

Looking deeper into renewables supply chains

Supply chain mapping and vendor assessment under Australia's enhanced CIRMP Rules

THE COMPLIANCE QUESTIONNAIRE

Tier 1 OEM

Grid-scale BESS · nameplate vendor

- ✓ ISO 27001 certified
- ✓ IEC 62443 certified
- ✓ Not FOCI-implicated

THE SBOM / HBOM ANALYTICS

Cells + BMS firmware

L1

Sub-supplier signs & pushes updates

Cellular gateway module

L1

Third-party firmware · always-on link

Power conversion ICs

L2

Provenance in HBOM · no update path

Controller SoC

L3

Designed onshore · fabricated offshore



update channel

Introduction

Most vendor assurance in Australian energy today is a tick-box exercise. Is the OEM foreign-owned? Does it hold the right certifications such as ISO 27001 and IEC 62443? Has it signed the security schedule of the long term services contract? Those answers describe the company's back office processes, but say very little about what is running inside the turbine controller, the battery management system or the inverter, and who can make changes to these critical systems.

The international community has already provided us with a de-facto approach - the Software and hardware bills of materials (SBOMs and HBOMs) are now the common language between vendors and the organisations that rely on them, endorsed by Australia's own cyber agency. This paper argues that SBOMs and HBOMs are the practical way to meet the new supply chain obligations, and that they can deliver the deeper insight that is needed.

1 What the enhanced Rules actually require

The Rules set out two linked supply chain obligations: map your supply chain, and assess each of your major suppliers.¹ Both apply from **June 2028**. However, foreign ownership, control or influence (FOCI), and offshore or remote access to critical components, must be managed as material risks a year earlier, from **June 2027**.² An operator cannot manage a FOCI risk it has not identified. In practice, the mapping has to be well advanced before the first deadline, particularly if projects are early and in recent procurement processes.

SOCI REQUIRES THE CIRMP TO... ³	WHAT IT PRACTICALLY REQUIRED
Map the supply chain for <i>major suppliers and critical components</i>	A component-level inventory of every critical system, not a list of vendors
Identify supply chain risks to critical components and business-critical data	Knowledge of what each component contains, company and country of origin, and its vulnerabilities
Identify the maximum acceptable outage for the asset and its critical components arising from supply chain disruption	Operational tolerances, set against how long each supply path would take to recover if retired
Minimise or eliminate those risks, or mitigate an outage beyond the maximum acceptable outage	Spares, redundancy, recovery, rollback, restoration plans tied to hardware and software components
For each major supplier: the FOCI-related laws it is subject to, and sanctions or other impediments	Ownership and jurisdiction analysis, including for sub-suppliers inside the product
The <i>access, influence and control</i> the supplier has over the asset through its product or service	Which team pushes firmware, who holds remote access, which cloud services the asset depends on
Whether those together create a material risk or could exceed the maximum acceptable outage, and the steps to mitigate	A defensible link between each supplier, the components it touches, and the asset's tolerance for losing them

The expected response to a FOCI-implicated sole supplier is mitigation: contracts, remote-access restrictions, monitoring and contingency plans, all of which require knowledge of the components in detail. We examine FOCI assessment and mitigation in our companion paper, *Navigating FOCI rules in the renewables sector*.

Maximum acceptable outage calculations

The Rules define **maximum acceptable outage** as "the maximum period of time for which a critical component, service or any other thing for the CI asset can be unavailable without unreasonably disrupting the ongoing availability, integrity, reliability or confidentiality of the CI asset."⁴ It is used twice: once when setting tolerances for the asset and its critical components, and again when judging whether a major supplier could cause an outage longer than that tolerance.⁵

What is new is the requirement to connect it to the supply chain. Setting a tolerance is the easy half: the plant can run for six weeks without a spare battery module, or three months without its vendor's cloud monitoring service. The hard half is knowing how long each supply path would actually take to recover, and that depends on detail that never appears in a vendor questionnaire:

- **Spares and replacement:** which field-replaceable units are single-sourced, where they are made, and their lead time if a source is sanctioned, embargoed or simply fails.
- **Software and update dependencies:** which components depend on a vendor's update channel, licence server or cloud service, and what happens when that dependency is cut, whether by the operator in an incident or by the vendor.
- **Support and knowledge:** which components only the OEM, or an offshore support centre, can diagnose and repair.

Once that detail exists, the calculation itself is simple. For each critical component, compare the operational tolerance with the realistic time to recover through the supply chain. Wherever recovery takes longer than the tolerance, the CIRMP needs a treatment:

CRITICAL COMPONENT	SUPPLY DISRUPTION	MAX. ACCEPTABLE OUTAGE	TIME TO RECOVER	GAP	TREATMENT
BESS cell monitoring board	Single offshore source; shipment held under sanctions	6 weeks	16 weeks lead time + 4 weeks clearance = 20 weeks	-14 weeks	Hold spares on site; qualify a second source
Turbine controller	Fault only the OEM's offshore support centre can diagnose; remote link severed	2 weeks	Fly in an OEM engineer: 3 weeks	-1 week	Train and certify local technicians; hold configuration backups onshore
Plant monitoring (vendor cloud)	Service withdrawn, or cut off during a three-month CI Fortify isolation	13 weeks	No recovery without the vendor	Unbounded	Local historian and offline operating procedures

Illustrative figures. Each component is analysed and mitigations determined based on understanding of internal dependencies.

SBOMs and HBOMs are international best practice

A **software bill of materials** lists every software and firmware component in a product, with version, supplier and dependencies. A **hardware bill of materials** does the same for boards, processors, communications modules and power electronics, including manufacturer and country of origin. Together, they are the equipment's ingredients list.

In the past year they have become the expected baseline across allied jurisdictions:

- **2026 Minimum Elements for an SBOM** (29 July 2026), co-authored by CISA and 17 partner agencies including the ACSC. It covers firmware as well as software, requires transitive dependencies, and states plainly: *"There is no minimum depth."*
- **EU Cyber Resilience Act** (Regulation 2024/2847). From 11 December 2027, manufacturers placing products with digital elements on the EU market must maintain a machine-readable SBOM. Many of the OEMs that supply Australian renewables also sell into Europe, so they will be producing SBOMs regardless.
- **CISA HBOM Framework** (2023), which gives purchasers a consistent format and taxonomy for hardware component disclosure.
- **Two open international formats:** SPDX (ISO/IEC 5962:2021) and CycloneDX (ECMA-424). Both can represent firmware nested inside the hardware it runs on.

Due to the accelerated international adoption, one can only assume that Australia will fall into line with international best practice with SBOMs and HBOMs. That means that all major OEMs can be expected to provide these on demand for every released version of hardware and software.

An SBOM is a structured data file, not a report. This fragment of a CycloneDX SBOM describes one firmware component inside a battery system:

```
{
  "bomFormat": "CycloneDX", "specVersion": "1.6",
  "components": [{
    "type": "firmware",
    "name": "bms-controller",
    "version": "4.2.1",
    "supplier": { "name": "Example Cell Co." },
    "hashes": [{ "alg": "SHA-256", "content": "9f86d081884c7d65..." }],
    "purl": "pkg:generic/example-cell-co/bms-controller@4.2.1"
  }]
}
```

Every field can be read by a machine: who supplied the component, which exact version it is, and a cryptographic hash that must match the firmware actually installed.

4 Tick-boxes versus security-in-depth

The uplift from questionnaire assurance to bill of materials assurance is stark when seen side-by-side.

	VENDOR QUESTIONNAIRE	SBOM / HBOM
Nature of the evidence	Qualitative statements: "we follow secure development practices"	Quantitative data: every component, version, supplier and hash
How it is checked	Taken at face value, or audited by sampling	Checked automatically against the firmware itself
Currency	A point in time, usually annual	Updated with every release, monitored continuously
Vulnerabilities	A described patching policy	Each component matched against vulnerability feeds every day
Comparability	Free text, different for every vendor	One standard format across every vendor

A questionnaire can only ever be trusted on face value. An SBOM can be tested.

- **Integrity:** the hashes in the SBOM must match the firmware running on site, so substituted or tampered images stand out.
- **Completeness:** scanning the vendor's firmware image produces an independent SBOM, and comparing the two exposes anything undeclared, such as a third-party communications module or an outdated library.
- **Exposure:** once components are known precisely, matching them to new vulnerabilities is automatic, not a request to the vendor.

That is what suits it to FOCI: a vendor subject to foreign compulsion may answer a questionnaire honestly and still not control what it is told to ship. HBOMs are harder to check, since hardware needs inspection rather than a scan, but software and firmware, which carry the remote-update and remote-access risk the Rules focus on, can be verified at scale.

5 The mapping exercise

Building a credible supply chain mapping has three stages. In the first, the operator builds a component-level digital inventory of its own critical systems: each asset with vendor, product/model and version. In the second step, each vendor supplies its SBOMs and HBOMs, sub-component provenance, lifecycle and end-of-support data, and vulnerability position. In the third, there are reviews for independent FOCI assessments and maximum allowable outage periods.

The second and third phases are the most time consuming. Our working estimate is around ten analyst-days per vendor for a first-time mapping done largely by hand. FOCI-implicated vendors often require longer. For your first assessment, this can take between 2-6 months to properly assemble a deep mapping of your supply chain.

Two choices bring that down substantially;

- **Standard tooling:** most manual effort goes on converting spreadsheets and chasing missing fields, whereas machine-readable SBOMs and HBOMs can be validated, matched to vulnerability feeds and kept live as firmware changes.

- **Clear requirements on OEMs** evidence is per vendor not per operator, so a common format that is shared across many sites is the optimal outcome. That is the purpose of our openly licensed industry reference model.

Finally, capturing in contracts closes the loop. Supply and service agreements signed now for assets with 25-year lives should specify SBOM and HBOM delivery and maintenance, disclosure of embedded third-party firmware and its update channel, end-of-life notice, ownership-change notification and independent verification.

6 What to do now

- **Set maximum acceptable outages for critical assets.** Start with your key operational processes. Let your tolerances point to where supply chain depth matters most.
- **Build your component-level inventory.** If done from the design stage, this step is easy. Reconstructing an inventory from mapping the floor is a slow and arduous task without robust change control processes to make sure your inventory is known.
- **Ask every vendor for SBOMs and HBOMs in SPDX or CycloneDX formats.** Ask about embedded third-party firmware and who controls the patch update process. Ask all vendors, and not just those flagged as FOCI-implicated.
- **Treat attestations as inputs, not evidence.** Verify FOCI-implicated vendors' claims independently as an operator or via third party assurance.
- **Review the contracts you are signing this year.** Build bill of materials delivery and update-channel disclosure into every agreement now under negotiation.
- **Align with your sector peers.** Common vendor requirements lowers cost for all operators and OEMs alike, and is far easier to defend as "all reasonable steps" than twenty bespoke approaches.

The enhanced CIRMP Rules expect operators to know what is inside their critical systems and who could reach into them. Tick-boxes will produce an attestations. Bills of materials will produce insights. A detailed mapping exercise along with ongoing change control processes will allow for sound supply chain risk mitigation.

Notes

- 1 *Enhanced CIRMP Rules 2026* (LIN 26/075), s 10A: supply chain mapping at s 10A(2)–(3) and vendor assessment at s 10A(4)–(5).
- 2 s 6A(2)(b)–(d). The Rules give a 12-month grace period for s 6A (to 10 June 2027) and a 24-month grace period for s 10A (to 10 June 2028) for assets already in scope.
- 3 Rows follow s 10A(2), (3)(a), (3)(b), (3)(c), (5)(a)–(b), (5)(c) and (5)(d)–(e) in turn, paraphrased.
- 4 Inserted into the definitions in s 3 of the CIRMP Rules (LIN 23/006) by the *Enhanced CIRMP Rules 2026*.
- 5 s 10A(3)(b) and s 10A(5)(d) respectively.

References

- *SOCI Legislation Amendment (Enhanced CIRMP) Rules 2026* (LIN 26/075), ss 6A, 10A and Explanatory Statement; ASD, *CI Fortify*.
- CISA, ASD's ACSC et al., *2026 Minimum Elements for a Software Bill of Materials* (July 2026); *A Shared Vision of SBOM for Cybersecurity* (Sept 2025).
- EU CRA (Reg. 2024/2847), Annex I; CISA, *HBOM Framework* (2023); ISO/IEC 5962; ECMA-424.
- CAPA Intelligence, *Navigating FOCI rules in the renewables sector* (forthcoming).



ABOUT CAPA

CAPA Intelligence is an Australian based cybersecurity company servicing the global electricity / renewables sector, and global supply chains involved in supporting critical infrastructure. Our clients sit across the supply chain – governments, networks, retailers, system operators, IPPs, integrators and OEMs with operations in Australia and abroad.

CAPA Intelligence — Looking deeper into renewables supply chains

Contact info@capaintelligence.com
capaintelligence.com