Response to 2023-2030 Cyber Security Strategy Discussion Paper

Horizon 2 (2026–2028): Safer Connected Energy and Transport

Submission by : Solution Tech

SOLUTION TECH
SIMPLIFYING CYBER SECURITY

EXECUTIVE SUMMARY

- **Australia** is rapidly adopting electric transport and smart energy in homes, workplaces and public services.
- Connected devices enable this change but create pathways for remote misuse that can affect availability, privacy and safety.
- By 2028, our goal is safer products by default, clear labels that guide purchasing, reliable updates, and simple reporting of incidents.
- We recommend: (1) a targeted security baseline for named device classes; (2) a simple product label and purchasing preference; (3) safer setup and sign-in; (4) separation of control signals from general traffic; and (5) a dedicated, secure mobile service with special SIM profiles and an isolated network path for energy and transport devices (the “Secure Utility Device Network”).
- Secure Utility Device Network — a dedicated mobile service reserved for energy and charging devices so control signals do not traverse the public internet.

1. CONTEXT AND VERIFIED SCOPE

Government policy under Safe technology highlights devices at the edge of the internet and consumer energy resources in homes and businesses. Consumer energy resources include rooftop solar, household and community batteries, electric vehicles and charging stations. Internet connectivity introduces cyber risk that can disrupt energy systems.

This submission responds within that scope with practical, testable recommendations.

1.1 SCOPE BOUNDARIES

This submission addresses devices that (a) influence energy use, metering or charging outcomes and (b) are remotely accessible for monitoring or control.

- In scope: home energy gateways, smart meters, household/community batteries, public and high-capacity charging systems, and the home/small-business internet routers used to connect these devices.
- Out of scope: purely offline devices without remote management, and general consumer gadgets unrelated to energy or charging.

2. THE PROBLEM AND ITS IMPACT

- Weak default settings and poor update practices create unnecessary exposure at the edge of the network and grid.
- Misuse can switch systems off, tamper with usage data or interfere with control signals that manage energy flows and charging.
- Incidents raise costs, erode trust and can disrupt essential services.

2.1 RISK SCENARIOS AND CONTROL MAPPING [PROPOSED]

Scenario	Likelihood / Impact	Primary controls
Mass remote misuse via stolen cloud or installer credentials	Medium / High	Extra confirmation at sign-in; unique device identity; deny-by-default gateways; rapid revocation

Household gateway takeover via weak defaults	Medium / Medium	Safe defaults; encrypted management only; owner binding at setup; automatic signed updates
Public charger control-plane exposure via mixed networks	Low / High	Dedicated secure mobile service; accredited endpoints only; isolated path; performance and recovery testing

3. OUTCOMES SOUGHT BY 2028

1. Safer products out of the box with secure settings on by default.
2. Clear labels to help households, businesses and operators choose safer products.
3. Trustworthy, prompt updates with published support periods.
4. Simple, single national portal for incident reporting and guidance.
5. Higher resilience across public charging and home energy through protected control paths.

4. DEVICE CLASSES IN SCOPE

- Home energy gateways that link rooftop solar, batteries and the grid.
- Smart meters used by households and small businesses.
- Household and community battery systems.
- Public and high-capacity vehicle charging systems.
- Home and small business internet routers used for these devices.

5. PROPOSED: SECURE UTILITY DEVICE NETWORK (DEDICATED SIM + DEDICATED MOBILE SERVICE)

This is a new policy proposal designed to meet Horizon 2 objectives using established telecommunications building blocks.

5.1 PURPOSE

Create a dedicated, secure mobile service solely for devices that control energy and charging. The service uses special subscriber identity modules(SIM) and an isolated network path so control signals do not traverse public internet pathways.

5.2 ARCHITECTURE AND CONTROLS

Layer	Design choice	Security control
Access	Private access path or logically isolated slice(path) on modern mobile networks	Traffic kept off public internet; deny incoming internet connections
Identity	Embedded subscriber identity module with remote provisioning; unique identity per device	Cryptographic verification; rapid revocation
Session	Mutual authentication before any command or telemetry	Strong encryption; replay protection
Routing	Gateways limited to accredited endpoints only	Deny-by-default firewall policies

Operations	Continuous monitoring of control traffic; anomaly detection	Fast suspension for compromised devices or installers

5.3 IMPLEMENTATION OPTIONS

Option	Description	Advantages	Considerations
Accredited private access service	Carrier-hosted private access with routing to accredited gateways.	Available on current networks; national reach.	Multiple carrier integrations; consistent policy needed across providers.
Isolated utility slice(path)	Logically isolated slice with service levels suited to control traffic.	Stronger isolation and telemetry; performance guarantees.	Depends on carrier capability and agreements.
Government-backed specialised service	Government-accredited mobile service or virtual operator for national coverage.	Uniform identity policy and incident response; procurement leverage.	Requires governance, accreditation and wholesale arrangements.

5.4 OPERATOR MODEL AND ACCREDITED ENDPOINTS [PROPOSED]

Carriers provide dedicated service; a government-appointed accreditation body approves carriers, gateway operators and device makers.

Accredited endpoints are cloud services and network gateways that publish ownership and location, implement baseline controls, undergo periodic audit, and support immediate certificate/key revocation. Gateways enforce an allow-list of accredited endpoints and block all others.

5.5 ONBOARDING AND LIFECYCLE (STEP-BY-STEP)

1. Accredit carriers and gateway providers against minimum technical and security benchmarks.
2. Register device makers and licensed installers; issue installer credentials tied to verified identity.
3. Provision an embedded subscriber identity module profile with a unique device identity at manufacture or installation.
4. Bind the device to its owner during setup; record support period and responsible party.
5. Enforce mutual authentication: device and service verify each other before any command or telemetry.
6. Restrict routing to accredited endpoints; block any other destinations.
7. Operate continuous monitoring; suspend identities quickly if compromise is suspected.
8. Support secure ownership change: revoke old identity and issue a new one with an audit trail.

5.6 FALLBACK FOR NON-CELLULAR DEVICES [PROPOSED]

Where devices lack a mobile radio, manufacturers must provide one of: (a) a pre-configured add-on cellular gateway enrolled on the dedicated service; or (b) a one-step “Energy Devices” home network join flow that requires no router configuration by the owner and still enforces allow-listed endpoints.

5.7 GOVERNANCE, PRIVACY AND ASSURANCE

- National accreditation scheme with periodic audits for carriers, gateways, device makers and installers.
- Minimum data collection and clear retention periods; publish privacy settings of the dedicated service.
- Independent oversight with annual public reporting on performance and incidents.

5.8 INDICATIVE COST AND FUNDING LEVERS

Cost category	Examples	Potential funding lever
Network service	Private access, slice management, monitoring	Tiered wholesale pricing; public procurement commitments
Device identity	Subscriber profiles, secure elements, provisioning	Volume-based pricing; grants for small makers
Gateways	Accredited routing, inspection, logging	Shared national gateways to reduce duplication
Implementation	Accreditation audits, installer onboarding	Vouchers and training support for small providers

5.9 COMPETITION AND NEUTRALITY GUARDRAILS (PROPOSED)

Accreditation shall be multi-provider. Identities must be portable between accredited carriers. Gateways implement open, published interfaces; logs are exportable. Wholesale pricing must be non-discriminatory; disputes escalate to the accreditation body.

6. SECURITY BASELINE FOR NAMED DEVICE CLASSES

The baseline below complements the dedicated service. It applies to devices whether connected via the dedicated service or a general network.

Control area	Requirement	Evidence of conformance
Identity and access for people	Extra confirmation at sign-in for any management portal.	Demonstrate sign-in flow and recovery process.
Identity for devices	Unique, cryptographic identity per device; no shared credentials.	Show certificate issuance and revocation records.
Onboarding and binding	Bind device to owner during setup; revoke and re-issue identity at ownership change.	Installer log and ownership change log.
Software updates	Signed updates with automatic install and rollback; publish security fix timelines.	Update manifest and protection of signing keys.

Secure communication	Encrypt command and telemetry; disallow plain-text protocols; restrict destinations.	Packet capture evidence; firewall rules.
Safe defaults	Disable debug and unused services; no open management from the internet.	Factory configuration; port scan results.
Logging and transparency	Keep minimal, useful logs; provide owner access without exposing private data.	Log retention policy and access view.
Support lifecycle	Publish support end-dates and patch timeframes; notify ahead of end of support.	Public notice and customer communications.

6.1 MINIMUM THRESHOLDS [PROPOSED]

- Critical security fixes applied within 30 days of disclosure; high within 60 days; medium within 90 days.
- Device identity keys must be hardware-protected; certificates rotated at least every 24 months.
- All command and telemetry uses encrypted transport; no plain-text management.
- Factory defaults must not include shared passwords; all remote management is closed until owner binding completes.

7. SAFER SETUP AND SIGN-IN

1. People: add an extra confirmation step for any account that can control devices; use a one-time code delivered out-of-band.
2. Devices: refuse management until identity is verified against the service; block direct access from the public internet.
3. Ownership change: require a secure handover that revokes old access and issues a new identity with an audit record.

7.1 RECOVERY AND DELEGATION [PROPOSED]

- Account recovery requires two independent proofs (for example, device-present confirmation plus verified contact).
- Delegated access allows time-bound or role-bound access for installers/operators; all delegations are logged and revocable by the owner.
- Owner can revoke all delegated access in one step.

8. SEPARATION OF CONTROL SIGNALS — DECISION RULE AND APPLICATION

If a device has a built-in mobile modem: enroll on the dedicated secure mobile service. If not: use a pre-configured add-on gateway on the dedicated service; failing that, the zero-touch “Energy Devices” home network path must be used. Control signals should not traverse general home browsing paths.

8.1 PRACTICAL APPLICATION

- Public and operator-run systems (mandatory): devices use the dedicated secure mobile service and are not reachable from the public internet. Management occurs through accredited gateways only.

- Homes and small businesses (zero-touch): internet providers and router makers pre-create a protected “Energy Devices” network in router firmware. Owners do not configure anything; devices join via one step (scan code or app), and the router silently enforces allow-listed endpoints.
- Where an ISP router cannot yet auto-create the Energy Devices network, manufacturers supply a pre-configured add-on cellular gateway enrolled on the dedicated service. Owners do not configure the router.
- Devices with a built-in mobile modem: if on the dedicated secure mobile service, no home network separation is required.
- Gateways (all cases): route only to accredited endpoints by default and block all other destinations.

9. PRODUCT LABEL AND PURCHASING SIGNALS

Label element	Purpose	Where shown
Baseline met	Signals that the device meets the national baseline.	Packaging and online listings.
Support period	Shows end-date for security updates.	Packaging and online listings.
Setup checklist	Gives owners the first five actions to stay safe.	Inside the box and online.
Privacy notice	States data collected and retention.	On-device setup and online.

9.1 VERIFICATION AND LOOKUP [PROPOSED]

Each label displays a Conformance ID verifiable via a public registry showing model, firmware branch, support end-date and audit status. Recall notices automatically flag in the registry and in the device companion app.

- Maintain a public list of conforming models to support purchasing and recalls.
- Use public purchasing to prefer products that meet the baseline.

10. GOVERNANCE AND ALIGNMENT WITH EXISTING OBLIGATIONS

The approach aligns with critical infrastructure risk management principles and current telecommunications security rules. Dedicated services and baselines can be recognised as controls in risk programs and vendor contracts.

10.1 ACCOUNTABILITY MAP [PROPOSED]

Function	Responsible	Accountable	Consulted	Informed
Baseline and label	Standards team	Minister or delegate	Industry; consumer groups	Public
Dedicated service accreditation	Accreditation body	Government agency	Carriers; gateway providers	Public

Market surveillance	Regulatory team	Regulator	Standards team; accreditation body	Public
Incident portal	Operations team	Lead department	Energy and communications regulators	Public

10.2 Regulatory levers (decision options)

Government may adopt one of three levers: *Option A (Voluntary code + label)*, *Option B (Co-regulatory with trigger at <60% label penetration by end-2027)*, or *Option C (Mandatory standard from 2028 for new models)*. The trigger moves market signals into enforceable minimums if voluntary uptake stalls.

11. IMPLEMENTATION TIMELINE (2026–2028) — GATES AND DEPENDENCIES

Year	Gate	Activities
2026	Pilots achieve ≥ 99.5% control-path availability and ≤ 30 days median patch time	Publish final baseline/label; open accreditation; pilot reports
2027	≥ 60% of new in-scope models labeled; ≥ 2 carriers accredited; incident portal live	Mandate label for all new models; national onboarding playbook
2028	≥ 85% of new models labeled; national dedicated service coverage	Enforcement; annual public reporting

12. MEASURES OF SUCCESS — TARGETS AND MEASUREMENT METHOD

Measure	Target	Method
Label penetration (new in-scope models)	60% in 2027; 85% in 2028	Market sampling; registry data
Patch latency (median days to deploy fixes)	≤ 30 days for critical	Vendor reports; audit sampling
Exposed control planes (findings per 10k devices)	Downward trend ≥ 30% per year	Routine scans; pilot telemetry
Small-business readiness (coverage of eligible sites)	≥ 50% by 2028	Voucher uptake; survey

12.1 MEASUREMENT GOVERNANCE

Label share measured by an independent evaluator via market sampling and registry reconciliation;

patch latency by vendor attestations audited quarterly; exposed control planes via independent scanning with a responsible disclosure process.

13. PILOT PROJECTS — ACCEPTANCE CRITERIA AND TELEMETRY

13.1 PUBLIC CHARGING PILOT

- Scope: ten diverse sites across metro, regional and remote areas.
- Method: dedicated secure mobile service; device identity end-to-end; performance and recovery testing under load and during faults.
- Acceptance criteria: meets availability and patch-latency thresholds; no critical control-path exposure in independent testing.
- Telemetry to collect: onboarding success rate; update success/failure; time-to-revocation; anomaly-detection false positives/negatives; support tickets.
- Time to commission a charger and clarity of the site operator guide (1 to 5 scale).

13.2 HOME AND SMALL BUSINESS ENERGY PILOT

- Scope: mixed households and small businesses with solar, battery and charging devices.
- Method: baseline trial; separate control paths; owner and installer checklists; privacy review.
- Acceptance criteria: adoption of safe defaults; timely updates; high-quality incident reports.
- Telemetry to collect: configuration compliance, update cadence, incident reporting quality.
- Time to set up the gateway and clarity of the household guide (1 to 5 scale).

13.3 SMALL BUSINESS SUPPORT PILOT

- Scope: three regions with different provider mixes.
- Method: vouchers for setup and ongoing care; templates and hands-on help via accredited providers.
- Acceptance criteria: readiness scores reach agreed threshold; time-to-resolve decreases.
- Telemetry to collect: readiness scores; mean time to resolve; participant satisfaction.
- Time from first booking to safe operation and clarity of the owner checklist (1 to 5 scale).

14. KEY RISKS AND MITIGATIONS

Risk	Mitigation
Fragmentation across providers	National accreditation and a common policy for dedicated service and labels.
Cost burden for small suppliers	Phased timelines; shared gateways; support vouchers.
Vendor lock-in	Open standards; portable identities; published exit processes.
Privacy concerns	Collect minimum data; publish retention periods; independent oversight.
Dedicated service outage or market exit	Multi-carrier profiles; roaming arrangements; escrowed gateway configs; mandated 90-day migration window.

WE WELCOME YOUR CONTACT

We are available to discuss this submission.

[redacted]