CSIP-AUS and 2030.5 Cybersecurity Review

Document Owner: CAPA Intelligence

Date: 31 Jul 2025

Disclaimer

 This project received funding from the Australian Renewable Energy Agency (ARENA) as part of ARENA's Advancing Renewables Program.

About CAPA Intelligence

CAPA Intelligence is a technology company focused on cyber defence and operational intelligence for electricity utilities and the global renewables supply chain. CAPA builds advanced tools that monitor, detect, and respond to cyber threats targeting fleets of distributed energy resources, helping operators secure complex, decentralised energy infrastructure.

Abbreviations

AMI	Advanced metering infrastructure
ACCC	Australian Competition and Consumer Commission
CSIP	Common Smart Inverter Profile
CSIP-AUS	Common Smart Inverter Profile - Australia
DERIAPITWG	DER Integration API Working Group
DER	Distributed energy resources
DNSP	Distribution network service provider
DNS	Domain name system
EV	Electric vehicle
EXI	Efficient XML interchange
XML	Extensible markup language
GUID	Globally unique identifier
HEMS	Home energy management system
HTTPS	Hypertext transfer protocol secure
IT	Information technology
ISC	Interoperability Steering Committee
LOR2	Lack of reserve 2
LFDI	Long form device identifier
NEM	National Energy Market
NEPKI	National Energy PKI
OCPP	Open Charge Point Protocol
OT	Operational technology
PEN	Private enterprise number
PKI	Public key infrastructure
SOCI	Security of Critical Infrastructure Act 2018
SSRF	Server-side request forgery
SEP2	Smart Energy Profile
SBOM	Software bill of materials
SAN	Subject alternative name
TCP	Transmission control protocol
TLS	Transport layer security
URI	Uniform resource identifier
URL	Uniform resource locator
VPP	Virtual power plant
WEM	Wholesale Energy Market

1 Executive Summary

The Common Smart Inverter Profile – Australia (CSIP-AUS) is a national specification for bidirectional communication between distributed energy resources (DERs) and electricity networks, retailers or other parties that may want to manage the operation of DER.

It has been adopted widely throughout Australia with respect to small scale solar and batteries in flexible export and emergency solar backstop programs, and nascently in virtual powerplant (VPP) orchestration. By 2030, there will be close to 10GW of residential rooftop solar installed which utilises the CSIP-AUS protocol.

This cybersecurity review of CSIP-AUS and its associated operational infrastructure aims to identify what is required for CSIP-AUS to be used in a cybersecure manner as the volume of DER under management scales. It defines the cybersecurity risks that implementations of CSIP-AUS can pose to consumers and the power system, best practices for CSIP-AUS clients and servers to operationally mitigate these risks and cybersecurity improvements that can be made to the standard and supporting functions over time.

CSIP-AUS represents an important step in standardising DER integration in Australia. As an implementation guide for IEEE 2030.5 (sometimes referred to as the Smart Energy Profile 2.0 (SEP2)) it inherits design decisions and specifications from this standard. While some of the original use cases for SEP2 or earlier versions of the standard were focussed on simpler management of smart energy devices often in localised private networks, CSIP-AUS is being applied towards the secure control of large fleets of DER through public internet communications. CSIP-AUS carries forward some assumptions and constraints from IEEE 2030.5 that are undesirable, and many modern cybersecurity features and robust design patterns that are industry best practice are underdeveloped.

In the short term there are many actions and controls that can be implemented by operators and vendors of CSIP-AUS technologies to mitigate these cybersecurity weaknesses in CSIP-AUS and improve the security of the CSIP-AUS ecosystem. These are outlined in chapter 4.

Over time the CSIP-AUS specification and associated documentation and infrastructure will require uplift to have cybersecurity considerations proportionate to the growing fleet size of assets utilising the specification. This uplift will take multiple years to implement and therefore work must begin now to be implemented as fleet sizes grow. If issues identified are not addressed within appropriate timeframes the risk profile will increase, potentially exposing critical systems to vulnerabilities at greater scale. Chapter 5 outlines

recommendations for CSIP-AUS uplift, identifying short-term opportunities to make small changes and larger opportunities when considering more fundamental changes to the specification in the future.

The areas identified in the report that are opportunities for uplift are:

- **Public Key Infrastructure (PKI)**. Significant uplift in capability of the PKI for securing CSIP-AUS communications is recommended to reflect industry best practice. This includes the ability to refresh and revoke certificates, hardening the certificates used for utility servers, and decoupling identity from operational certificates. The National Energy PKI (NEPKI) may be a suitable body to oversee this work.
- **Access Control**. More clarity in the standard and associated testing to ensure that clients can only access resources that they are scoped to.
- **The Subscription/Notification function set**. These functions require the server to interact with arbitrary URIs set by the client, which presents risks of resource exhaustion and server-side request forgery. To increase the security of this function set, changes to URI registration, validation and sanitisation are recommended.
- **Server and Client State**. 2030.5 and CSIP-AUS has inherently a stateful protocol where data is exchanged, such as telemetry, depend on prior context. This creates cybersecurity weaknesses through decoupling client and server state. These risks can be mitigated through close monitoring or limiting state changes in the short term and moving to a more stateless protocol in the long term.
- **Registration and Testing**. There are opportunities to collect more detailed information on organisations, devices and systems to improve the security of CSIP-AUS. This includes when organisations such as aggregators register with utility sever operators and provide information about their organisation, devices during the site commissioning process, and during server and client testing processes.
- **Cybersecurity Governance.** Formalised disclose policies and vulnerability management working groups related to CSIP-AUS allow appropriate notification and remediation of vulnerabilities discovered by researchers and industry.
- **Threat Detection and Incident Response**. Many weaknesses are related to details inherent in the CSIP-AUS protocol and are challenging to mitigate in the short-term. Tailored threat detection and incident response processes provide an opportunity to mitigate these risks while these changes are enacted over the coming years.

There is a risk analysis of many of these areas in chapter 3.5 and summaries of mitigations and recommended uplift in appendix A and appendix B.

While there are weaknesses in the CSIP-AUS specification and associated operational infrastructure, there are immediate mitigations and opportunities to uplift the ecosystem over time to limit these weaknesses. As the rollout of CSIP-AUS in Australia scales, prioritising consistent security improvements will ensure that there is a cybersecurity posture proportional to the level of uptake of the specification.

Table of Contents

2 Introduction

The Common Smart Inverter Profile – Australia (CSIP-AUS) is a national specification for bidirectional communication between distributed energy resources (DERs) and electricity networks, retailers or other parties that may want to manage the operation of DER.

It has been adopted widely throughout Australia with respect to small scale solar and batteries in flexible export and emergency solar backstop programs, and increasingly in virtual powerplant (VPP) orchestration.

The implementation of the standard in Australia enables the efficient management or control of a large number of devices and aggregate capacity to the benefit of consumers and the grid. With that opportunity comes a threat of these systems being used maliciously to create local or system wide issues on the power system.

CAPA Intelligence estimates, using Clean Energy Regulator commissioned solar uptake projections[1] and estimated dates of solar emergency backstop of flexible export implementations, that over 1GW of nameplate solar capacity will be managed using CSIP-AUS in 2026, increasing to almost 10GW by 2030. Commercial solar, batteries and other DER would further increase the total amount of capacity under management.

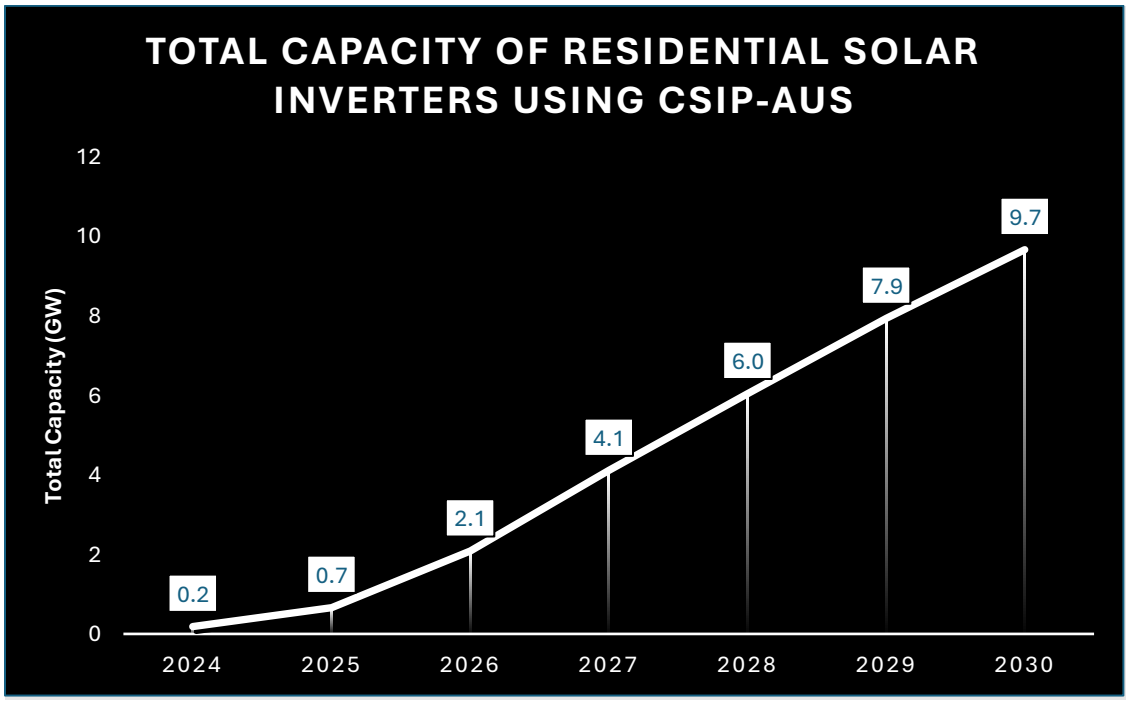

Figure 1 Estimated residential solar uptake of CSIP-AUS

[1] https://cer.gov.au/document/stc-modelling-report-jacobs-august-2024

This cybersecurity review of CSIP-AUS and its associated operational infrastructure aims to identify what is required for CSIP-AUS to be used in a cybersecure manner, as the volume of DER under management scales. It defines the cybersecurity risks that implementations of CSIP-AUS can pose to consumers and the power system, best practices for CSIP-AUS clients and servers to operationally mitigate these risks and cybersecurity improvements that can be made to the standard and supporting functions over time.

This report is broken up into four main sections:

CSIP-AUS Cyber Risk Profile outlines the history and use of CSIP-AUS, threat actors who would have an interest in using CSIP-AUS as part of a cybersecurity attack and the potential impacts of those attacks, a vulnerability assessment of weaknesses in the protocol and implementations of CSIP-AUS that an attacker could leverage, and a risk assessment of these weaknesses.

Cybersecurity mitigations for CSIP-AUS servers and clients documents cybersecurity mitigations to increase the security of the CSIP-AUS ecosystem. These recommendations don't require changes to the protocol or the overall implementation of CSIP-AUS, meaning that individual organisations implementing CSIP-AUS infrastructure can apply these mitigations immediately.

Recommendations for CSIP-AUS cyber development and uplift includes ways to increase the security of the CSIP-AUS protocol and broad industry implementation of CSIP-AUS over time. It includes short term recommendations that could be implemented over the next 1-3 years in minor version updates to CSIP-AUS or minor changes to implementation of the standard, and longer-term recommendations that could be implemented in major version updates to CSIP-AUS or reforms to supporting infrastructure approaching 2030.

Existing work related to CSIP-AUS Cybersecurity covers current groups or projects related to cybersecurity development or uplift in the Australian ecosystem. This provides context on related work underway.

3 CSIP-AUS Cyber Risk Profile

3.1 CSIP-AUS context

CSIP-AUS is a guide that describes how to implement the standard IEEE 2030.5-2018 in Australia. The CSIP-AUS guide outlines the parts of 2030.5 it uses with some changes, extensions and clarifications to make it suitable for Australia.

IEEE 2030.5 has a long history. In 2008 the Zigbee Smart Energy standard was published. This focused on sending messages within the home or a neighbourhood to smart appliances, in home displays and electricity meters. This standard supported devices with low powered compute resources with limited internet access within the context or a closed private network.

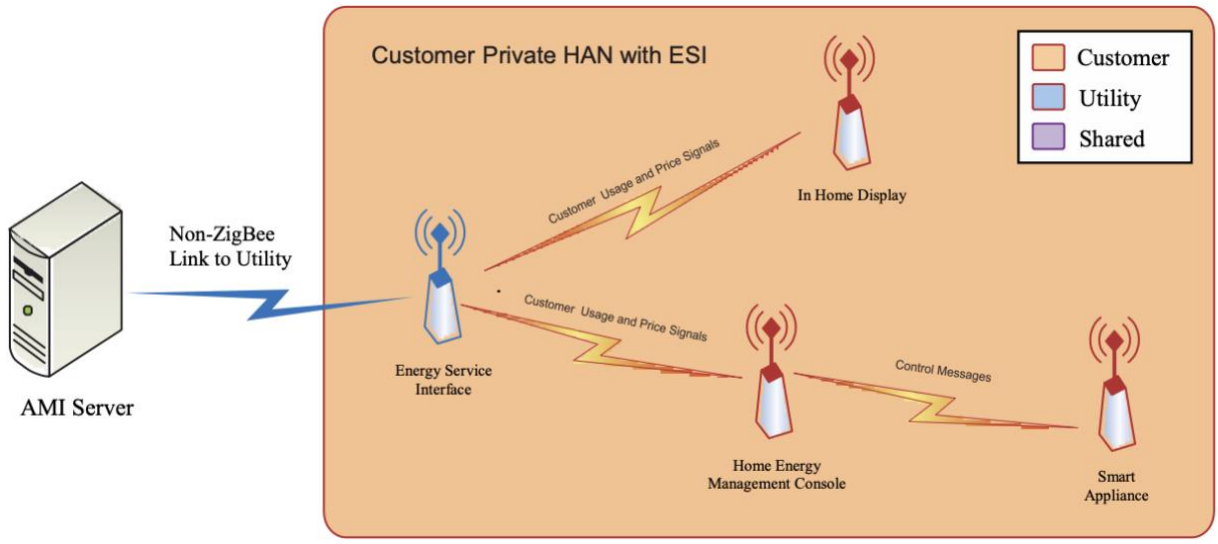

Figure 2 Example of communication with Zigbee Smart Energy within a home area network. Source: ZigBee Smart Energy Standard[2]

In 2013, the Smart Energy Profile 2.0 (SEP2) was published. This broadened the standard to use communication protocols and functions other than ZigBee, which enabled it to be used to communicate with devices over the internet through a range of connectivity types (e.g. Wi-Fi, ethernet, cellular). This allowed utilities to consider using this standard for remotely controlling distributed energy resources and formed the core of IEEE 2030.5 which was a formalisation of the standard for worldwide in 2013.

[2] https://zigbeealliance.org/wp-content/uploads/2019/11/docs-07-5356-19-0zse-zigbee-smart-energy-profile-specification.pdf

IEEE 2030.5-2018 was a 2018 update which included clarifications and enhanced functionality to the standard to support remote inverter control such as ramp rates and grid support functions (e.g. volt-var, volt-watt, etc) and updates to provide clarifications to the standard where there were ambiguities.

The CSIP-AUS implementation guide was published in 2021, which adopts large parts of the 2030.5-2018 standard in a similar manner to California's Common Smart Inverter Profile (CSIP)[3] with certain extensions such as the support of dynamic import and export limits.

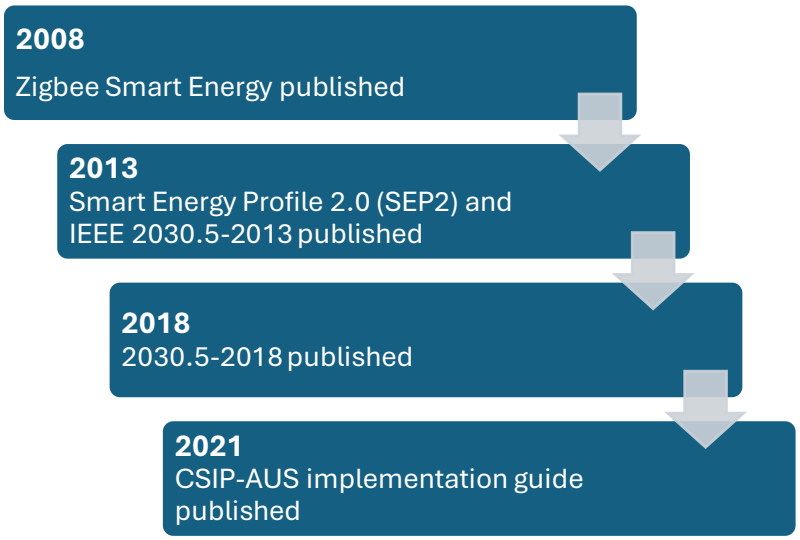

Figure 3 Evolution of the smart energy standard

CSIP-AUS represents an important step in standardising DER integration in Australia. As an implementation guide for IEEE 2030.5 (SEP2) it inherits design decisions and specifications from this standard. While some of the original use cases for SEP2 or earlier versions of the standard were focussed on simpler management of smart energy devices often in localised private networks, CSIP-AUS is being applied towards the secure control of large fleets of DER through public internet communications. CSIP-AUS carries forward some assumptions and constraints from IEEE 2030.5 that are undesirable, and many modern cybersecurity features and robust design patterns that are industry best practice are underdeveloped.

Over the evolution from Zigbee SEP to 2030.5, improvements were made to the architecture and security of the standard to support the remote operation and

[3] https://sunspec.org/common-smart-inverter-profile-csip/

communication to fleets of DER. This section of the report highlights vulnerabilities and weaknesses in the protocol which remain, with later sections of the report outlining how they can be mitigated now and strengthened in the future.

3.2 Asset Ecosystem of CSIP-AUS

CSIP-AUS involves utility servers and clients communicating with each other.

Utility servers register and store state about the client, can send instructions or configuration settings and receive telemetry and other information from clients. In Australia, servers are run by distribution network service providers (DNSPs) in the east coast to set export limits or limit on-site generation for DER on their network, and Synergy in Western Australia for setting limits and VPP operation of DER. In the future others may use utility severs to connect to CSIP-AUS clients to set limits or orchestrate fleets of DER.

Clients register themselves and their capability with severs, receive instructions and settings and send back telemetry or other information from DER.

Clients can connect to DER in a variety of ways:

- **Direct-to-device**: The CSIP-AUS client operates on the DER itself, such as inbuilt into an inverter. Here the CSIP-AUS signal terminates at the DER device itself, and the manufacturer has full control of the CSIP-AUS client and device.
- **HEMS-to-device**: The CSIP-AUS client operates in a home energy management system (HEMS[4]). The HEMS then connects to the DER through a local communication protocol such as SunSpec modbus and must translate the CSIP-AUS messages into another control protocol for the hardware to enact. Often the HEMS and DER are made by different manufacturers, and the HEMS has limited connectivity or control of the DER.
- **Cloud-to-device**: The CSIP-AUS client operates in a data centre which is remote from the DER. The CSIP-AUS signal terminates in the data centre environment and the CSIP-AUS message is translated into an alternative protocol (often proprietary) which is then sent to the DER over the internet.

[4] HEMS is referred to as GFEMS in CSIP and CSIP-AUS

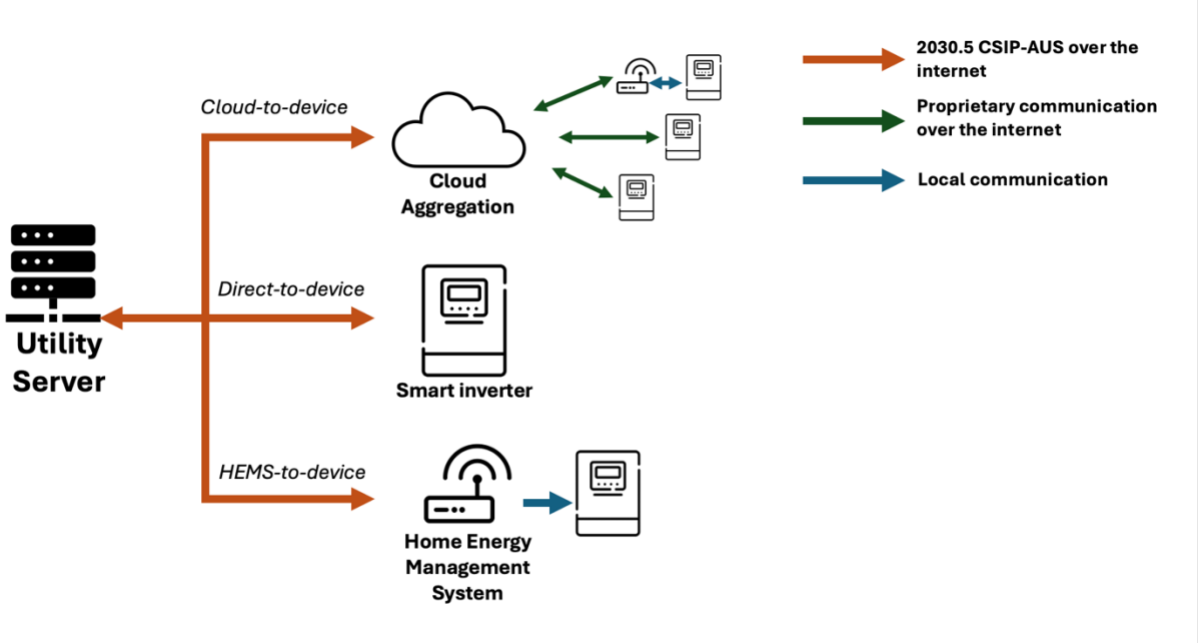

Figure 4 CSIP-AUS utility server to device domain

These multiple options for control paths present challenges to the security and reliability of CSIP-AUS infrastructure. Such as:

- **Parts of the control path are out of band to CSIP-AUS**, such as HEMS and cloud aggregation methods. This presents challenges for ensuring reliable and consistent implementation of CSIP-AUS instructions. This also can make it difficult for the server to understand what is occurring at the device level, or between the device and client, and client to understand what is happening at the device level.
- **A third party can be between the utility server and DER device** in the control path. An example of this is a cloud aggregator or HEMS which is a different company to the manufacturer of the DER.
- **CSIP-AUS message payloads aren't explicit which connection method the client is using**, and therefore it can be difficult for a CSIP-AUS server to understand what type of client is connecting (e.g. HEMS-to-device or direct-to-device).

A further challenge is that DER devices are accessible outside the CSIP-AUS protocol to manufactures or technology providers for control and software update purposes. This becomes a higher risk for entities under the Security of Critical Infrastructure Act 2018 (SOCI) compliance.

Additionally, operators of utility servers implementing CSIP-AUS are typically critical infrastructure operators, such as electricity networks or gentailers (retailers that also operate large generators). These servers often interface, directly or indirectly, with critical systems such as Advanced Metering Infrastructure (AMI) and Distributed Energy Resource Management Systems (DERMS), making them part of the broader critical infrastructure environment.

At the same time, CSIP-AUS clients that operate on HEMS or DER exist in untrusted environments. They are widely distributed in homes, often contain the certificates and credentials that authenticate them to CSIP-AUS servers and may be exposed to physical tampering or compromise via local networks. This creates a distributed attack surface where a compromise of a single client can potentially be leveraged to access or disrupt critical systems in the utility's control environment or other CSIP-AUS clients.

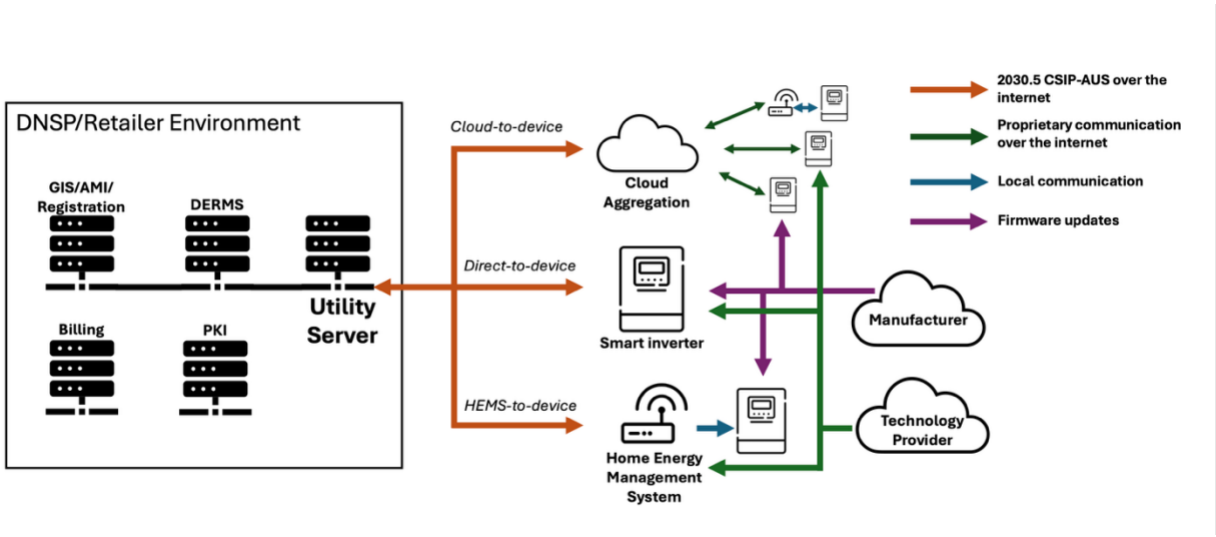

Figure 5 DER and utility operational ecosystem

To mitigate some weaknesses introduced by this complex architecture and multiple trust environments, it's essential that:

- Server operators have strong registration and asset inventory to understand how CSIP-AUS clients are connected to downstream DER, what that downstream DER is and who is in the control path.
- Server operators have some understanding of actors who can influence large amounts of DER out of band, and when they apply that influence (e.g. widespread firmware updates).

- Certificates and key material stored on devices are adequately protected. Notably, CSIP-AUS does not currently require the use of secure elements and disk encryption for device credentials.

3.3 Threat Landscape

3.3.1 Impact of attacks on CSIP-AUS infrastructure

A feature of implementations of CSIP-AUS is it facilitates the ability of utility server operators and aggregators to influence the output or directly control large fleets of DER devices. These fleets of DER devices are growing large enough to materially impact and change behaviour to the bulk power system.

This is by design, for instance when the operational demand of the power system is below a safe operating level, being able to reduce the output of rooftop solar by a gigawatt (or multiple gigawatts in the late 2020s) leads to positive outcomes. In contrast, reducing the output of solar by gigawatts during the second day of a heatwave when a lack of reserve 2 (LOR2) event is in progress leads to poor outcomes such as widespread blackouts. If this reduction in solar output during a heatwave were part of a cyberattack, power system operators to would need to understand the depth and persistence of the attack and any damage or impairment of digital infrastructure that could introduce complexities in restoring power, impacted DER devices and digital infrastructure to a safe operating state.

While not exhaustive, below are some examples of the impact that attackers may seek when attacking CSIP-AUS infrastructure:

Denial of control: When there is a loss of communication between CSIP-AUS clients and servers, the clients are required to fallback over time to a default operating state. For example, it's common for solar systems to fallback to a zero-export limit.

There are many ways an attacker could impair the communication between client and server, for example, a denial of server attack on the server, disabling the server or changes to databases. In these scenarios, the attacker gains indirect control of the solar inverters connected to this utility server, as they will deterministically fall back to this default operating limit.

In the case this default operating limit is zero-export for solar inverters, that could cause a large reduction of solar generation on the power grid. If this is during a time that solar generation was relied on, then power system security issues could emerge.

Manipulation of control: By taking over or impersonating a utility server or aggregator, an attacker may gain control over large fleets of DER. If the DER fleet is large enough, it could be operated in ways that cause power system security issues. Additionally, the attacker could make it difficult to recover the systems to a safe and consistent operating state.

Loss of productivity and revenue: Maliciously impacting the control of fleets of DER could cause a financial loss to individuals or broader power systems users. This could put increased pressure and confusion on operators of CSIP-AUS systems compromised by attackers.

3.3.2 Threat actors

3.3.2.1 Ransomware Actors

CSIP-AUS implementations may be of particular interest to a ransomware actor due to the high level of pressure a ransomware attack could put on the target of an attack to quickly pay the ransom to restore operational control.

If a ransomware actor were able to compromise a utility server, aggregator client or PKI infrastructure, they would gain a powerful ability to control the devices connected to that server or client such as switch off or disable a large number of rooftop solar systems. This could lead to a multi-directional crisis for the utility server or aggregator client to handle, with issues such as:

- Causing immediate and widespread financial loss to the owners of those systems who can no longer generate power.
- Overwhelming customer support lines and damaging the organisation's public trust.
- Threatening power system security if these ransomware attack occurs at a time that the grid is under stress such as a heatwave.

3.3.2.2 Insider threat

Employees and contractors within a utility, DER vendor or aggregator may misuse their access to compromise the integrity or availability of the CSIP-AUS infrastructure. This could include leaking certificates or other credentials, implementing malicious code in systems or issuing widescale configuration changes.

3.3.2.3 State-backed actor

The ability to disrupt power systems and other critical infrastructure is a key capability that many state-backed threat actors seek. While larger power system infrastructure is protected through OT systems and a legislated requirement of robust cybersecurity, the distributed and internet-based nature of CSIP-AUS infrastructure may be a more viable target gain the persistent capability to disrupt power system operations if required.

It is also important to note that CSIP-AUS utility server infrastructure interfaces with OT systems, either directly or indirectly. This interconnectivity can potentially increase the attack surface area on these critical OT systems, thereby creating additional vulnerabilities that threat actors may seek to exploit.

3.3.2.4 Opportunistic Attacker

Utility servers implementing CSIP-AUS are often directly connected to the public internet and are easily discoverable, being referenced in utility connection handbooks and documentation that is publicly accessible. This visibility can make them attractive targets for opportunistic attackers, including individuals with moderate technical skill who are motivated by curiosity, challenge or notoriety rather than financial or geopolitical incentives. These actors may scan for and probe exposed endpoints, exploit weak or unpatched configurations or attempt other exploits simply to see if they can influence real-world systems.

3.4 Vulnerability Assessment

Below are areas of weakness in the CSIP-AUS protocol or implementations which could be targeted by a threat actor to achieve their objectives.

It is important to acknowledge that all protocols have weaknesses to some extent and that weaknesses and vulnerabilities are risks to be managed. These risks can be managed through mitigations implemented by users of the protocol, such as monitoring and alerting relating to a known weakness, and improving the protocol over time.

Additionally, the vulnerabilities and weaknesses outlined below are commonly known to users of CSIP-AUS/IEEE2030.5 or are easily deduced by a cybersecurity practitioner through reviewing publicly available documents.

3.4.1 Public Key Infrastructure

In CSIP-AUS, Public Key Infrastructure (PKI) and digital certificates form the backbone of authentication and trust. Utility servers and clients use X.509 certificates to establish their identity through mutual TLS.

CSIP-AUS relies on a PKI framework that cannot provide appropriate security and operational capabilities for the near-term scale of assets under control. To date, CSIP uses the IEEE-2030.5 PKI specification with only minor variations[5]. The 2030.5 PKI is designed to provide an irrevocable device identifier with several key properties. Certificates are intentionally non-expiring, irrevocable records of the manufacturer, make, model, version and unique serial of a 2030.5 device[6]. This design targets the original use case of IoT devices on local networks, but does not align with the operating model and capabilities introduced by CSIP-AUS.

In Australia, industry consensus around the default 2030.5 PKI introduces multiple weaknesses to the CSIP ecosystem. The following touches on some of the key areas of concern:

- **Identities are immutable:** Immutability is built into the PKI and relied on by the protocol. At a PKI-level, certificates have no expiry and cannot be altered or revoked once issued. At a protocol level, the canonical identity (LFDI) is derived from the certificate. As a result, any change to a certificate detaches the existing state and potentially requires re-registration and manual reconciliation of operational and historical data.

[5] CSIP-AUS permits DNS and IP records in the subjectAltName of a notification server.
[6] Conceptually, a device may be hardware or software, but the original framework is designed around IoT systems.

- **Public internet controls are absent**: Privileged CSIP-AUS services (utility server, cloud proxy, notification server) typically use 2030.5 PKI certificates on public endpoints. They don't contain essential attributes needed to verify the validity of a connection (e.g. mandatory DNS hostnames, expiry, CRLs). As a result, some of the most critical parts of a CSIP-AUS deployment are susceptible to a range of impersonation attacks.
- **Revoking access is challenging:** The IEEE-2030.5 PKI disallows certificate revocation (and formal CRLs) and recommends using some form of access control list. The standard defines no distribution method or requirement for devices to use this information (if it existed). As a result, simply being a device in a trusted manufacturing PKI is sufficient proof to gain access, unless a system is specifically configured to prevent access.
- **CSIP-AUS functions are undefined:** CSIP-AUS implements a central control plane on top of IEEE 2030.5 via utility server, cloud proxy and notification modalities. They have substantial privilege in a CSIP-AUS ecosystem. However, the current PKI provides no information for a subsequent authorisation system to positively establish what role any device has. As a result, information in the current PKI does not allow an authorisation system to differentiate between different parts of the CSIP-AUS ecosystem.
- **No scoped privilege:** CSIP-AUS introduces significant privileges to the cloud proxy, which is allowed to represent an arbitrary range of devices by synthesising LFDIs. The capability to create and or claim LFDIs is unbounded, aside from any discretionary implementation or configuration in a utility server. Without the PKI including attributes about the entity that could be used by an authorisation system, it makes it more difficult to secure a server against cloud proxies acting on behalf of devices that are outside their actual scope of responsibility.

The culmination of these weaknesses translates to an attacker, being able to attain a valid certificate at any level of the hierarchy, could under many CSIP-AUS implementations impersonate clients or servers, issue commands, or access privileged services within the CSIP-AUS ecosystem. This is compounded by the limited ability to detect, constrain or revoke access to potential attackers, and non-expiring certificates enabling attackers to persist.

It should be noted that whilst the specification does allow for other PKI implementations, the industry has converged on the default 2030.5 implementation approach, in the absence of any other published implementation.

The recent ACCC approval of establishing a national energy PKI (NEPKI)[7] provides an opportunity to uplift the PKI used for CSIP-AUS implementations.

3.4.2 Server and Client State

CSIP-AUS stores most device and message metadata centrally on the utility server, rather than sending it alongside client communications. By separating data from metadata, clients can minimise what they send, reducing bandwidth and complexity – but also introducing security risks.

As metadata isn't co-signed or co-transmitted, clients and servers can easily diverge in their understanding of a session or message. A server can silently alter its record of a client's activity, and the client has no way of knowing. The client may keep sending the same data, unaware that the server now interprets it differently. This creates a large surface for confusion, exploitation or deliberate state manipulation.

When a client registers, it sends a POST request containing all configuration details (meter type, service type, measurement unit, scale factor and device identifier). The server stores this information indefinitely, assigns an internal identifier and a dedicated URL, and thereafter expects telemetry packets to include only a numeric value and a timestamp. Because clients do not resend configuration metadata, any undetected modification of the server's record causes clients to continue reporting under outdated assumptions, introducing risks of confusion, exploitation and deliberate state manipulation.

For example, when sending telemetry, CSIP-AUS clients only send a numerical value in the payload (e.g. "5"). The unit that value refers to (e.g. "kilowatts") is stored on the utility server, having originally been sent by the CSIP-AUS client when it registered.

[7] https://www.accc.gov.au/public-registers/authorisations-and-notifications-registers/authorisations-register/energy-networks-association-limited-and-ors

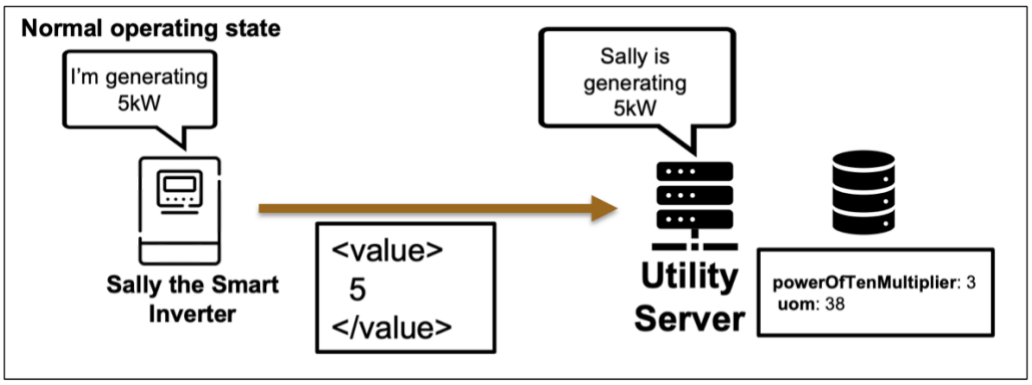

Figure 6 CSIP-AUS client sending telemetry to server under normal operating state

If an attacker gained access to a valid certificate to impersonate this inverter it could change the unit of measurement on the server (e.g. from "kilowatts" to "megawatts"). The inverter would keep reporting its telemetry as 5, expecting the server to interpret this as 5 kilowatts, but instead the server would interpret it as 5 megawatts.

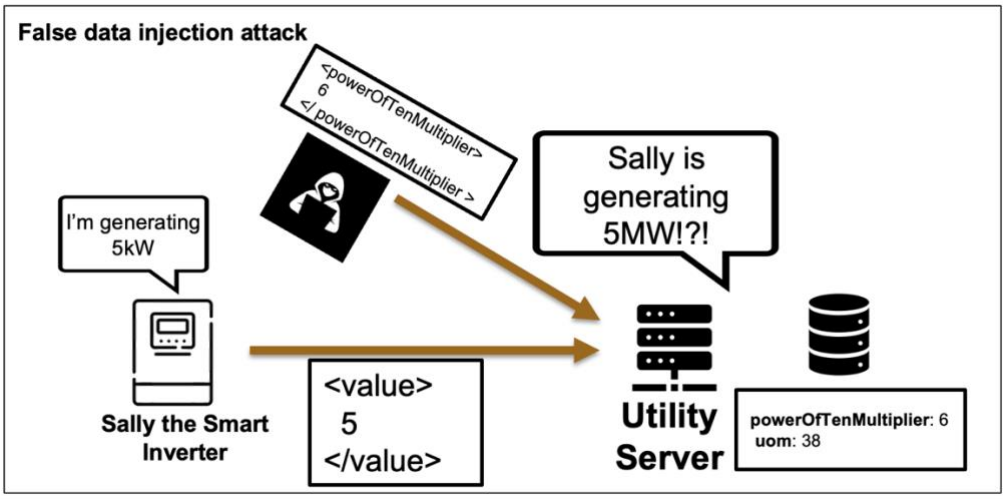

Figure 7 Attacker changing units of telemetry, causing the server to misinterpret telemetry

In effect this allows an attacker to create a false data injection attack, using the valid client which is still online and reporting telemetry as part of the attack.

3.4.3 Access Control

The lineage of CSIP-AUS leads it to a general posture of high trust towards all clients operating in the ecosystem. Once the server confirms that a client has a valid certificate in the trust hierarchy, implementations can often be permissive with actions allowed to clients, on the assumption that a client would have no reason to control or learn about

devices other than their own. Trust granted to aggregators is often even more permissive than that granted to individual devices.

2030.5 contains some high-level guidance around access control but fundamentally does not mandate any mechanism to ensure that a particular client (aggregator or device) may only control the devices it should operationally be allowed to control. Control implementation will ultimately be custom to each server, and a server that implements no access policy at all, and allows any client to access any resource, is still fully compliant with CSIP-AUS.

To give an example, in section 10.11.3 (e) of the 2030.5 standard, the section describing how clients can control device telemetry data stipulates only that “The Metering Mirror server SHOULD only accept POSTs to a given MirrorUsagePoint from the client that created the mirror”. While this encourages ACL usage, no specific solution is described for practically implementing this restriction, and the ambiguous operational relationship between clients and LFDIs makes it difficult to persistently bind them without custom logic. If a server does not implement thorough, custom access policy, a malicious actor could trivially acquire access to a legitimate certificate (for example by purchasing and registering a real solar device) and immediately use it to control all other devices on the network.

Though 2030.5 permits access policy enforcement, it does not mandate a solution to constrain client behaviour after authentication. In practice, this leads to a default-permit posture, where any client presenting a valid certificate is implicitly authorised to perform broad operations unless explicitly denied by local configuration. If a server does not implement such controls thoroughly, authentication becomes de facto authorisation, and critical operations are exposed by default. This broad trust model enables several clear client-side vulnerabilities. For example, without policy controls to limit registrations, a malicious actor could acquire a legitimate certificate and use it to register thousands of non-existent devices, reading points, and subscriptions. Even a small number of phantom resources could distort the server’s view of reality, leading to bad instructions being sent to real devices; at scale this attack could overwhelm server internals and function as a denial-of-service.

Additionally, since there is no mandated tracking of client action and ownership of registrations, if a server implementation does not take additional action to ensure security via tracking and custom attribution of action, it is not necessarily possible to identify which certificate created which registrations and therefore to identify if a device is real or was created maliciously in the event of an attack. This means that, in the aftermath of such an attack, where a malicious actor has registered many non-existent devices, it could be very

difficult to identify compromised or fabricated registrations and potentially lead to a scenario where the only way to reset the server to a trusted state is via a full database purge, and the loss of all associated data.

The following is a short-form enumeration of the specific vulnerabilities identified in the current CSIP-AUS minimal allowed access control model:

- **Transitive trust via certificate hierarchy**. Any client with a valid certificate is implicitly trusted to perform sensitive operations, regardless of origin or role.
- **Undefined resource ownership enforcement**. There is no requirement to bind resources to entities. This means that potentially clients may act on LFDIs they did not create. While server implementations can enforce ownership, it is often done on an ad hoc, per-resource basis with is mistake prone.
- **Aggregator role overreach.** Aggregators may create and modify arbitrary LFDIs, with no scoping or delegation constraints defined in the protocol.
- **Lack of authorization boundaries.** The protocol does not define role-based access or fine-grained permissions; all authenticated clients share a common default privilege tier.
- **No mandatory logging of client actions.** In the absence of persistent attribution, malicious registrations or changes cannot be traced to a source.
- **Susceptibility to registration flooding.** Without limits or controls, a single certificate may register thousands of false devices or resources, degrading server accuracy and stability.
- **Resource enumeration exposure**. The lack of access scoping allows brute-force discovery of valid LFDIs or other resource identifiers.

3.4.4 Subscription/Notification

CSIP-AUS supports a Subscription/Notification function to avoid constant polling. A client can subscribe to a resource on a utility server and then will be notified by the server when the resource changes. Notably, when a client subscribes to a resource, it provides a callback endpoint URI for the server to send notifications to.

An attacker may abuse the Subscription/Notification function set to read or exfiltrate unauthorised data, perform SSRF attacks, probe internal networks, exhaust resources on local or remote systems, or relay information through the CSIP server.

Authenticated clients may subscribe to any resources not explicitly disallowed by a server, and, as part of the subscription, may provide a client-defined notification endpoint for the subscribed events.

- Clients may request a subscription to any resource on the server. The server will disallow subscriptions based on a discretionary permissions model.
- Clients may supply a notification endpoint with a subscription request that is a client-defined and arbitrary URI. This may allow attackers to target internal admin endpoints (SSRF), enumerate internal systems by combining notifications with the NTFY_FAIL log event, or sent data to a network of remote hosts.
- Clients may request an arbitrary number of subscriptions and notifications, which may allow an attacker to exhaust TCP connection pools or saturate networks.

The CSIP-AUS specification has limited guidance or requirements for allowances or validation of subscribe/notify targets. To improve this, future CSIP-AUS versions could incorporate mandatory default subscription policies, limits on the number of subscriptions per client, sanitisation of notification URLs (including protocols, private networks, and domains) and domain ownership checks for notification endpoints.

3.4.5 Entity Attestation

The security and trustworthiness of entities (hardware devices and software products such as a utility server or cloud-proxy) participating in a CSIP-AUS environment cannot be meaningfully assessed. It is highly likely that insecure, uncertified or non-genuine entities will be active in a system, and CSIP-AUS provides no method to detect these systems. This creates physical, cyber and operational risk.

This limitation is a result of:

- The reliance on the IEEE2030.5 PKI for device identity without additional mechanisms to capture, verify and distribute additional data and proofs of authenticity to CSIP-AUS operators.
- A lack of baseline requirements in the hardware and software security requirements that reflect current standards (e.g. Cyber Resilience Act, OT devices)

As a result, the underlying security of physical and software entities is:

- Insufficient: Software provenance, versions and standards compliance is not reported or updated.

- Low integrity: There is no method to test, distribute or validate any information about a device, other than possession of a certificate.
- Untrusted: There are no consistent requirements[8] that hardware or software devices are implemented via methods that can meet external baseline security standards that are relevant to a CSIP-AUS deployment.

3.4.6 Other Weaknesses

There are other various weaknesses in CSIP-AUS, primarily inherited from older versions of the originally Zigbee smart energy or SEP2 standard. A few examples where the standard falls below today's best-practice include:

- **XML payloads:** CSIP-AUS messages are XML documents. The complexity of XML introduces a large attack surface for XML based cybersecurity attacks. These attacks can include the ability to read local files on the server, exhaust system resources or inject unexpected structures.
- **Older transport protocols**: TLS 1.2 and older cipher suites (TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8) are used in CSIP-AUS which are weaker to attacks[9], are not widely adopted by industry and have known vulnerabilities. Forcing older versions of TLS downgrades libraries on both client and server and requires custom cloud TLS offload proxy implementations with common cloud service providers.
- **Increased attack surface from unused functions:** 2030.5 has many functions or implementations that aren't necessary for CSIP-AUS and increase the ways an attacker could exploit the protocol. As one example, unused message formats Efficient XML Interchange (EXI) and support for multicast DNS that aren't explicitly disallowed in CSIP-AUS, and if supported may open a wide range of potential exploits.

[8] Noting that some individual utility server operators require 3rd parties to meet cybersecurity requirements. Such as SA Power Network's "Dynamic Export – Cyber Security Requirements"
[9] Including future post-quantum cryptography attacks.

3.5 Risk Assessment

Below is a risk assessment that can be used to understand the level of risk each of the weaknesses present to power system security. This risk assessment of impacts to the power system is carried out in the context of a utility server or aggregator being connected to over 500 MW of DER in the National Energy Market (NEM) or 200 MW of DER in the Wholesale Energy Market (WEM)[10], which in most cases is not currently the case, but will become more common leading up to 2030.

The risk assessment assess risk on a 4-point scale (Low, Medium, High, Critical) and takes the factors 'exploitability' and 'impact' into consideration.

Exploitability / Impact	Low	Moderate	High	Critical
Low	Low	Low	Medium	High
Medium	Low	Low	High	High
High	Low	Medium	High	Critical
Critical	High	High	Critical	Critical

Table 1 Combining exploitability and impact to forma risk rating

Exploitability is the difficulty the attacker may encounter in carrying out the attack. For example, where an attacker requires any valid CSIP-AUS certificate, many which are on DER devices in the home, the exploitability rating may be high or critical due to the ease of accessing this information. Conversely, if an attacker requires access to highly secured information or privileges then the exploitability rating would be low.

Impact assesses the potential level of impact to the power system. It scores the impact of each weakness against:

- **The scale of impact to the power system**. This can range from disabling or maliciously operating individual or small groups of systems, up to complete control of the fleet of clients connected to a utility server. Attacks on the significant scale may result in localised outages and system level responses such as increasing reserves (defined as "significant" in scale) whereas attacks on the complete scale could result in wider outages in some circumstances (defined as "complete" in scale).

[10] This reflects aggregate sizes approaching the largest single contingency in each power grid, which the power system operator procures reserves to protect against changes in power output of this size. More sophisticated attacks such as an attacker having a high level of real-time direct control over a fleet of DER may trigger these risks below the 500MW and 200MW levels stated.

- **The duration to restore normal operations.** Some attacks can be recovered from, including evicting the attacker, quite quickly. An example of a brief duration may be simply blocking a certificate or group of IPs that will result in a return to normal operations. Where attackers are harder to evict, critical databases take longer to restore or equipment is damaged, it may take longer to recover to a reliable operating state.

Scale / Duration	Brief (<1h)	Temporary (<6hr)	Sustained (6hr-24hr)	Protracted (>24hr)
Individual	None	None	None	None
Limited	None	Low	Low	Moderate
Significant	Moderate	Moderate	High	High
Complete	High	High	Critical	Critical

Table 2 Combing scale and duration to form an impact rating

Below is the risk assessment of weaknesses identified in the vulnerability assessment, noting that this applies to utility servers that are connected to an amount of DER that could cause significant power system disturbances if operated maliciously.

It's recommended that risk that are rated as high or critical are prioritised in uplift to the CSIP-AUS specification or associated infrastructure (such as PKI) and all risks are mitigated where possible by operators of CSIP-AUS clients and utility servers. Recommendations on mitigations for operators are in the next section.

Weakness	Impact	Exploitability	Risk
PKI			
No expiry or revocation	High	High	High
No mechanism to verify server identity	Critical	Critical	Critical
No CSIP-AUS identifiers	High	Medium	High
Server and Client State			
Configuration decoupled from operational values	Medium	Medium	Medium
Access Control			
Lack of resource ownership enforcement or authorisation boundaries	High	Medium	Medium

No least-privilege authentication/authorisation	High	High	High
No privilege controls	High	Low	Medium
Subscription/Notification			
Malicious endpoint causing server resource exhaustion	Medium	High	Medium
Malicious endpoint SSRF attack	Critical	Medium	High
Entity Attestation			
Lack of entity attestation and baseline security requirements	Medium	Medium	Medium
Other Weaknesses			
XML	High	Medium	High
Older transport protocols (DER devices)	Low	Low	Low
Older transport protocols (Aggregator/utility server)	High	High	High
Increased attack surface from unused functions	High	TBD	High

Table 3 Risk rating for identified weaknesses in the vulnerability assessment

4 Cybersecurity mitigations for CSIP-AUS server and clients

This sections documents cybersecurity mitigations to increase the security of the CSIP-AUS ecosystem. These recommendations don't require changes to the protocol or in many cases the overall implementation of CSIP-AUS, meaning that individual organisations implementing CSIP-AUS infrastructure can apply these mitigations immediately. Additionally, many of these mitigations could be used in other internet-based communications to DER in the Australian market, such as Open Charge Point Protocol (OCPP) for electric vehicle (EV) fleets or proprietary APIs for VPPs.

Appendix A summarises recommended mitigations by category.

4.1 Asset Inventory

It's imperative for utility server operators and aggregators to understand physical and digital assets in the CSIP-AUS ecosystem, and the entities who control those assets. This includes accurately recording:

- **Physical assets**: identity (make, model, serial number, etc), location, capability, operational attributes.
- **Digital assets**: versions of software or firmware running on DER or in clouds, links to physical assets, IP addresses/hostnames where applicable, 3rd party software dependencies

Additionally, it's recommended recording accurate and detailed information about parties which operate these systems, such as manufacturers and technology providers, including how access and operations occur.

Having an accurate understanding of what assets are in the CSIP-AUS ecosystem, what their capabilities are and who has access to them ensures that sufficient planning and responding to cybersecurity threats can occur.

4.2 Tailored Threat Detection

Many of the weaknesses described in Section 3 are inherent to the CSIP-AUS protocol and will take time to strengthen through future updates to the protocol or implementations.

Tailored threat detection searching for actors attempting to exploit these weaknesses can increase the difficulty of threat actors trying to exploit assets in the CSIP-AUS ecosystem.

Some examples of specific CSIP-AUS threats that could have tailored detections of malicious behaviour:

- **Unexpected request sequences from clients**. CSIP-AUS is a 'chatty' protocol, requiring multiple messages to be passed back and forth between the client and server to perform actions. This is advantageous for threat detections when detecting message sequences from clients or the server in an unexpected pattern, particularly when it relates to a potential weakness in the protocol.
- **Unexpected behaviour towards resources on the utility server**. Many updates to configurations or subscriptions, or clients attempting to access resources they are not associated with.
- **Certificates used in multiple contexts**. Certificates being used to represent different devices, coming from multiple IPs, or other behaviour suggesting re-use of certificates.

In cases where CSIP-AUS is implemented on DER devices in the home, transmitting information over the internet, with a wide range of implementation parties, such as solar emergency backstop, DOE, and VPP programs, it's expected that many detections of a threat may be false positives. This may be due to non-malicious errors such as device misconfigurations, widescale internet outages or infrastructure outages. Operators of these detection systems must tune them to separate behaviours that may be link to malicious threats and behaviours that indicate a non-malicious cause to avoid being overrun by false positive detection results.

Finally, it's recommended operators being able to map these positive detections of malicious behaviour to their threat model, to prioritise the investigation and actions that should occur against the detected threat, and to be able to identify if individual detections are related to each other, indicating a larger attack.

4.3 Incident Response and Recovery Processes

Where threat behaviour is correctly identified and understood, operators need the ability to isolate, contain and recover from an attack.

This includes having multiple layers of response and recovery processes, such as:

- **Automated abilities** to block IPs and certificates due to suspicious behaviour, with further review processes to investigate and rectify any root causes of this behaviour.
- **Inter-company incident response processes**. For example, if an aggregator certificate or infrastructure is compromised, multiple parties need to communicate and take coordinate actions to resolve the threat. Additionally, an ability to share threat information between utility server operators is highly recommended.
- **Disaster recovery processes**. Many attacks on CSIP-AUS infrastructure may be maliciously creating or changing many resources on utility servers. This makes it difficult to understand how resources on the utility server relate to the real-time energy systems being operated. If these data corruption attacks are rectified in an ad hoc manner it may take days or weeks to recover. Being able to evict any attacker and revert to a last known good state to maintain some operational control of the DER is imperative.

4.4 Public Key Infrastructure

While there are limitations in the ability to apply 2030.5 certificates securely and robustly, there are steps implementers of PKI infrastructure and utility server operators can apply to best secure those functions:

- **Implement access control mechanisms**. Implementations of PKI certificates in CSIP-AUS do not allow modern methods to revoke certificates such as certificate revocation lists (CRL) or methods using online certificate status protocol (OCSP). Operators are recommended to create alternative methods of denylisting suspicious or compromised certificates.
- **Use internal MICAs if possible, rather than issuing MICAs to manufacturers.** Allowing manufacturers to directly create and sign client certificates with MICAs introduces risks to the integrity of the PKI hierarchy. To ensure certificate issuance is tightly controlled and tracked it's recommended utility server operators or owners to sign device certificates for manufacturers on request.
- **Allowlist aggregator IP addresses**. Parties using aggregator certificates have privileged access to represent, create and update may different end devices. Compromises of certificates from aggregators or cloud proxies can create a large threat vector to the CSIP-AUS ecosystem. As such, it is highly recommended to require connections from aggregators be done only through approved IP addresses,

with secure processes for the aggregator to update the addresses they connect from.

4.5 Server State

As described in the vulnerability assessment, CSIP's architecture relies heavily on server-side state: devices send minimal data per-transaction and trust the server to know and supply context. This design simplifies clients but creates a critical security vulnerability – if server state is incorrect, incomplete, or maliciously altered, devices can't detect it, and servers likely won't either. The following section outlines mitigations that CSIP server operators can use to detect and respond to this set of threats without altering the schema. Framed around telemetry config but broadly applicable, each measure binds server actions to verifiable state, checks for unexpected deviation, and triggers alerts for review. Taken together, these mitigations describe a lightweight path toward telemetry-driven integrity enforcement.

- **Hash & set config at registration**. Establish a baseline: at registration, serialise and hash the device config, and store the hash. On each telemetry POST, rehash the current server-side config, and compare it to the stored hash. If the two don't match, raise an alert. This detects backend tampering, admin errors, or misconfigurations that the device can't see. Valid config overwrites can update the hash, and no alert will be raised.
- **Immutable audit log for config changes.** Record every config mutation with timestamp, actor, and diff, in append-only storage if possible. Alerts from *Hash & set config at registration* (above) could also be cross-referenced against this record to distinguish expected updates from anomalies.
- **Enforce trust-on-first-registration.** Treat the initial config registration as authoritative unless a re-registration or approved overwrite occurs. Block or flag backend changes that aren't traceable to device-side intent or sanctioned updates.
- **Telemetry sanity checks**. Validate incoming telemetry against a reasonable expected range for the device's config. Flag implausible values, e.g. 5GW from a rooftop solar inverter. Alerts here can suggest desync even when config wasn't visibly changed.
- **Optional client-config echo.** Encourage clients to include a copy or hash of their current config alongside telemetry within the payload. This is not required by the

spec but is allowed. If included, the new config can be compared to server-stored config with an alert on mismatch.

- **Restrict config change surface area.** Limit who and what can mutate stored config. Enforce RBAC, MFA, and change approvals. This could at least mitigate much of the risk from internal tooling or operator error.
- **Disallow config overwrites**. A broad policy to reject in-band config changes from devices, even if permitted by the spec, would provide a significant security improvement by guaranteeing that any actioned overwrites are suspicious. A manual process for changes could still be allowed when an overwrite is strictly needed.

4.6 Subscription/Notification

Utility server implementations can employ a range of mitigations against subscription/notification exploits:

- **Disallow redirects.** Servers should ignore redirects to avoid resource exhaustion attacks using HTTP redirect loops. Implementers of CSIP-AUS clients should be instructed to not respond with redirects in their notification URIs.
- **Implement timeouts.** Servers should implement an appropriate timeout (such as 10 seconds) when sending notifications to avoid attackers implementing slow HTTP attacks where the server at the callback URL responds to the request very slowly.
- **Monitor number of subscriptions per client.** A large number of subscriptions from a client may indicate a non-malicious configuration error or malicious attack which could impact utility server operations.
- **Require clients to register domains.** Where operators of CSIP-AUS clients are utilising the subscription and notification functions, it's recommended that the callback domains are registered with the utility server operator, and the utility server operator implements an allow list of domains scoped to specific clients.
- **DNS resolution verification.** Before sending notifications, utility servers can perform DNS resolution of the notification URI to detect anomalies such as IP address changes or redirections to suspicious domains. Additionally, implement DNSSEC where possible to prevent DNS spoofing.
- **Prevent loopbacks and internal access.** Deny notification URIs that resolve to internal network addresses or the utility's server own loopback interface to mitigate SSRF attacks.

4.7 Least Privileged Authorisation

CSIP-AUS adopts a high-trust model in which authenticated clients are broadly permitted to act, often without constraints or attribution. Aggregators can perform privileged operations on arbitrary devices, and there is no mandated mechanism to bind resources, such as LFDIs or mirrors, to specific clients. Combined with the lack of mandatory default-deny posture, audit trails, or registration limits, this enables a wide surface for potential abuse: impersonation, injection of false state, enumeration, and internal denial-of-service. These weaknesses stem not from specific bugs, but from structural omissions in the protocol's approach to access control.

In the short-term, hardened policy-based access controls can be implemented completely in accordance with the protocol, which alone can provide significant protections against the vulnerabilities described above.

- **Bind resource ownership at creation.** Whenever a client creates an LFDI, mirror, or subscription, store its certificate alongside. Reject future modifications from clients whose certificate doesn't match the creator.
- **Enforce scoped aggregator permissions.** Alternatively, or alongside the above, build a configuration layer that associates aggregator certificates with allowed LFDIs. Block operations targeting out-of-scope IDs.
- **Move to mandatory default-deny policy.** Treat all clients as untrusted by default. Only allow operations from a given certificate if there is an explicit allow-list entry or ownership record. Anything not explicitly permitted is denied.
- **Throttle and rate-limit sensitive operations.** Impose caps, or potentially just alerting thresholds, on number of registrations, mirror readings, etc. per certificate.
- **Implement mandatory action logging.** Log every registration, mirror creation, update, and deletion along with the client identity, and store this immutably if possible. This provides forensics and enables building sophisticated heuristics for detecting abuse later.

4.8 Security testing framework, risk assessments and threat models

As CSIP-AUS differs to how many modern, secure internet-based communication standards operate, typical pen testing, security testing, risk assessment and threat modelling exercises may miss the nuances and specific weaknesses of the CSIP-AUS protocol. Therefore, it is critical to tailor security assessments to the unique characteristics and known weaknesses of the protocol.

Risk assessments must also account for the systemic dependencies introduced by the CSIP-AUS architecture, threat actors that may want to target critical infrastructure and how these risks apply to organisational wide compliance requirements such as the Security of Critical Infrastructure Act (SOCI).

5 Recommendations for CSIP-AUS cyber development and uplift

This section outlines ways to increase the security of the CSIP-AUS protocol, associated infrastructure and broad industry implementation of CSIP-AUS over time.

It includes short term recommendations that could be implemented over the next 1-3 years in minor version updates to CSIP-AUS or minor changes to implementations of the standard, and longer-term recommendations that could be implemented in major version updates to CSIP-AUS or reforms to supporting infrastructure approaching 2030.

Appendix B summarises and groups the recommendations into short-term and long-term timeframes.

5.1 Public Key Infrastructure

Improving the PKI is a high priority as CSIP-AUS is rolled out to more jurisdictions and fleet sizes grow. The National Energy PKI (NEPKI) being established creates an opportunity to carry out this uplift, ensuring the PKI improvements are done in a nationally consistent manner.

The PKI used within CSIP-AUS covers two use cases: Device Identity, and Operational Identity. In 2030.5, these two usages are established by the one PKI that uses unchangeable and non-expiring certificates. The lack of revocation and expiry is appropriate for an enduring device identity but poses problems in operational use. Operational policies such as what authority a device has, how long it may be active for or how it is identified cannot be expressed in the PKI. Additionally, the current certificate specification cannot represent the CSIP-AUS device types or functions in any form.

While the IEEE2030.5 specification details the use of other PKIs (for example a standard Web PKI) It appears to be common practice to use a IEEE2030.5 PKI for all systems in a CSIP-AUS domain. The use of IEEE2030.5 certificates for web services substantially diminishes the security of the overall control plane.

There are several key outcomes in any change to the PKI:

- DNS and revocation verification of server certificates
- Revocation and expiry of client certificates
- Future-hardened cryptography
- Decoupling CSIP-AUS operational identity from immutable certificate fingerprints.

5.1.1 2030.5 compatible improvements

5.1.1.1 Use generic certificates for service endpoints

Clarify the expected roots of trust that should be used to verify each type of device used within CSIP-AUS. Specifically, client certificates MUST be IEEE-2030.5 certificates. Web Service endpoints (utility server, notification server) that are resolved via DNS over the public internet MUST be standard web certificates from CAs that comply with CABForum requirements. This may be a subset of CAs that are selected for Australian use.

Change CSIP-AUS certification to include assessment that client devices appropriately verify certificates, and are able to synchronise any additional state (time, revocation) needed to perform accurate verification.

5.1.1.2 Require DNS records in any 2030.5 server certificates and allow re-issuance

This is a fallback requirement if generic certificates (above) are not used. It is not preferred as there are still substantial issues with expiry and revocation, and overloads the concept of a Manufacturing PKI by using those certificates for service endpoints. However:

Require any server (notification, utility) that is accessed over the public DNS must:

1. Include appropriate DNS entries in the subjectAltName
2. Have an expiry of no more than 6 months (which is substantially greater than generic certificates)
3. Be permitted to be re-keyed and renewed

Require that any CA that issues server certificates publish revocation data (via CRLs or OCSP) for server certificates.

Change CSIP-AUS certification to require that any CSIP-AUS client that connects to a server will reject connections where a SAN is absent and verifies the SAN and other expiry-related data.

5.1.1.3 Implement CSIP-AUS certificate device extensions

Implement appropriate csip-aus-dev-* and csip-aus-po-* extensions under a csip-aus policy arc. These would be sufficient for utility server operators to unambiguously identify the nature of interoperating systems.

Device types would be used to identify the modality of a device (DER, cloud proxy, notification server, utility server).

A policy would be used when a device is a cloud proxy to explicitly define the LFDI scope assignment to that proxy. Minimally, this policy would express the PEN. Optionally, this policy could be used to further constrain the allowed LFDIs.

Notably, some utility server operator handbook policies describe requiring the PEN in any aggregator generated LFDIs, but formalising the above approach will ensure consistency across implementations and separate policy and scope from certificate or identifier management.

5.1.1.4 Update the minimum TLS version and ciphersuites

Updating minimum TLS version and ciphersuites increases security not only from the enhancements within these updates, but also the increased breadth of infrastructure that supports these more modern versions such as many web application firewalls.

5.1.2 More substantial improvements

These recommendations attempt to substantially improve the CSIP-AUS PKI while leveraging the existing 2030.5 PKI substrate.

5.1.2.1 Implement Operational certificates

CSIP-AUS currently relies on the IEEE-2030.5 manufacturing PKI for identities. That PKI is intended to provide a permanent, unique and immutable device identity (subject to pragmatic realities, e.g. cryptography).

5.1.2.1.1 Problem

This introduces considerable complexity to CSIP-AUS implementations for several reasons outlined elsewhere:

- **Permanence:** Operators must accommodate non-expiring, non-revocable certificates, potentially maintaining ever-growing access lists in perpetuity.
- **Manufacturing hierarchy management:** To handle multiple device types, operators must either add multiple manufacturer roots of trust to their systems then actively allow/preclude systems or maintain their own equivalent manufacturing PKI and distribute identities to devices from multiple manufacturers.
- **Identity coupling:** Identities within CSIP-AUS specifically use a device certificate fingerprint as the LFDI. This prevents changes to a certificate under any circumstances, which means that it's impossible to upgrade the cryptographic foundations of the operating environment.
- **Public internet:** The most critical and significant parts of the system (utility servers, cloud proxies) located and accessed over the public internet. These systems are often treated as Devices despite having no need to be represented as such, with the

result that the certificates used for them are as limited as permanent Device certificates.

- **Policies and usage:** The behaviours of systems in CSIP-AUS differ from those defined in IEEE 2030.5. For example, the addition of cloud proxies adds the ability to synthesize LFDIs for other devices. This capability cannot be represented within the existing PKI, and if it were represented as policy objects, the capability cannot be changed without a certificate (and therefore LFDI change).

5.1.2.1.2 Recommendation

Implementing the concept of **Operational Certificates** allows a decoupling of Device Identity from Operational Identity. This model is analogous to the Matter Protocol (see Commissioning), in that:

1. Physical devices are provisioned with a manufacturing-time certificate. For CSIP-AUS, this would be an IEEE 2030.5 Manufacturing PKI based certificate.
2. At the time of commissioning, the device certificate is used as part of the registration process to test the device identity. It's possible to do checks against other resources to make sure that the device and firmware are a certified version.
3. The device is issued an Operational Certificate that is used to participate in the ecosystem, in this case a CSIP-AUS implementation. The Operational Certificate may be given a lifespan, policies, identifiers etc nominated by the operator.
4. Operational certificates may be replaced or updated via several processes, including device-driven renewals (e.g. following firmware upgrades), as expiry dates approach, on re-induction following disconnection, or on changes to significant attributes.

These changes would provide significant improvements to the security, operations and functionality of identities within CSIP-AUS.

5.1.2.2 Implement non-LFDI primary identifiers within CSIP-AUS

CSIP-AUS inherits a requirement to use a truncated certificate fingerprint as the Globally Unique Identifier (or LFDI) within the protocol. While this may be appropriate for native 2030.5 implementations, it renders the certificates used in CSIP-AUS immutable. This would not specifically uplift cybersecurity but enables compatibility with the current CSIP-AUS framework of immutable identifier if operational certificates are adopted.

5.1.2.2.1 GUID in place of LFDI for DER and Proxy Devices

For DER and Proxy Devices (i.e. physical devices installed at a site) we recommend using an alternative UUID in place of the certificate fingerprint would allow operators to

decouple device identity from a single and non-modifiable certificate. The UUID would simply be provided as a value in the Subject field of the certificate and used as the LFDI.

These changes would be very achievable if using Operational Certificates (above) - in this case the LFDI could simply be populated with the certificate fingerprint, requiring minimal changes to a utility server to support this new model without modifying the identifiers for existing devices and records. This would not specifically uplift cybersecurity but improve quality of life and maintainability in the CSIP-AUS framework.

5.1.2.2.2 PEN-based LFDI for Cloud Proxy Devices

Cloud-proxies operate as devices in CSIP-Aus and need to be represented in a utility server via an LFDI.

The nature of web-based services and the number of devices a cloud proxy may act on behalf of means their certificates should be rotated frequently. However, the resultant change to their LFDI has percolating effects. The association with all subordinate systems needs to be changed in the live and historical records.

Using a synthetic LFDI for these systems removes obstacles for better certificate management practices. Options for generating the LFDI include:

Method	Compatibility	Advantages	Disadvantages
Random values, per DER LFDI	Full	Nil	Nil
DNS name	Nil - substantial code changes.	Semantically meaningful	LFDI changes if DNS record changes
PEN-based LFDI	Full	Semantically meaningful, supplements Interconnection Handbooks	Nil

We note that the CSIP-AUS spec requires that cloud proxies *"generating LFDIs for managed devices use the technology provider's private enterprise number (PEN) as the last 8 hex digits with leading zeros."*. Identifying the entity bound to a downstream (or managed) device is an important attribute that can be represented in the LFDI.

For this reason, we recommend that the LFDI for a cloud proxy be a 40 character string comprised of zeros, with the manufacturer PEN as the last digits.

The LFDI would be included as a Subject attribute, per the device recommendation above.

5.2 Server State

In CSIP-Aus, devices periodically transmit only raw values, while metadata like units, scale factors, and measurement types are transmitted at registration, and subsequently stored server-side. This creates a fragile dependency: if the server's understanding of a device's config changes silently, incoming data may be misinterpreted without either party noticing. This opens the door to subtle corruption, undetected drift, and attack surfaces that are invisible at the protocol level. CSIP-AUS will go through a revision process over time that may address these risks. In the meantime, additional controls may be recommended for utility server operators.

Non-breaking recommendation (CSIP-AUS 1.3/1.4)

The most effective non-breaking patch to CSIP-AUS is to mandate that devices include a config hash in each stateless packet. When a device registers, it sends its configuration to the server. The server stores the config, computes a deterministic hash of the config, and returns it to the device. The device stores this hash, and includes it in every subsequent telemetry message. The server, on receipt, re-hashes its current config, and compares to the hash included in the message. Any mismatch indicates a desynchronisation: either the server's config has changed, or the device's view has been corrupted.

For audit purposes, the server may also sign the config at registration and include this signature in the hash. This binds the device's future telemetry to a server-signed statement of context, giving both sides a minimal, tamper-evident anchor of shared state, without requiring changes to the telemetry schema beyond the hash itself.

Breaking recommendation (CSIP-AUS 2.0)

Long-term, it would be safest to eliminate implicit state dependency from the CSIP-AUS schema wherever possible. The most robust way to achieve this is to simply deprecate server-side state retention and rather mandate that clients embed the full configuration object in every message where it applies. This renders each packet a simple, self-contained unit – interpretable without reference to prior context, verifiable in isolation, and immune to server-side drift.

While this adds minor bandwidth overhead, typical config blocks are small, and modern solar devices are more than capable of handling the added payload.

5.3 Subscription/Notification

Below are options to increase the security of the subscription/notification functions that could be implemented in upcoming revisions to the CSIP-AUS specification. Alternatively, individual utility server operators could implement these requirements.

Non-break recommendation (CSIP-AUS 1.3/1.4)

- **Enhanced sanitisation and validation of notification URIs**. Notification URIs created by CSIP-AUS clients create various weaknesses, particularly if naively processed by the server. There are various ways to increase the security of using notification URIs through various constraints and validation on the URIs themselves. This includes:
    - Allowlist-based domains and IP validation. Operators of CSIP-AUS clients utilising the subscription/notification function should register the domains and IP addresses used with utility server operators. Utility servers should reject notification URIs or IPs not on the allowlist.
- **Defined subscription profile.** CSIP-AUS could define specific subscription profiles that pre-package allowed resources for different client roles. Profiles with access to a larger number or more sensitive resources would require higher levels of authorisation and validation during registration and operational activities.

Breaking recommendation (CSIP-AUS 2.0)

- **Certificate-based domain validation.** Tie the domain of the notification URI to the subject alternative name (SAN) extension of the client's X.509 certificate. This would ensure the entity requesting the subscription is bound to the domain receiving notifications.

5.4 Common Cybersecurity Requirements

Introducing security requirements into CSIP-AUS or a subsequent document that specify required and recommended capabilities will substantially reduce operational and security risks. These requirements should be aligned with relevant external standards (e.g. https://www.european-cyber-resilience-act.com/) and near-neighbour implementations such as Matter.

These additions include hardware security requirements, software supply chain controls, methods to federate reporting and tracking, and methods of proof for the state of all hardware and software entities in the CSIP-AUS ecosystem.

The inclusion of these requirements will help achieve secure by design/default principles outlined by the ASD. We suggest that many of these goals can be informed by elements of the Matter Device Attestation Specification. To implement device attestation within the CSIP-AUS ecosystem, basic requirements such as firmware requirements on CSIP-AUS devices would need to be established before it becomes feasible to enable many of these goals.

It's possible that utility server operators such as DNSPs and retailers can create these requirements for devices and aggregators connecting to their servers, similar to SA Power Network's cybersecurity requirements for dynamic exports[11].

5.4.1 Hardware

Key hardware-specific security inclusions are:

- Key and system storage, such as secure elements/enclaves and disk encryption.
- Physical hardening, such as signed boot and disabling hardware debug interfaces.
- Firmware controls, such as signing, secure update methods, A/B images with safe rollback, and options to define and the ability to configure an operator-defined firmware distribution endpoint in place of manufacturer-direct locations.
- Control interfaces, such as composed commands rather than interactive shells, least privilege/RBAC command sets, and the ability to configure an operator-defined control endpoint in place of manufacturer-direct locations.
- Support lifespan requirements.

5.4.2 Software and Security

All entities should be required to:

- Provide a software bill of materials (SBOM) for each release
- Provide details and visibility into vulnerability handling and reporting.
- Release signing and verification.

5.4.3 Compliance verification

While the IEEE 2030.5 PKI is sufficient to identify the manufacturer, make and model of a device, it's insufficient to map that device to a more comprehensive operational state. A variant of the Matter Distributed Ledger would enable CSIP-AUS operators to reconcile the manufacturer, make and model against additional attributes such as the software and

[11] https://www.sapowernetworks.com.au/public/download/?id=327395

firmware versions, their certification status, and methods of proof for the veracity of the firmware image and version.

5.5 Security Testing Improvements

Client and server testing procedures, or specific security tests outside the standard testing procedures to incorporate a wider range of failure behaviours. This includes rigorously testing scenarios where clients attempt to access resources beyond their authorised scope. By simulating and explicitly disallowing such out-of-scope access during testing, implementers can proactively identify and mitigate vulnerabilities, ensuring that the system robustly enforces access controls and prevents unauthorized data exposure or manipulation. Other scenarios such as malicious subscription/notification attacks and XML exploits should also be tested.

5.6 Access Control

The protocol's approach to access control as it exists currently relies on a high-trust paradigm which potentially gives authenticated clients, including potential attackers, overly broad operational privileges. The protocol has no mandated mechanism for enforcing resource ownership, defining granular permissions beyond basic authentication, or ensuring comprehensive, attributable logging of client actions. These omissions create a permissive environment vulnerable to unauthorised resource control, data integrity breaches, and potential denial-of-service attacks.

Non-breaking recommendation (CSIP-AUS 1.3/1.4)

Mitigations are suggested in Section 4.7 which thoroughly enforce and monitor the various protection mechanisms which are possible under CSIP-AUS but are not enforced or described. Simply, the recommendation for future changes to the protocol is to make these protections mandatory, and provide recommended mechanisms for their implementation, so that following these new requirements does not put onerous expectations on server operators.

Key changes mapping to the above mitigation recommendations are as follows:

- mandating the enforcement of strict resource ownership,
- adopting a mandatory 'default-deny' authorisation model where permissions are explicit,

- requiring mechanisms for defining and policing operational scopes (especially for aggregators),
- enforcing comprehensive and attributable logging for all significant actions, and
- implementing rate-limiting for sensitive operations.

These measures aim to establish a consistent, high-security baseline for all CSIP-AUS deployments, ensuring critical protections are no longer optional interpretations, rather fundamental requirements of the protocol.

Additional non-breaking changes are recommended to improve the protocol's security posture in this area. These include the standardisation of more granular error codes, to clearly communicate the reasons for access denial; the introduction of an optional mechanism whereby a client can register its expected operational permissions on registration, and thus provide clear indication of anomalous behaviour should it later violate that expectation; and relatedly, the introduction of an optional interface for a client to pro-actively query their access rights in this newly authorisation-controlled environment. These measures will improve system transparency, aid client-side adaptation to stricter server policies, and enable more sophisticated, layered security postures and threat detection within the protocol.

5.7 CSIP-AUS Cybersecurity Governance

Establish a structured framework for identifying, documenting and communicating vulnerabilities associated with the CSIP-AUS protocol or implementation. This process should clearly define reporting channels, responsible parties, and escalation procedures to ensure that vulnerabilities are addressed systematically. This includes:

- **Formalised vulnerability disclosure policy.** Develop and release a clear and comprehensive vulnerability disclosure policy for CSIP-AUS.
- **Standardised vulnerability classification and scoring.** Adopt an internationally recognized vulnerability scoring system, such as the Common Vulnerability Scoring System (CVSS), to consistently assess the severity and impact of identified vulnerabilities. This facilitates prioritisation and resource allocation for remediation.
- **Establish a dedicated vulnerability management team or working group.** This designated team would be responsible for triaging and validating reported vulnerabilities, coordinating remediation efforts throughout industry, and managing communication with vulnerability reporters and public disclosure.

It may be suitable to set up these groups and functions to focus more broadly on DER cybersecurity issues, instead of specifically just CSIP-AUS, and for the groups to have a national remit.

6 Existing work related to CSIP-AUS Cybersecurity

6.1 National Energy PKI (NEPKI)

Mutual TLS using X.509 certificates is the method used to identify clients and servers in CSIP-AUS. To do this a public key infrastructure must be established and operate to create, sign, store and manage these certificates. For the initial CSIP-AUS use cases of the solar emergency backstop mechanism and flexible exports, distribution networks[12] must operate their own PKI.

NEPKI[13] is an initiative led by Energy Networks Australia and Synergy to establish a PKI that could optionally be used by all DER operators. This would mean that distribution networks could use NEPKI instead of operating their own PKI.

Many of the recommendations made in this report to improve PKI security could be carried out through NEPKI.

6.2 DNSP Cybersecurity Guidelines

Operators such as distribution networks and the retailer Synergy are creating cybersecurity guidelines for manufacturers, technology providers and aggregators with systems or devices connecting to the utility server operator (e.g. SAPN dynamic export cybersecurity requirements[14]).

These guidelines provide an opportunity to provide clear and standardised guidance to industry on organisational cybersecurity requirements for operating in the CSIP-AUS ecosystem.

Enhancing these guidelines to include enhanced testing, registration or reporting requirements or best practices would increase the cybersecurity of the CSIP-AUS ecosystem.

A national approach to these guidelines would ensure consistency between operators.

[12] or in the case of Western Australia, the electricity retailer Synergy
[13] https://www.accc.gov.au/public-registers/authorisations-and-notifications-registers/authorisations-register/energy-networks-association-limited-and-ors
[14] https://www.sapowernetworks.com.au/public/download/?id=327395

6.3 CAPA Intelligence – Cyber Risk Study (Project CERby)

Project CERby is an ARENA funded CER threat detection and incident response program run by CAPA Intelligence[15]. It focuses on emerging cybersecurity risks of how aggregate CER operated maliciously could threaten power system security, and how these risks can best be mitigated. The project is a collaboration between many different parties in the industry such as DNSPs, retailers and government.

[15] https://arena.gov.au/projects/capa-intelligence-cyber-risk-study/

7 Appendix A: Summary of Mitigations

Category	Mitigation
Asset inventory	• Accurately record identity, location, capability and operational attributes of physical assets. • Accurately record versions of software or firmware running on DER or in clouds, links to physical assets, IP addresses/hostnames where applicable, 3rd party software dependencies.
Tailored threat detection	• Ability to monitor and identify suspicious behaviour relating to specific CSIP-AUS weaknesses and characterise the potential level of impact of those behaviours.
Incident response and recovery processes	• Automated containment responses to suspicious behaviour, with further processes to investigate. • Inter-company incident response processes. • Sufficient disaster recovery processes.
PKI	• Implement access control mechanisms such as denylisting. • Use internal MICAs, rather than issuing MICAs to manufacturers. • Allowlist aggregator IP addresses.
Server State	• Record configuration at registration to establish baseline. Monitor changes to client configuration closely. • Validate incoming telemetry against expected ranges. • Allow clients to optionally send config information in telemetry payload.
Subscription/Notification	• Disallow redirects, implement timeouts. • Monitor number of subscriptions per client. • Require clients to register domains, monitor domains for changes in DNS records and implement DNSSEC. • Prevent loopbacks and internal access.
Least Privileged Authorisation	• Bind resource ownership at creation. • Enforced scoped aggregator permissions. • Move to mandatory default-deny policy • Throttle and rate-limit sensitive operations.
Penetration test strategies, risk assessments and threat models	• Tailored penetration tests, risk assessments and threat models tailored to the unique characteristics and known weaknesses of the protocol.

Table 4 Summary of mitigations

8 Appendix B: Summary of Recommendations

Short term recommendations could be implemented over the next 1-3 years in minor version updates to CSIP-AUS or minor changes to implementation of the standard, and long-term recommendations that could be implemented in major version updates to CSIP-AUS or reforms to supporting infrastructure approaching 2030.

Relevant parties are those well placed to oversee these uplift activities. Note that utility server operators are those who are responsible for procuring and operating the utility server such as DNSPs or retailers.

Category	Recommendation	Relevant Party
PKI	Short-term • Use generic certificates for service endpoints • Improve server certificate management • Implement certificate device extensions • Update minimum TLS version and ciphersuites Long-term • Decouple device and operational identity • Transition from LFDI as primary identifier • Standardise PEN-based LFDIs for cloud proxies	NEPKI
Server State	Short-term • Send optional hash of configuration in messages Long-term • Require sending full configuration in each message	DERIAPITWG (CSIP-AUS change)
Subscription/ Notification	Short-term • Enhanced sanitisation and validation of notification URIs • Defined subscription profile Long-term • Certificate-based domain validation	DERIAPITWG (CSIP-AUS change)
Common Cybersecurity Requirements	Long-term • Hardware specific security such as secure elements, hardening, firmware controls and limited control interfaces. • Software specific security such as software bill of materials, visibility into vulnerability handling and reporting, and release signing and verification.	Utility Server Operators

Security testing	Short-term • Client and server security test procedures to test against a wide range of malicious and failure behaviours.	Utility Server Operators
Access Control	Short-term • Provide recommended mechanisms for better access control.	DERIAPITWG (CSIP-AUS change)
Cybersecurity governance	Short-term • Formalised vulnerability disclosure policy. • Standardised vulnerability classification and scoring. • Establish a dedicated vulnerability management team or working group.	ISC/ DERIAPITWG

Table 5 Summary of recommendations