technology can be defined as including hardware, software, policy, governance and capability.

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

The most concerning function of the concentration of Information and Communication Technology (ICT) infrastructure is the fact that the vast majority of all communication in Australia relies on the NBN. This means that a single point of failure can result in a total collapse of communication.

To mitigate such a risk there needs to be an alternative, and affordable means of communication that do not rely on either the NBN (nbn Co).

National Broadband Network (NBN) is now the legal owner of the fixed-line infrastructure, with NBN Co Ltd building and operating the network. While Telstra historically owned the copper-wire network, it was separated during the NBN rollout, and now NBN Co uses these lines. Additionally, Australia has three major mobile networks (Telstra, Optus, and Vodafone), which operate independently.

Fixed-line Network (Phones & Broadband)
NBN Co: The NBN is the legally owned, government-operated wholesale provider of the national broadband network.

Telstra's role: Telstra still owns some lines, particularly those in wireless and satellite coverage areas, and provides services to some customers. However, it also uses the NBN network like other providers.

Mobile Network
Three Major Networks: Telstra, Optus, and Vodafone each operate their own independent mobile network infrastructure.

MVNOs: Other smaller internet service providers (ISPs), known as mobile virtual network operators (MVNOs), but all of these use the networks of the three main carriers to offer their services.

3.6 Shield 6: Strong region and global leadership

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

SolarEdge does agree that the attributions, advisories and sanctions are effective tools for countering growing malicious cyber activity in the context of individuals and entities. When state-backed actors engage in cyber activity, such mechanisms could not be as effective.

Where state-backed actors operate via data harvesting through known devices and/or have access to critical infrastructure, such as DER/CER, there should be safeguards or limitations on such products to reduce risk. Furthermore, where such risks exist, there should be high conformance levels for cyber access imposed on products under a risk-based framework of access and control.

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cybersecurity?

The current engagements with Southeast Asia and the Pacific regions seem appropriate, assuming that momentum to continue to strengthen and coordinate the cyber incident readiness and response is ongoing and mutually supported.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

The current design and scope are appropriate.

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

Australia should have permanent representation within the IEC Standards committees to assist in the development of Standards and be able to support the direct or modified adoption into Australia.

The IEC provides cybersecurity standards, most notably the IEC 62443 series for industrial automation and control systems (IACS) and IEC 62351 for securing electrical networks. Additionally, the IEC collaborates on the ISO/IEC 27000 family of standards for information security management systems, which is a framework for managing information security risks in general.

<u>IEC 62443 Series:</u>
This is a family of standards specifically designed for the cybersecurity of Operational Technology (OT) and Industrial Automation and Control Systems (IACS).
It covers policies, processes, and controls across all stages of IACS, including manufacturing, deployment, integration, maintenance, and operation.

(Australia has already adopted this as the national standard, known as the AS IEC 62443, to protect critical infrastructure, although this is not called up for DER/CER aggregated fleets).

<u>IEC 62351:</u>
This standard focuses on securing the IT networks used for monitoring, controlling, and optimising power system operations, particularly within smart grid contexts.

ISO/IEC 27000 Family:
A collaborative effort with the International Organisation for Standardisation (ISO), this family provides a framework for managing information security risks across various organisations and industries.

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

The governance structure around regulation is a missing, yet fundamental requirement for domestic, as well as international cyber regulatory alignment.

Currently. Although cyber regulation and policy exist, it is very hard to find out what requirements should be applied and how meeting requirements are enforced or reported.

There needs to be much clearer information defining industry-specific requirements, specifically the DER/CER space and have a body in place to administer and enforce the requirements.

Thank you for the opportunity to provide input into the Consultation Paper. If you would like to have any further information or would like clarification to any of the points raised, please contact me directly to discuss.

Yours sincerely,

[redacted]

SolarEdge Technologies (Australia) PTY LTD.
[redacted]
Melbourne
VIC 3000
Australia