Attachment 2

FILED
06/03/24
04:13 PM
R2106017

Working Group Report

Smart Inverter Operationalization Cybersecurity Subgroup (SIO-CS)

Preface

Smart Inverter Operationalization Cybersecurity (SIO-CS) Subgroup Scope

The SIO-CS subgroup was formed under Track 3 Phase 1 within the "*Order Instituting Rulemaking to Modernize the Electric Grid for a High Distributed Energy Resources Future*", Rulemaking 21-06-017. The SIO-CS focused on answering the third Track 3 Phase 1 question in the High DER Amended Scoping Ruling of Rulemaking 21-06-017:[1]

3. *"What existing cybersecurity standards should be applied for smart inverter operationalization and DERMS to ensure communications between the equipment and management systems are secure (e.g., Institute of Electrical and Electronics Engineers (IEEE) 1547.3?"*[2]

The previously published Smart Inverter Operationalization (SIO) Working Group Report on DER Business Cases and Use Cases focused on the first two questions in the Amended Scoping Ruling:

1. *"Which smart inverter operationalization use cases should be prioritized and implemented to leverage the capabilities of smart inverters to provide value to grid operators and ratepayers?"*
2. *"What technology roadmaps or other relevant Commission directives related to DERMS and to smart inverter operationalization should be adopted to ensure the utilities are able to implement the Working Group's recommendations?"*

These two SIO working group reports will be followed by a California Public Utilities Commission (CPUC) Staff Proposal that will focus on identifying recommended CPUC actions. The Staff Proposal will be developed based on the working group reports, as well as party comments, staff research and analysis, and consultant input.

SIO-CS Process.

The SIO-CS was facilitated by Xanthus Consulting International in partnership with Verdant Associates LLC on behalf of the CPUC. Outreach to other groups, including the Smart Inverter Operationalization Working Group (SIOWG), the Smart Inverter Working Group (SIWG), and other CPUC lists, requested interested parties to join this group. About 80 people joined, including personnel from the Distribution System Operators (DSOs),[3] DER aggregators, DER owners, consultants, academics, and CPUC staff, although only a smaller group of interested parties actively participated in most of the meetings.

The following actions were taken:

- Bi-weekly meetings of 1.5 hours each, starting in May 2022
- Materials for each meeting, including agendas and updated documents, prepared by Xanthus
- Most meetings captured in videos
- Open discussions and chat inputs by participants were captured during meetings

---

[1] *Assigned Commissioner's Amended Scoping Memo and Ruling in Rulemaking 21-06-017, COM/DH7/smt 8/11/2023, https://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M516/K786/516786462.PDF*

[2] *IEEE Std 1547.3-2023, IEEE Guide For Cybersecurity Of Distributed Energy Resources Interconnected With Electric Power Systems, 2023*

[3] *The DSOs are currently Pacific Gas & Electric (PG&E), Southern California Edison (SCE), and San Diego Gas & Electric (SDG&E)*

- Presentations were made by participants, including the DSOs under CPUC jurisdiction
- Assignment of action items were made to specific participants
- Comments and tracked changes on documents were uploaded to the Verdant SharePoint site
- Draft documents were prepared between meetings
- Review of draft SIO-CS Working Group Report by CPUC staff
- Review of draft SIO-CS Working Group Report comments by the CPUC staff and by SIOWG participants
- Update of draft SIO-CS Working Group Report based on CPUC staff comments
- Delivery of the final SIO-CS Working Group Report to the CPUC High DER Future [R.21-06-017] Service List for comments.

The following actions are planned after the finalization of the SIO Working Group Report:

- Development of draft SIO Staff Proposal by Xanthus and Verdant, in collaboration with CPUC staff and reflecting formal party comments and reply comments on the SIO Working Group Report and this SIO-CS Working Group Report.
- Review of draft SIO Staff Proposal by the CPUC staff
- Review of draft SIO Staff Proposal by SIOWG participants
- Update and delivery of Final SIO Staff Proposal
- A proposed decision based on the SIO Staff Proposal

Report Contents This report describes the working group process and outcomes. Within this report,

- Section 1 covers the Scope of the SIOWG and includes terms and definitions
- Section 2 provides background on cybersecurity for DERs
- Section 3 provides an overview of the entire SIO-CS process
- Section 4 provides a summary of the Phase 1 Primary Cybersecurity Requirements
- Section 5 presents regulatory alternatives to operationalize these requirements
- Section 6 presents the Non-Consensus Qualifications on “Phase 1 Primary DER Cybersecurity Requirements” Document
- Annex A is the Phase 1 Primary DER Cybersecurity Requirements
- Annex B is the entire table of IEEE 1547.3 and SIO-CS participant comments, used to develop Annex A.

Executive Summary

SIO-CS Goal The goal of the SIO-CS subgroup was initially to identify what existing cybersecurity standards (and guidelines) should be applied for smart inverter operationalization. This goal was expanded by the group to include paths to implementation in accordance with the second scoping question for smart inverter operationalization. Details of how this report fits in with other activities can be found in the Preface above.

SIO-CS Development of Cybersecurity Requirements. Starting in early May 2022, the SIO-CS group met bi-weekly. The first discussions centered around the goals that could be achieved and how to achieve those goals. The first major decision was to use IEEE Std 1547.3-2023, Section 5, as the basis for which cybersecurity requirements and recommendations should be assessed for interconnected DER systems.[4] At that time, it was the only cybersecurity standard that focused on DERs, even though it only included recommendations, not requirements.

Discussions then addressed what documents would be delivered to the CPUC. It was decided to develop a separate document from the SIO-CS Working Group Report which would contain a set of primary DER cybersecurity requirements. This document eventually became the *Phase 1 Primary DER Cybersecurity Requirements,* now included as Annex A.

To facilitate discussion of cybersecurity requirements, a table was created which included all the items from IEEE 1547.3 Section 5[5] as the first column, with other columns dedicated to an assessment of the items from the SunSpec Alliance, ASE Systems, Pacific Gas & Electric (PG&E), Southern California Edison (SCE), and eventually the National Renewable Energy Laboratory (NREL)[6], along with a column for comments.[7] These organizations were asked to assess whether each of the Section 5 cybersecurity items ought to be a "**Shall**" cybersecurity requirement, a "**Should**" cybersecurity recommendation, or "**N/A**" (not applicable). During the bi-weekly meetings, the Section 5 cybersecurity items were discussed individually, and qualifications and comments were added to the table. In some cases, organizations revised their initial assessments or added qualifications based on working group discussions. **The goal was to identify those cybersecurity items which all members agreed ought to become "Shall" requirements, sometimes with modifications of the Section 5 item to clarify or constrain the requirement**.

During the subgroup process, it became clear that a phased approach would be beneficial. The first phase would consist of identifying the areas of agreement and leaving other items out for future discussion, rather than attempting to identify a complete set of cybersecurity requirements. Multiple phases would permit updates to the initial assessments of the Section 5 items, with additional or updated cybersecurity controls being rolled out over time as new threats emerged and/or better understandings of the cybersecurity risks became apparent. Therefore, the first phase started with

---

[4] Although the scoping memo focuses on smart inverters and the operationalization functions covered in the main SIOWG, cybersecurity is relevant to all types of DERs, not just those with smart inverters. Therefore, the term "DER" is used in this report.

[5] IEEE Std 1547.3-2023 was not a standard when first used by the SIO-CS. However, there were no substantial changes in the Section 5 between the draft and the final standard published in December 2023.

[6] SDG&E switched personnel attending these meetings and therefore did not develop a column of comments.

[7] San Diego Gas & Electric SDG&E did not have staff available to comment at this stage but SDG&E was able to provide consensus/non-consensus and qualifications later in the process.

basic cybersecurity requirements, with the anticipation that additional cybersecurity requirements and recommendations would follow in subsequent phases.

Summary of Phase 1 Primary DER Cybersecurity Requirements

Annex A includes the list of the Phase 1 Primary DER Cybersecurity Requirements agreed to as **"Shall"** by the subgroup. These requirements are grouped into the categories used by IEEE 1547.3:

- **RA: Risk Assessment and Management:** These requirements cover assessing and managing risks from cybersecurity threats. However, the subgroup did not identify any of the IEEE 1547.3 items as **"Shall",** so no Phase 1 requirements exist for this category.
- **NE: Network Cybersecurity Requirements:** These requirements identify the necessary network setup, management, logging, monitoring, and equipment needed to ensure the networks used for communication and control of DERs remain secure.
- **AC: Access Control Cybersecurity Requirements:** These requirements control user and system authentication and authorization, including password requirements, to access networks and devices. These guarantee that only appropriate users or systems (such as hardware and/or software) have access to these DERs and associated networks.
- **DS: Data Security Requirements:** These requirements control how data is protected both when stored and when communicated or transferred.
- **SM: Security Management Requirements:** These requirements control the lifecycle management of assets (including both hardware and software), management of security patches, and that security events such as detecting malicious code, changes to settings, updates, and deletions are logged and stored.
- **CM: Coping and Recovery Requirements:** The shall requirement in this category identifies that any security event must be captured and logged with an accurate timestamp by all stakeholders to identify when and where the security issue happened.

Possible CPUC Regulatory Paths. During the latter part of the debates on which items should be a "**Shall**" requirements, working group members raised concerns about how these requirements would be operationalized by the CPUC. The wording used in the IEEE Std 1547.3-2023 is that of a guide with *recommended* cybersecurity items (Should), not *required* cybersecurity items (Shall). Thus, taking the IEEE 1547.3 language verbatim and just adding "Shall" to the items could cause overly stringent and inflexible cybersecurity requirements. To address those concerns, the subgroup developed two sets of recommendations:

- A set of Phase 1 items that should be proposed as initial requirements (see the *Phase 1 Primary DER Cybersecurity Requirements* document in Appendix A derived from the assessment of the IEEE 1547.3 Section 5 items in Annex B), and
- Recommendations to the CPUC that identify the implementation paths on how the initial requirements could be made operational and how new requirements could be integrated in the future.

The SIO-CS identified several paths forward that could be recommended to the CPUC:

A. Path A. Wait for California legislation to develop cybersecurity requirements for DER

B. Path B. Wait for the Department of Energy and NARUC to develop cybersecurity requirements for DER

C. Path C. Wait for the IEEE 1547 revision to develop cybersecurity requirements for DER

D. Path D. Recommend that the CPUC provides guidance only and leave the DER cybersecurity requirements up to utilities

E. Path E. Recommend that the CPUC defines specific DER cybersecurity requirements, including testing cases

F. Path F. The CPUC recommends (but does not mandate) that the DSOs use the SIO-CS Phase 1 Primary DER Cybersecurity Requirements

G. Path G. The CPUC initiates Phase 2 DER Cybersecurity Requirements based on SIO-CS Phase 1

H. Path H. Recommend that the CPUC endorses the establishment of testing and certification programs that would meet the SIO-CS Phase 1 DER cybersecurity testing and certification needs

Proposed CPUC Regulatory Paths. Ultimately the SIO-CS recommended that the CPUC pursue paths F, G, and H in parallel, namely:

- **Path F: The CPUC *recommends* (but does not mandate) that the DSOs use the SIO-CS Phase 1 Primary DER Cybersecurity Requirements** in the short term (until the results from Path G are finalized) as part of their cybersecurity requirements for DER facilities. DSOs could optionally undertake pilot projects to test the applicability and/or efficacy of some cybersecurity requirements in different scenarios.
  - PG&E, SDG&E, and other stakeholders who expressed their opinions were in consensus with this approach as Path F.
  - SCE was not in consensus with this approach as Path F.
- **Path G: The CPUC initiates the development of Phase 2 DER Cybersecurity Requirements.** This could be split into 2 efforts:
  - **Path G1**: The CPUC initiates a Phase 2 cybersecurity working group, building on the SIO-CS. This working group should be comprised of the California DSOs and DER stakeholders to review and update the SIO-CS Phase 1 Primary DER Cybersecurity Requirements based on input from the DOE/NARUC "*Cybersecurity Baselines for Electric Distribution and DER*", the UL 2941 Outline of Investigation, the "SunSpec Cybersecurity Certification" document, the new CPUC-SCE VGI effort,[8] SAE J3400, and other cybersecurity requirements sources. The updated Primary DER Cybersecurity Requirements would include qualifications on where they are (or are not) applicable and flexibility on where they would be deployed since cybersecurity threats are expected to change over time.
  - **Path G2:** The CPUC initiates and/or supports the establishment of a Cybersecurity Coordination Forum comprised of cybersecurity experts from different organizations. This forum would provide additional input to the Phase 2 DER Cybersecurity Requirements.

[8] *Southern California Edison Company's (U 338-E) Vehicle-grid Integration Strategies Annual Report for 2022, March 15, 2023 in Rulemaking R.18-12-006 to Continue the Development of Rates and Infrastructure for Vehicle Electrification*

- **Path H: The CPUC endorses the establishment of testing and certification programs** that would meet the SIO-CS Phase 1 DER cybersecurity testing and certification needs, such as those being developed by UL and SunSpec.

Challenges. Cybersecurity is complex and challenging, where one solution does not fit all situations. Cyber threats are constantly evolving while cybersecurity technologies are continuously advancing to counter those threats. Interoperability between different implementations of cybersecurity techniques is also challenging: the cybersecurity requirements in the Phase 1 Primary DER Cybersecurity Requirements are "What" requirements, addressing What cybersecurity requirements should be met, but not "How" they should be met (e.g., which cryptographic suites, whether multi-factor authentication is required for access to which systems). Different implementations could then use different methods for achieving the same security results, but nonetheless not be interoperable. Thus, the DSOs should still identify some of the "How" cybersecurity requirements to better achieve interoperability, such as requiring default cryptographic suites and standardized security logging formats.

Consensus/Non-Consensus. By agreement of the SIO-CS Subgroup, the contents of Annex A: *Phase 1 Primary DER Cybersecurity Requirements* reflect the **consensus by ALL parties** on the inclusion of the specific cybersecurity requirements extracted from the IEEE 1547.3 recommendations. However, although SCE agreed with the contents of Annex A, they do not agree with Path F in which the CPUC recommends the use of Annex A by DSOs on a short term basis.

There were also qualifications where the parties generally agreed with the inclusion of a requirement but felt that additional rewording or qualifications by DER type and/or size must be included. It is for this reason that the Path G1 is recommended: The CPUC initiates a cybersecurity working group to update the Phase 1 Primary DER Cybersecurity Requirements to Phase 2 DER Cybersecurity Requirements, based on recent efforts by other groups.

Contents

Figures

1 Introduction

1.1 Scope of the SIOWG Cybersecurity Subgroup

The CPUC's Rulemaking 21-06-017, "*Order Instituting Rulemaking to Modernize the Electric Grid for a High Distributed Energy Resources Future*", identified 3 Tracks, of which Track 3 was defined as "*Smart Inverter Operationalization and Grid Modernization Planning*". Phase 1 of Track 3 established a Smart Inverter Operationalization Working Group (SIOWG) to address 3 topics, of which cybersecurity was identified as the 3rd topic. The scope of this cybersecurity effort is defined as, "*What existing cybersecurity standards should be applied for smart inverter operationalization and DERMS to ensure communications between the equipment and management systems are secure (e.g., Institute of Electrical and Electronics Engineers (IEEE) 1547.3)?*"

The scope of the SIOWG Cybersecurity Subgroup (SIO-CS) was further elaborated during the initial meetings to clarify where the cybersecurity requirements ought to be applicable:

- *The Cybersecurity Subgroup of the SIOWG shall determine the cybersecurity requirements and/or recommended practices for Smart Inverter-based Distributed Energy Resources (DER) to help ensure security for the SIOWG use cases and associated DER types selected for prioritization.*
- *These cybersecurity requirements and/or recommended practices shall address:*
  - *DER, including the individual DER units, which are directly (in front of meter) or indirectly (behind the meter) interconnecting to the grid*
  - *The DER stakeholders, including DSO DERMS/SCADA, aggregator energy management systems, DER owner/operator systems, DER gateways, manufacturers, and third-party installers/maintainers*
  - *Communication networks, protocols, and related equipment between the DER and the stakeholder systems*
- *These cybersecurity requirements and/or recommended practices shall be based on existing cybersecurity standards and guidelines. Where cybersecurity standards or guidelines are still under development, such as IEEE 1547.3[9], these may be considered.[10]*
- *Specific gaps in existing cybersecurity standards and guidelines shall be identified by the Cybersecurity Subgroup to the extent that resolving the gaps is necessary for implementation of the prioritized SIOWG use cases.*

1.2 Report Overview

This report describes the process used by the Smart Inverter Operationalization Cybersecurity Subgroup (SIO-CS) to develop recommendations on cybersecurity for the CPUC. Those recommendations are expected to become the principal input into the SIO-CS Staff Proposal that will be prepared for the

[9] *IEEE Std 1547.3-2023 is now a standard.*

[10] *See Section 2.2 for discussion of other ongoing efforts impacting cybersecurity.*

CPUC. If these recommendations are accepted, they would give the CPUC both an immediate plan of action as well as a long-term process roadmap. The report is divided into the following sections:

- Background on Cybersecurity for DER, including the importance of this effort and a review of other relevant cybersecurity efforts.
- Smart Inverter Operationalization Cybersecurity Subgroup, including goals and deliverables
- Regulatory alternatives for achieving the goals
- Subgroup member qualifications on deliverables

The documents to be delivered to the CPUC include:

- This SIO Cybersecurity Subgroup Working Group report covers the process used and the recommendations developed for the *Phase 1 Primary DER Cybersecurity Requirements* document *(s*hown in *Annex A)*. When combined with party comments, these will be used as the basis for creating the Staff Proposal.
- The Staff Proposal will **propose** what the CPUC **should** do with the *Phase 1 Primary DER Cybersecurity Requirements* document.
- The Phase 1 Primary DER *Cybersecurity Requirements* document is the first step in a phased approach for developing specific cybersecurity "**shall**" requirements for DER, power control systems, communication networks, and associated connected equipment which are interconnected to the DSO grid, based on these items described in Section 5 of IEEE Std 1547.3-2023. These cybersecurity requirements cover more than just the communications between DSOs and DERs since cybersecurity must be integral to the entire environment.

The SIO Cybersecurity Subgroup recognized that more discussions will be necessary on exactly how cybersecurity requirements can be incorporated into a CPUC proceeding, including some "flexibility" and/or "discretion" on when certain aspects might be required by the DSO for which types and sizes of implementations.

1.3 Terms and Definitions

1.3.1 Terms

Acronym	Meaning
ADMS	Advanced Distribution Management System
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CSIP	Common Smart Inverter Profile
DER	Distributed Energy Resource
DER Facility	{equivalent to} Generating Facility
DER Operator	{equivalent to} Generating Facility Operator
DER System	{equivalent to} DER

Acronym	Meaning
DERMS	Distributed Energy Resource Management System (of the DSO)
DOE	Department of Energy
DOT	Department of Transportation
DSO	Distribution System Operator
EEI	Edison Electric Institute
EMS	Energy Management System
EPS	Electric Power System
EV	Electric Vehicle
FDERMS	Facility DER Management System
IBR	Inverter-Based Resource (see IEEE 2800)
IOU	Investor-Owned Utility, e.g., PG&E, SCE, SDG&E
ISO	Independent System Operator
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OI	Outline of Investigation (UL term)
PCC	Point of Common Coupling == metering point == service point
PCS	Power Control System (as used in this report)
POC	Point of Connection
POI	Point of Interconnection
POU	Public Owned Utility
PUC	Public Utility Commission
SBOM	Software Bill of Materials
SIWG	Smart Inverter Working Group
SIOWG	Smart Inverter Operationalization Working Group
SIO-CS	Smart Inverter Operationalization Cybersecurity Subgroup
UL	Underwriters Laboratory

1.3.2 Definitions

The following are some definitions of terms used in this report. Many come from IEEE Std 1547-2018. Where a term is used in this report but not found here, it may be found in IEEE 1547-2018. Some definitions may change as IEEE 1547 is revised.

- **ADMS**. A software platform that supports the full suite of distribution management and optimization. An ADMS includes functions that automate outage restoration and optimize the performance of the distribution grid. ADMS functions being developed for electric utilities include fault location, isolation and restoration; volt/voltampere reactive optimization; conservation through voltage reduction; peak demand management; and support for microgrids and electric vehicles. [Source: Gartner IT Glossary]
- **ADMS/DERMS.** Combined distribution and DER energy management systems. Sometimes used in this combination to indicate the joint assessments of both the distribution system and the interconnected DER characteristics and capabilities.
- **Aggregator.** An entity that aggregates one or more DER systems for purposes of DER monitoring, DER energy management, and/or participation in the capacity, energy and/or ancillary service markets of the DSOs, RTOs, and/or ISOs.
- **Business Case.** Description of business objectives or purposes that could be provided through regulations, procedures, and/or technology. Typically, business cases stay at a high level to focus on ***what*** or ***why*** a process is needed, but ***not how*** that process might be implemented.
- **Distributed Energy Resource (DER).** A source of electric power that is not directly connected to a bulk power system. DER includes both generators and energy storage technologies capable of exporting active power to an EPS. An interconnection system or a supplemental DER device that is necessary for compliance with this standard is part of a DER.
- **Distributed Energy Resources Management System (DERMS).** A platform which helps distribution system operators (DSO) manage their distribution systems that include significant numbers of distributed energy resources (DER).
- **Distributed Energy Resource (DER) operator.** Entity responsible for management and operation of their DER units and DER systems.
- **Distributed Energy Resource (DER) system.** Any grouping of DER units acting as a system. Equivalent to “DER” as defined in IEEE 1547-2018.
- **Distributed Energy Resource (DER) unit**. An individual DER device inside a group of DER that collectively form a system.
- **Distribution System Operator (DSO)**. Entity responsible for ongoing planning and operation of the distribution system. In California, the DSO is the same as the distribution DSO, e.g. an DSO or POU.
- **Facility DER Energy Management System (FDERMS).** A platform which helps DER operators manage the distributed energy resources (DER) within their facility. Alternate terms include Customer Energy Management System, Power Control System, Generating Facility Management System.
- **Generating Facility (aka. DER Facility)**. A facility containing generating equipment.

- **IEEE Std 1547-2018.** IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.
- **IEEE Std 1547.3-2023.** Draft IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems.
- **Load**. Devices and processes in a local EPS that use electrical energy for utilization, exclusive of devices or processes that store energy but can return some or all of the energy to the local EPS or Area EPS in the future.
- **Point of Common Coupling (PCC).** The point of connection between the Area EPS and the Local EPS. (IEEE Std 1547-2018). The transfer point for electricity between the electrical conductors of Distribution Provider and the electrical conductors of Producer. (Rule 21)
- **Point of Connection (POC).** Point where the DER unit is electrically connected to the Local EPS (BTM) or to the Area EPS (FTM).
- **Power Control System (PCS)**. A system consisting of one or more device(s) that electronically limits or controls the steady state AC and/or DC current(s) or power on conductors or busbars to programmable limit(s) or level(s). [Source: draft UL 3141 Outline of Investigation]
- **Use Case**. Description of technical methods for supporting Business Cases. Use Cases may also be high level or may be detailed but are focused on ***how*** the process might be implemented.

2 Background on Cybersecurity for DER

2.1 Importance of Cybersecurity for DER

The electric power system is critical because electrical energy is vital to all sectors of society, including the industrial, commercial, and residential sectors. But due to the increasing numbers and different sizes of DER interconnected to the power system – ranging from large power plants down to residential rooftop solar systems – the operation of the power system is being progressively restructured, requiring the use of new technologies and posing novel and complex engineering challenges. DER systems, like all generators, can introduce grid safety and reliability vulnerabilities, thus necessitating an increased level of control and operational information to be exchanged amongst the many dispersed DER installations and the varied types of stakeholders usually from different types of organizations. Cybersecurity for the DERs themselves, and for managing DERs, is therefore looming as one of the key challenges to ensure the safe and continued operation of this critical cyber-physical system.

From a DSO's perspective, cybersecurity for their interactions with DERs is essential for secure, reliable, and resilient operation of the power system. Interconnected DERs could have common vulnerabilities and therefore could run the risk of simultaneously causing the disconnection of massive quantities of power generation, which could lead to localized power disruptions or even cascading system collapse. Individually, each DER may not significantly affect the power grid, but in aggregate, they have the potential to provide excellent energy services, to cause extensive energy disruptions, or both.

Cybersecurity is not just about protection against malicious actors. In addition to protection from deliberate attacks, DERs also need to be protected against communication network failures, inadvertent errors, equipment malfunctions, and natural disasters.

Resilience should be the overall strategy for ensuring business continuity for power system operations. Resilience in this case is defined as mitigation or rapid recovery of a system from a disruptive event whether cyber or physical. Resilience is not just a technical issue; it must involve an overall business approach that combines cybersecurity techniques with system engineering and operations to prepare for and adapt to changing conditions, and to withstand and recover rapidly from disruptions. Resilience includes security measures that can mitigate impacts, not only before incidents (identify and prevent), but also during such incidents (detect and respond) and after incidents have been resolved (recover).

Many of the security requirements that are critical to Operational Technology (OT) systems can utilize Information Technology (IT) cybersecurity techniques: risk assessment, confidentiality, integrity, and availability. However, these requirements' priorities will be different between IT and OT systems, with OT systems generally prioritizing availability over confidentiality and integrity.

Increasing adoption of new technologies to improve operational efficiencies and services to grid modernization can also expand the attack surfaces and increase the cybersecurity risks that may have serious impacts on grid operations. Adopting cybersecurity risk guidelines is a necessary measure that enables organizations to identify vulnerabilities and prioritize risk mitigations. This is particularly true for the DER implementations since there is little history in performing risk assessments for these emerging technologies.

Testing cybersecurity for DERs also raises many questions. Such testing may ultimately include not only the type-testing of individual devices with well-defined systems, networks, and communication protocols, but also may include the testing of systems and combinations of these elements at specific sites. Cybersecurity testing would also require tests between equipment from different organizations who may not have coordinated their cybersecurity procedures and technologies sufficiently. DERs are physically located throughout a DSO's territory and communication channels could consist of many different media and protocols, making lab testing difficult if not impossible.

Sites with many different DER types will need to have both the individual equipment type-tested and, in some cases, the whole facility site-tested. Although lab "type testing" of a specific system (gateway, power control system, facility energy management system) may simplify any additional site testing, additional cybersecurity testing of combinations of networks, protocols, systems, and devices would still be needed at specific sites. Smaller, "cookie-cutter" installations may not need extensive site testing, but the larger, more heterogeneous installations will need comprehensive site testing – both for functionality and for cybersecurity. Additional discussion is warranted on specific approaches based on facility size and use case.

Such cybersecurity testing programs are still in their infancy and will need time, testing technologies, and experience to fully achieve their goals.

2.2 Existing Cybersecurity Strategies, Regulations, and Standards

2.2.1 Cybersecurity Standards and Guidelines

Figure 1 illustrates key cybersecurity standards and guidelines for smart energy operational environments[11]

[11] *An enlarged version is available in Annex C.1.*

It is useful to categorize the key cybersecurity standards and guidelines. For instance, some standards and guidelines are focused on the high-level organizational security requirements and more detailed recommended controls (*What*), while other standards focus on the technologies that can be used to supply these cyber security controls (*How*). A third category provides guidance on how to comply with the standards (*Process toward Compliance*).

In addition, the standards can be categorized for different focus areas. Many are identified as being generally applicable to IT environments (*purple*), while others are focused on the organizational and procedural aspects for energy operational environments (*yellow*). A few standards address the more detailed aspects where technologies can be used to meet the requirements (*blue*). Although the figure shows these categories in boxes in specific columns and with specific colors, these standards do overlap in many areas, often stating the same requirement with different words.

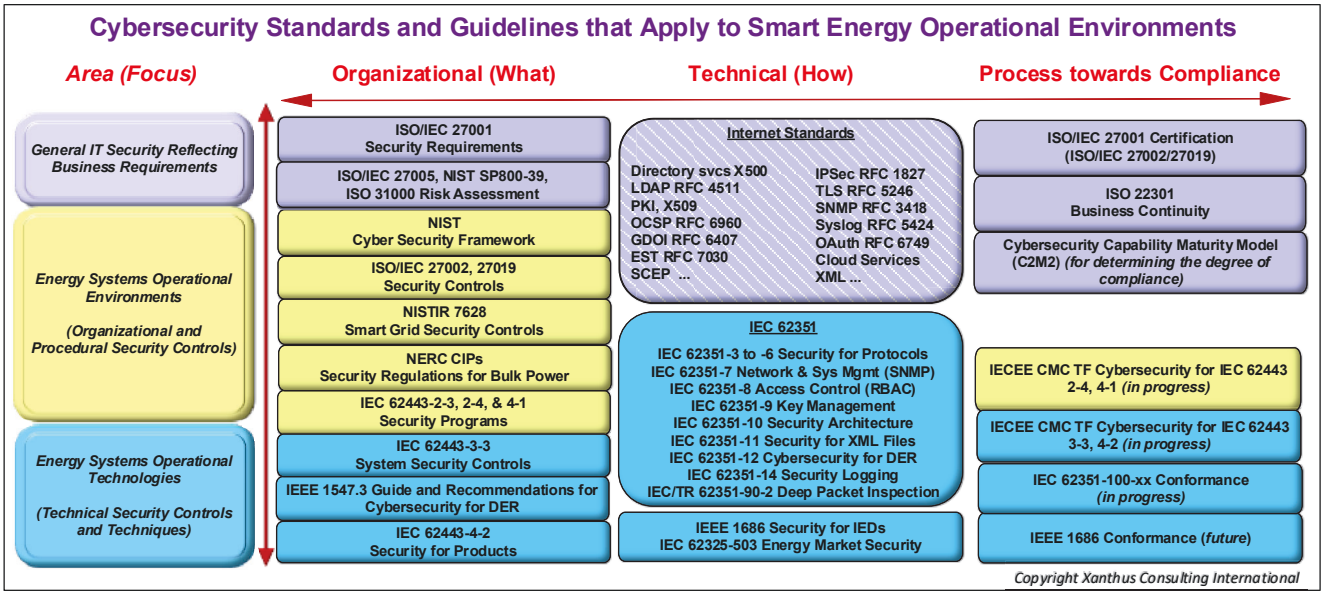


Figure 1: Cybersecurity standards and guidelines for the Smart Energy OT environment

The following is a list of the key standards and guidelines pertinent to distribution systems and DER:

- IEEE Cybersecurity Standards
  - IEEE 1547.3, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
  - IEEE 1686, IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities
- NIST cybersecurity documents
  - NIST Cybersecurity Framework (CSF)
  - NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
  - NIST 7628, Guidelines for Smart Grid Cybersecurity
- IEC Cybersecurity Standards
  - IEC 62443 series, Cybersecurity for Operational Technology in Automation and Control Systems
  - IEC 62351 series, Cyber Security Series for the Smart Grid

- UL Cybersecurity for DER and Inverter-Based Resources (IBR)
  - UL 2941 Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, (currently being updated)

It is important to note that there are other cybersecurity guides and programs that could be studied in the future for their applicability to DER. This is a small subset of existing cybersecurity efforts:

- NERC Critical Infrastructure Protection (CIP)[12] (only applicable to DER larger than 75 MW)
- DOT-VNTSC-NAVY-20-01[13]
- CISA Secure Software Development Attestation Form[14]
- ARM-PSA[15]
- CTIA Cybersecurity Certification Test Plan for IoT Devices[16]
- NISTIR 8259[17]
- Linux Foundation OpenSSF[18]
- CIS Controls Internet of Things Companion Guide[19]

2.2.2 National Cybersecurity Strategy 2023

In March 2023, the Federal Government released a National Cybersecurity Strategy document. The key sections for DER cybersecurity are quoted below: [20]

Cybersecurity for Critical Sectors

> *"The Federal Government will use existing authorities to set necessary cybersecurity requirements in critical sectors. Where Federal departments and agencies have gaps in statutory authorities to implement minimum cybersecurity requirements or mitigate related market failures, the Administration will work with Congress to close them. Where states or independent regulators have authorities that can be used to set cybersecurity requirements, the Administration will encourage them to use those authorities in a deliberate and coordinated manner.*
>
> *Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance—including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of*

[12] *https://www.nerc.com/Pages/default.aspx*

[13] *https://rosap.ntl.bts.gov/view/dot/43606/dot_43606_DS1.pdf?*

[14] *https://www.cisa.gov/sites/default/files/2023-11/Secure%20Software%20Development%20Attestation%20Form_508c.pdf*

[15] *https://www.arm.com/architecture/psa-certified*

[16] *https://ctiacertification.org/program/iot-cybersecurity-certification/*

[17] *https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series*

[18] *https://openssf.org/*

[19] *https://www.cisecurity.org/insights/white-papers/cis-controls-v8-internet-of-things-companion-guide*

[20] *https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf*

Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity— and be agile enough to adapt as adversaries increase their capabilities and change their tactics. In setting cybersecurity regulations for critical infrastructure, regulators are encouraged to drive the adoption of secure-by- design principles, prioritize the availability of essential services, and ensure that systems are designed to fail safely and recover quickly. Regulations will define minimum expected cybersecurity practices or outcomes, but the Administration encourages and will support further efforts by entities to exceed these requirements.

Further, these and other critical sectors rely upon the cybersecurity and resilience of their third-party service providers. Cloud-based services enable better and more economical cybersecurity practices at scale, but they are also essential to operational resilience across many critical infrastructure sectors. The Administration will identify gaps in authorities to drive better cybersecurity practices in the cloud computing industry and for other essential third-party services, and work with industry, Congress, and regulators to close them."

Strategic Objective 4.4: Secure Our Clean Energy Future

"Our accelerating national transition to a clean energy future is bringing online a new generation of interconnected hardware and software systems that have the potential to strengthen the resiliency, safety, and efficiency of the U.S. electric grid. These technologies, including distributed energy resources, "smart" energy generation and storage devices, advanced cloud-based grid management platforms, and transmission and distribution networks designed for high-capacity controllable loads are far more sophisticated, automated, and digitally interconnected than prior generations of grid systems.

As the United States makes a generational investment in new energy infrastructure, the Administration will seize this strategic opportunity to build in cybersecurity proactively through implementation of the Congressionally-directed National Cyber-Informed Engineering Strategy, rather than developing a patchwork of security controls after these connected devices are widely deployed. The Administration is coordinating the work of stakeholders across the Federal Government, industry, and SLTT to deploy a secure, interoperable network of electric vehicle chargers, zero-emission fueling infrastructure, and zero-emission transit and school buses. DOE, through efforts such as the Clean Energy Cybersecurity Accelerator (CECA) and the Bipartisan Infrastructure Law-directed Energy Cyber Sense program, and the National Labs are leading the government's effort to secure the clean energy grid of the future and generating security best practices that extend to other critical infrastructure sectors. DOE will also continue to promote cybersecurity for electric distribution and distributed energy resources in partnership with industry, States, Federal regulators, Congress, and other agencies."

2.2.3 Edison Electric Institute (EEI)

The Edison Electric Institute (EEI)[21] stated the need for coordination on DER cybersecurity. They were concerned that a patchwork of cybersecurity regulations would lead to an inefficient focus on compliance rather than actual improvements in safety, reliability, and resilience. Therefore, they urged

[21] *https://www.eei.org/*

a collaborative effort of stakeholders including state regulators, the DOE, FERC, NIST, NERC, electric companies, as well as DER developers, integrators, operators, providers, and vendors.

2.2.4 DOE and NARUC

The National Association of Regulatory DSO Commissioners (NARUC), with support from U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, is developing a Cybersecurity Baseline(s) which would be applicable to distribution DSOs and to the distributed energy resources (DER) that interconnect with the distribution grid. Once the baselines are completed, additional efforts will include the development of implementation and compliance guidance for states who decide to adopt the baselines as requirements. The status can be found in the DOE/NARUC "*Cybersecurity Baselines for Electric Distribution and DER version 1.4*".[22]

2.2.5 Legal Cybersecurity Privacy Requirements from California

Legal requirements for cybersecurity information privacy already exist, as noted below.

> ***California SB 327, Jackson. Information Privacy: Connected Devices, that was signed by the Governor on September 28, 2018.[23]***
>
> As quoted from this bill: *"Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.*
>
> *This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.* "

2.3 DER Cybersecurity Requirements

2.3.1 DER Environment

As more computers and systems have become interconnected, deliberate cyber-attacks have become more prevalent and inadvertent cyber failures and errors are affecting more business processes. In

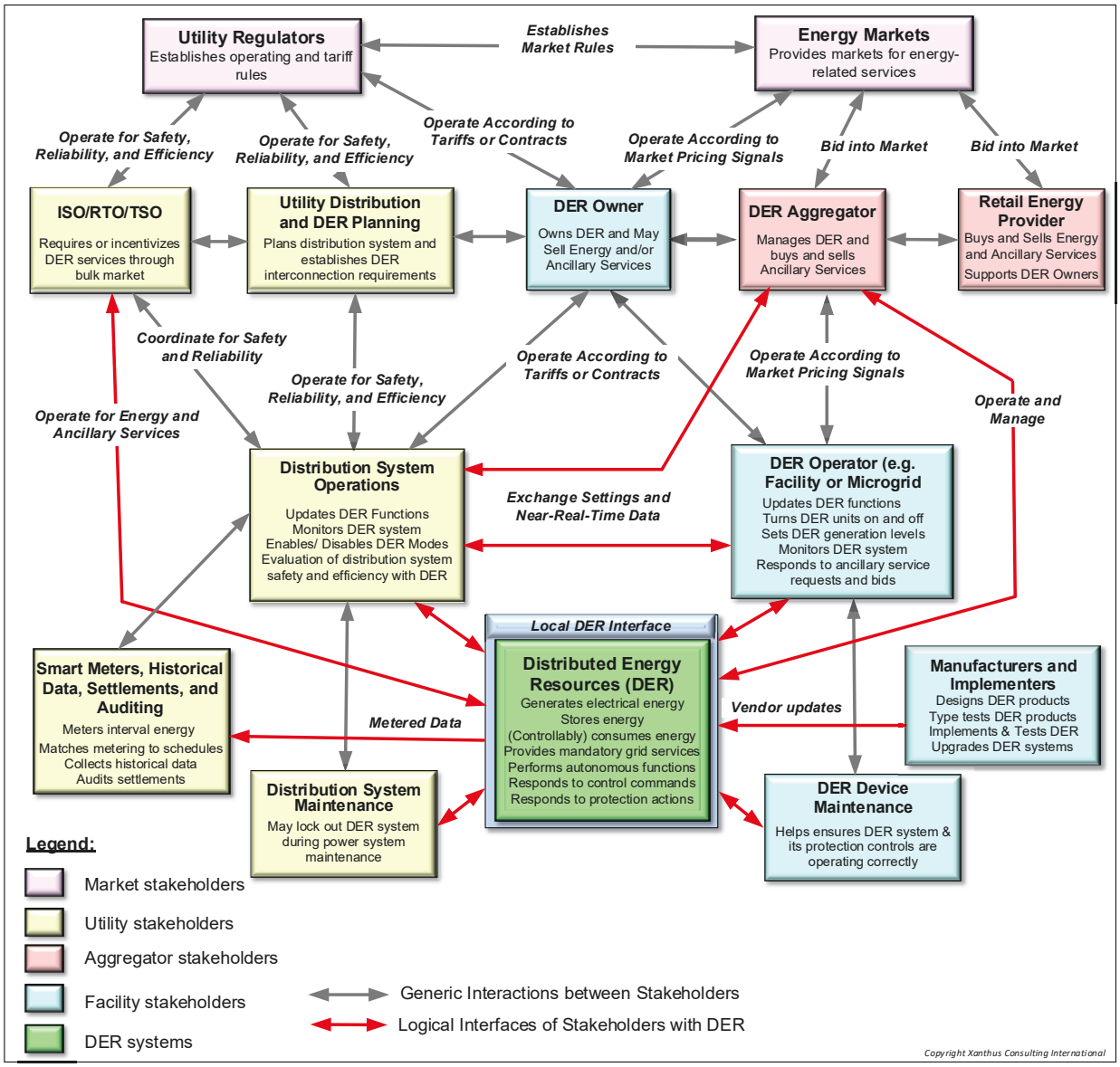
---

[22] *DOE/NARUC, Cybersecurity Baselines for Electric Distribution Utilities and DER, published February 2024, https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/*

[23] *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327*

response, many standards and guidelines have been developed to identify and even mandate best practices for minimizing these cyber risks. Although the main focus of cybersecurity has been in the Information Technology (IT) domain, increasingly the need for cybersecurity in the "Operational Technology (OT)" domain has become important as devices and operational systems have become more interconnected, and as a safe and resilient smart grid has become increasing critical to the modern world.

DERs were not viewed as critical in the past since they were generally small in size and number, and for the most part could be viewed as simply "negative loads" or demand reducers, just small variations to existing loads. However, now and into the High DER future, DERs are impacting the grid and also able to provide services to it. The enabling technology for these services is communications, where the need to exchange information between the many DER stakeholders, as illustrated in Figure 2[24], is vital to a safe and resilient grid. These communications requirements also necessitate more robust cybersecurity. For this reason, many cybersecurity strategies, regulations, and standards are starting to focus on DER cybersecurity requirements.



[24] *An enlarged version of this diagram is available in Annex C.2*

Figure 2: Stakeholders in the DER Environment

2.3.2 DSO-DER Architecture with Gateways for Cybersecurity

Although detailed DSO-DER architectures may vary significantly and, except for direct DSO SCADA control, DSO-DER architectures need to use some form of gateways for cybersecurity, privacy, and management of information flows between the DSO systems and the aggregator systems or the facility systems – see Figure 3[25].

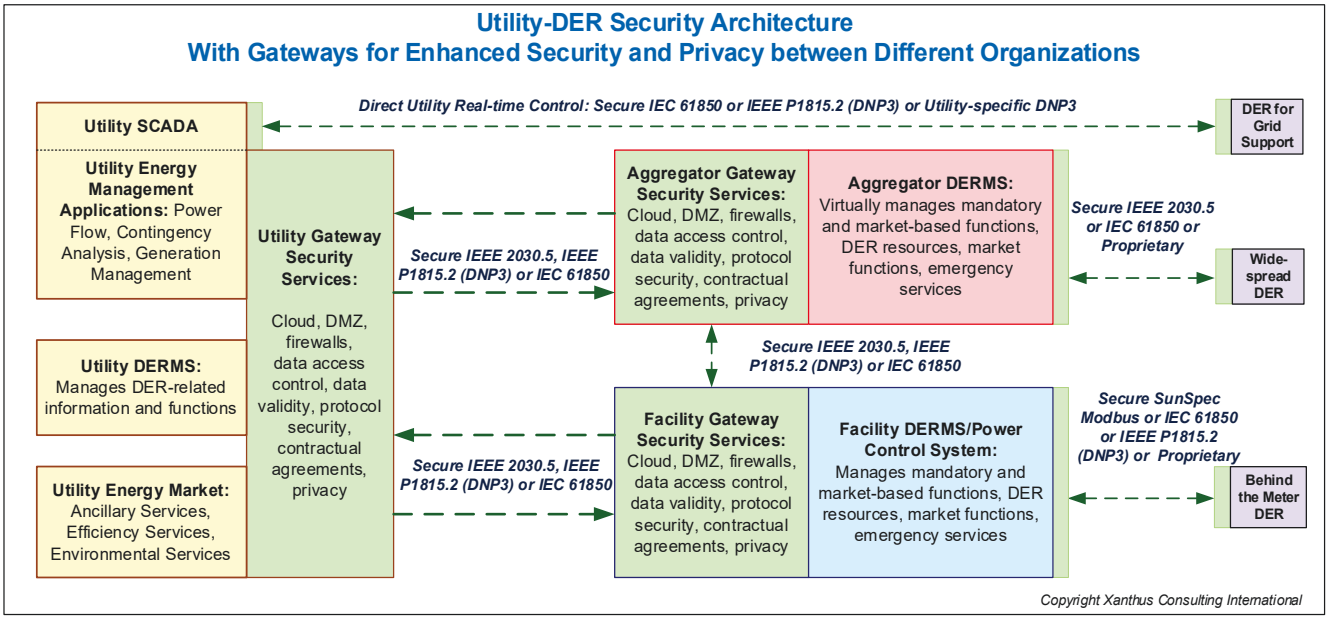


Figure 3: Generic DSO-DER Architecture with Gateways for Cybersecurity

2.3.3 Correlations between DER Cybersecurity Requirements

Most of the cybersecurity standards and guidelines mentioned above are either general or are focused on areas other than DERs. Some of the key cybersecurity efforts focused explicitly on DERs are identified in this section. Although all these cybersecurity documents have provided excellent strategies and recommendations, only one was available at the beginning of this SIO-CS working group: IEEE 1547.3.[26] Unfortunately, IEEE 1547.3 is not a standard- it is a set of guidelines. Nonetheless, it was the only DER-focused source available in mid-2022 and was therefore used as the basis for the SIO-CS effort.

There is a considerable amount of work required to convert IEEE 1547.3 into testable requirements, and recent priorities at the federal level have highlighted the need for additional requirements. Given the relatively recent work to develop DER cybersecurity requirements, a very preliminary draft of correlations across these recent efforts was developed as a step to developing a comprehensive set of DER cybersecurity requirements from 3 different sources:

- SIO-CS cybersecurity requirements (selected and derived from IEEE 1547.3)

[25] *An enlarged version of this diagram is available in Annex C.3.*

[26] *https://standards.ieee.org/ieee/1547.3/10173/*

- UL 2941 Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources (from January 13, 2023)[27]
- SunSpec Cybersecurity Certification Phase 1 Requirements[28]

These correlations are far from perfect, given that the focus, style, and wordings can be quite different, even within the same scope of a requirement. For instance, the UL requirements are often more detailed, while the SunSpec requirements are very focused on device certification. In many cases, the same requirement from one source could be correlated with multiple requirements from different sources.

What can be derived from these correlations? Broadly speaking there are good correlations in some areas between these sources. These areas include:

- Network port handling
- Transport protocol security
- Authentication for access control
- Authorization, in some cases through role-based access control
- Security logging

However, each source also has certain "gaps" due to their specific focuses:

- **SIO-CS Cybersecurity Requirements**. Since these were selected from IEEE 1547.3, not all recommendations became requirements and some areas like cryptography were not covered in depth.
  - Cryptography was not addressed in detail (e.g., algorithms or cipher suites)
  - Confidentiality was not directly addressed
  - Certificate and key management were not addressed directly, but through reference to IEC 62351-9
  - Risk management issues were deemed to be "should" and so were not included
  - Application layer protocol security was identified but not required
- **UL 2941 Cybersecurity Requirements.** The focus of UL is on type testing of devices, so issues related to system or site testing were not included.
  - Network management was not directly addressed except for port blocking and logging
  - Patch management was not addressed
  - Power logs were not mentioned
  - Although risk management was addressed, it focused on device risk and not cross-organizational risk
  - Application layer protocol security was only addressed for DNP3
- **SunSpec Cybersecurity Requirements**. The focus of SunSpec is type testing of devices, so like UL 2941, issues related to system or site testing were not included.
  - Network management was not directly addressed except for port blocking and logging

[27] *https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity*

[28] *https://sunspec.org/sunspec-cybersecurity-certification-program-2024-requirements-test-procedures/*

- System authentication was not addressed
- Rule Based Access Control (RBAC) was not addressed
- Data security only addressed the avoidance of deprecated cryptographic algorithms of data in transit
- Cryptography was not addressed in detail
- Key management was not addressed
- Patch management was not addressed
- Risk management was not addressed

In addition, all three efforts are light on supply chain management, including inventory, tracking, and bill of materials. This area is now a focus for federal-level efforts in Cybersecurity and Infrastructure Security Agency (CISA) addressing "Software Bill of Materials" (SBOM): Executive Order 14028, Improving the Nation's Cybersecurity.[29]

None of these cybersecurity requirements have been "tested" in real world environments with actual DER units, DER plants, or gateways to DER facilities, although both the UL and SunSpec requirements are focused on testability. It may be a significant challenge to achieve such testability and will require additional rounds of refining the requirements.

Additional cybersecurity "requirements" could be even more difficult, such as risk management, cross-organizational agreements, supply chain management, and coping strategies for the inevitable security breaches. But "baby-steps" are needed to achieve any "Phase 1" goal.

3 Smart Inverter Operationalization Cybersecurity (SIO-CS) Subgroup

3.1 Formation of the SIO-CS Subgroup

As stated in the Scoping Memo, the overall goal of the SIO CS subgroup was to determine "*What existing cybersecurity standards should be applied for smart inverter operationalization and DERMS to ensure communications between the equipment and management systems are secure (e.g., Institute of Electrical and Electronics Engineers (IEEE) 1547.3)?"*

In response to the High DER Future cybersecurity topic of R.21-06-017, a Smart Inverter Operationalization Cybersecurity Subgroup (SIO-CS) was formed. Outreach to other groups, including the Smart Inverter Operationalization Working Group (SIOWG), the Smart Inverter Working Group (SIWG), and other CPUC lists requested interested parties to join this group. Eventually about 80 people joined the group, including personnel from the DSOs, DER aggregators, DER owners, consultants, academics, and CPUC staff, although usually only a smaller group actively participated in the meetings.

[29] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

3.2 Development of the Phase 1 Primary DER Cybersecurity Requirements

Starting in May 2022, the SIO-CS subgroup met bi-weekly. The first discussions centered around what goals could be achieved and how to achieve those goals. The first major decision was to use IEEE 1547.3, specifically Section 5, as the basis for which cybersecurity requirements and recommendations should be assessed for interconnected DER systems. At that time, it was the only cybersecurity standard that focused on DER, even though it only included recommendations, not requirements. Additional discussions then addressed what documents to deliver to the CPUC, and importantly, what approaches might be suggested to the CPUC for achieving the goals of the SIO-CS subgroup.

To facilitate these discussions, a table was created which included all the items from IEEE 1547.3 Section 5 as the first column in a table, with other columns dedicated to assessment from different organizations and a column for comments. These organizations included the SunSpec Alliance, ASE Systems, Pacific Gas & Electric (PG&E), Southern California Edison (SCE), and eventually the National Renewable Energy Laboratory (NREL).[30]. The organizations were asked to assess whether each of the Section 5 cybersecurity items ought to be a "**Shall**" cybersecurity requirement, a "**Should**" cybersecurity recommendation, or "N/A" (not applicable).

During the bi-weekly meetings, there were discussions on each cybersecurity item in IEEE 1547.3 Section 5, and qualifications and comments were added. In some cases, the organizations revised their initial assessments due to the discussions and the addition of qualifications. **The goal was to identify those cybersecurity items which all members agreed** should be reworded to make them **"Shall" requirements, potentially with modifications of the Section 5 item to constrain the requirement**.

It also became clear that a phased approach toward achieving this goal would work better than trying to get agreement for all items. Multiple phases would permit updates to the initial assessments of the Section 5 items as cybersecurity measures are rolled out over time and as better understandings of the cybersecurity risks would become apparent. Therefore, the first phase would not be all inclusive but would start with basic cybersecurity requirements with the anticipation that additional cybersecurity requirements and recommendations will follow in subsequent phases.

In addition, during the latter part of the process when there was debate on which items should be a "Shall" requirement of Phase 1, there was concern about how these requirements would be used by the CPUC. The wording of IEEE 1547.3 is that of a guide, not a standard with testable requirements. Thus, taking the IEEE 1547.3 language verbatim and making them all "Shall" requirements could lead to a confusing, incoherent, inflexible, and narrow set of rules that would not be appropriate in all situations. As a result, the subgroup felt the need to provide not only a set of Phase 1 proposed controls that should be put forward as proposed initial requirements (see the *Phase 1 Primary DER Cybersecurity Requirements* document in Annex A and the full assessment of the IEEE 1547.3 Section 5 items in Annex B), but implementation recommendations that addresses how the requirements could be used as well as how future requirements could be integrated.

3.3 Changes to the SIO-CS Vision over its Lifetime

Due to the rapid developments in the cybersecurity industry during the year-and-half that the SIO-CS Subgroup has met, it lacked the time required to solidify all language for all requirements. As

[30] *SDG&E switched personnel attending these meetings and therefore did not develop a column of comments. SDG&E was able to provide consensus/non-consensus and qualifications later in the process*

mentioned above, the SIO-CS Subgroup started with the language in IEEE 1547.3, which is a guide, not a standard or certification program. During the time the SIO-CS was meeting, multiple other groups started to develop DER cybersecurity requirements (UL, SunSpec, IEC 62443, DOE). It became clear that it would take significantly more time to produce a SIO-CS requirements document with solid requirements language that would be coordinated with items identified and specified by these other groups.

Furthermore, cybersecurity requirements can never be finalized without including test cases to ensure that those requirements are testable. Finalizing requirements language necessitates writing test procedures to catch the inevitable ambiguities and oversights in the requirements language. Therefore, whichever implementation path the CPUC ultimately decides on will need to address the development of testing procedures, which will then lead to updates to the cybersecurity requirements language.

4 Summary of Phase 1 Cybersecurity Requirements

Annex A presents the details of the Phase 1 Primary DER Cybersecurity Requirements as agreed to as **"Shall"** requirements by the subgroup. As can be intimated by the terms "Phase 1" and "Primary", this set of cybersecurity requirements only addresses some of the basic controls and is not a complete set of requirements.

These requirements are grouped into six of the categories used by IEEE 1457.3. This section presents the highlights of the Phase 1 Primary DER Cybersecurity Requirements in each of those categories. This is not intended to be a comprehensive list but is provided here to give readers a summary of what the requirements cover without needing to read Annex A.

4.1 RA: Risk Assessment and Management

These requirements cover assessing and managing risks from cybersecurity threats. However, the subgroup did not identify any of the IEEE 1547.3 items as **"Shall",** so no Phase 1 requirements exist for this category.

4.2 NE: Network Cybersecurity Requirements

These requirements address the security for networks, including management, logging, monitoring, and the equipment needed to ensure the networks used for communication and control of DERs remain secure.

Requirements in this category include that networks shall be segmented based on trust levels, with public internet access using specific communication protocols. The network boundary and equipment shall be configured to limit access as much as possible while still meeting functional requirements. Additionally, the network shall be monitored with appropriate logging to capture security-related actions.

4.3 AC: Access Control Cybersecurity Requirements

These requirements address user and system authentication and authorization, including specifying password requirements, to access networks and devices. These requirements help guarantee that only

authenticated and authorized users or systems (such as hardware and/or software) have access to DERs and associated networks.

This category includes requirements that:

- Users shall follow specific requirements for passwords, access, and authorization.
- Systems, software, and devices shall follow specific authentication and authorization.
- Access shall be managed to ensure passwords are not shared or set as defaults, secure interfaces are documented, and any access changes are logged.
- Interactions between users, systems, software applications, and devices shall follow the principle of Role-Based Access Control (RBAC) to restrict access based on the role of users and systems.

4.4 DS: Data Security Requirements

These requirements control how data is protected both when stored (data-at-rest) and when communicated or transferred (data-in-transit). Data-at-rest needs to follow rule-based-access-control to limit access to only necessary individuals and organizations. In addition, data-at rest must be secured using appropriate cryptography and security certificates. Finally, data must be sanitized and removed when devices are repurposed, decommissioned, or reset. Data-in-transit must be authenticated by both the sender and receiver using mutually agreed upon security policies. These communication sessions renew their cryptographic keys and are time-stamped to track data interactions.

4.5 SM: Security Management Requirements

These requirements control the lifecycle management of assets (including both hardware and software), management of security patches, and that security events such as detecting malicious code, changes to settings, updates, and deletions are logged and stored. Within this category:

- Assets (such as hardware, installed firmware, software, applications, and external services) shall be tracked. Asset time clocks shall be synchronized and asset upgrades and decommissioning or disposal shall be tracked.
- Patches (such as those developed to respond to identified cybersecurity threats) are implemented, verified, and checked regularly for all assets within a specified timeframe. DER owners shall maintain a record (log) of all patches.
- Security events such as successful and unsuccessful login attempts; Detected malicious code; Detected failure of event logging; Changes to device settings; Software updates and changes; Changes to access controls such as RBAC permissions and roles, account creation, updates, and deletions shall be logged within specific parameters.

4.6 CM: Coping and Recovery Requirements:

The requirement in this category identifies that any security event must be captured and logged with an accurate timestamp by all stakeholders to identify when and where any security issue occurred.

5 Regulatory Alternatives

5.1 Need for Regulatory Cybersecurity Requirements

The CPUC has not developed any regulations related to cybersecurity for DERs and has relied primarily on the DSOs to develop cybersecurity requirements for DERs interconnecting with their systems. However, as more DERs are interconnected to different DSOs, it has become very difficult and expensive for DER vendors and implementers to meet all different cybersecurity requirements. Those difficulties contributed to the development of the IEEE 1547.3 DER cybersecurity recommendations as a first step. However, cybersecurity recommendations are not adequate for ensuring complete compliance or providing true security. For this reason, the CPUC initiated the SIO-CS Subgroup to develop the cybersecurity requirements for the SIOWG use cases and DERs in general.

DER cybersecurity regulations are critical to make DERs implementable and operational. These regulations can help ensure that DER stakeholders meet the cybersecurity requirements through identifying at least basic cybersecurity **requirements** that are **testable**. This is equivalent to the CPUC's development of Rule 21 – or now the reference to the IEEE 1547-2018 for DER functional requirements – and the development of UL 1741 SA and SB for testing those functional requirements.

However, most regulators are not cybersecurity experts and need to rely on outside expertise to identify cybersecurity and testing requirements for DER stakeholders. Different regulatory paths could be taken for the CPUC to accomplish these requirements. Some of these regulatory paths are discussed in the next section.

5.2 Guiding Principles for a DER Cybersecurity Plan

The primary purpose of the SIO-CS Subgroup is to give the CPUC recommendations on developing a plan to secure DERs connected to the distributed grid in California. The results of the SIO-CS efforts, outlined in this Working Group Report, are expected to help direct the recommendations in the upcoming Staff Proposal. Such a plan should be based on standards, should balance the needs of all stakeholders, and should follow ten guiding principles, including:

1. **Principle #1: Make a baseline assessment of cybersecurity readiness**. The state of DER cybersecurity in the distributed grid is unknown. Some companies appear to spend significant resources protecting their products and assets, feeling that the impact of a security incident justifies the resources. Others do not have the expertise or conviction to significantly deter adversaries and appear to spend little. Since a system is only as secure as its weakest link, an adversary would only need to attack weak links to disrupt the grid. Requiring a baseline will help California eliminate the weakest links.
2. **Principle #2: Require the appropriate level of cybersecurity for different types of assets**. There is no such thing as perfect security. Given enough time and resources, any asset can be compromised. Therefore, rather than requiring all assets to implement the maximum amount of security possible, cybersecurity requirements should determine the level of risk that can be accepted within defined circumstances (i.e., use cases) and craft requirements appropriately. In other words, **not all cybersecurity requirements should or could be applied to all DER assets**. DER installations vary significantly by size, location, configuration, and criticality. For these reasons, flexibility is needed in determining which cybersecurity solutions or mitigations might be required, which might be recommended, and which may not be necessary. This

flexibility should reflect the appropriate risk assessments. SCE noted that discussion is warranted to determine which types of DERs should be subject to the proposed cybersecurity requirements.

3. **Principle #3: Encourage resilience and fast recovery from cyber incidents**. Since there is no such thing as perfect security, requirements must include resilience and help ensure distributed grid stakeholders are able to quickly identify, respond to, and recover from cyber incidents and accidents. Stakeholder agreements on who must respond, what actions must be taken, and when, based on the type of cyber incident, must be determined. This level of detail was out of scope for this effort, and DSOs may already require notification if a counterparty is impacted by a cybersecurity incident.
4. **Principle #4: Allocate cybersecurity compliance to different stakeholders.** Different stakeholders (manufacturers, implementers, aggregators, DER owners/operators, and DSOs) need to be responsible for meeting different cybersecurity requirements. Just requiring manufacturers to comply via "type testing" may not ensure security of DERs once they are operating, since network security, access control, security management, and many other aspects might require confirmation and evaluation once a DER site is configured and is operational. DSOs are also subject to NERC CIP requirements as applicable at the system level.
5. **Principle #5: Use risk assessment to balance risk impacts against cybersecurity costs**. The growth of DERs connected to the distributed grid can be attributed in large part to falling costs of bringing DER sites online. Any cybersecurity program should account for the resources needed to implement, maintain, and update its requirements over time. Not accounting for these resource needs could affect the value equation in a way that stunts the growth of the distributed grid. However, it is imperative that cost is viewed as only one consideration point in a risk analysis.
6. **Principle #6: Ensure that compliance requirements are transparent and universal**. To ensure equal opportunity to participate in the distributed grid, compliance requirements should be publicly available as appropriate and clearly understood.
7. **Principle #7: Enable quick adaptation to counter new threats and to take advantage of technological innovations.** Cybersecurity is a fast-moving discipline. Adversaries are constantly creating new tools and utilizing new methods to circumvent protections. Innovators are constantly introducing new solutions that could replace older ones. Any cybersecurity program needs the ability to quickly change or add requirements to address new threats and allow innovative solutions.
8. **Principle #8: Ensure open and transparent governance**. Any cybersecurity plan should have clear governance that allows all stakeholders to both participate in the plan formulation process and in the decisions on which cybersecurity requirements are included.
9. **Principle #9: Get "to market" quickly** to meet the increasingly critical DER security requirements to better ensure that DER systems going into the field are at a higher "trust" level.
10. **Principle #10: Flexibility for rapid response:** Cyber incidents require rapid response, and organizations (DSOs, vendors, asset owners and operators, etc.) should have the flexibility, in certain cases, for adding and/or modifying requirements in response to this changing threat landscape. These requirements will be reviewed with a more formal process after the initial

modification. Organizations must have the right, flexibility, and authority to make reasonable changes in response to the changing DER and threat landscape.

5.3 Possible CPUC Paths

There are multiple paths for implementing cybersecurity requirements for DERs in California. These paths have differing potential to adhere to the ten principles presented in section 5.2 above. Possible regulatory paths include:

A. **Path A. The CPUC waits for California legislation to develop cybersecurity requirements for DERs**: The California legislature could pass a law that stipulates what stakeholders must do to be compliant when participating in the distributed grid. This path meets Principle #6 (*transparent compliance requirements*) and might meet Principle #1 (*baseline assessment*) depending on the enforcement mechanisms but has multiple challenges. First, the legislative process is slow, and the more detailed the law the slower the process. In addition, no such effort is foreseen currently. This path would clearly inhibit achievement of Principles #7 (*quick adaptation*), #8 (*open governance*), or #9 (*get to market quickly*). Second, legislation is often not detailed enough to give stakeholders the necessary clarity, so Principles #4 (*allocation of compliance*) and #5 (*use risk assessment*) are not likely to be achieved.

B. **Path B. The CPUC waits for the Department of Energy and NARUC to develop cybersecurity requirements for DERs**: DOE and NARUC undertook an effort to develop ***cybersecurity baselines*** *for DSOs and DERs* (completed in February 2024) and are working on an implementation guide for those baselines. They do not plan to develop cybersecurity requirements but will leave that effort up to the PUCs. These requirements address the cybersecurity needs of the 3000+ US DSOs, including rural electric cooperatives and small DSOs with no or few large (> 1 MW) DERs. These baselines meet Principle #1 (*baseline assessment*) and Principle #6 (*transparent compliance requirements*), but do not meet most of the other Principles, similar to Path A. In particular, these cybersecurity baselines do not meet the cybersecurity requirements of California's high DER future without additional development per Principle #9 (*get "to market" quickly*).

C. **Path C. The CPUC waits for the IEEE 1547 revision to develop cybersecurity requirements for DERs:** IEEE 1547 is being revised and is expected to include some cybersecurity requirements. It is using the SIO-CS review of IEEE 1547.3, Section 5[31] as its basis. However, the revision is expected to take about 3 years to complete and would largely duplicate the work already performed in the SIO-CS Subgroup. Since IEEE 1547.3 is being used as the basis, this effort will meet Principle #1 (*baseline assessment),* Principle #2 (*appropriate level*), Principle #3 (*resilience*), and Principle #6 (*transparent compliance requirements*).

D. **Path D. The CPUC provides guidance only and leaves the DER cybersecurity requirements up to DSOs**: This path is similar to what is currently occurring. The DSOs could continue to develop their own cybersecurity requirements and would need to verify each DER's implementation before granting interconnection. This path does not achieve Principle #6 (*transparent compliance requirements*) nor Principle #5 (*use risk assessment*) if the DSO requirements are too onerous.

E. **Path E. The CPUC defines specific CPUC DER cybersecurity requirements, including testing cases**: The CPUC could specify the set of DER cybersecurity requirements for all stakeholders. This is the

[31] *See Annex B.2*

path the CPUC took for Rule 21, in which Rule 21 was updated (over time) to include all Phase 1, 2, and 3 smart inverter functions. This path would require the CPUC to specify the cybersecurity requirements, but also the testing and certification procedures. The CPUC would also need to take on the responsibility to quickly change these requirements if new cybersecurity threats were identified. This would make it difficult to meet the agility Principle #7 (*quick adaptation*).

F. **Path F. The CPUC *recommends* (but does not mandate) that the DSOs use the SIO-CS Phase 1 Primary DER Cybersecurity Requirements** in the short term as part of their cybersecurity requirements for DER facilities. The DSOs would add this cybersecurity document plus any cybersecurity testing and certification requirements to the contractual agreements for some or all DER interconnections, as justified by size (e.g., > 1MW) or by communication requirements. Any modifications of these Phase 1 cybersecurity requirements by a DSO would require well-documented justification based on DER size, location, situation, newly identified threat, or other circumstances. This approach meets most of the principles, except Principle #6 (*transparent compliance*) and Principle #8 (transparent governance).

G. **Path G. The CPUC initiates the development of Phase 2 DER Cybersecurity Requirements** for the California DSOs. If combined with Path F, this approach meets all principles. The process could be split into 2 efforts:

    a. **Path G1: The CPUC initiates a Phase 2 cybersecurity working group**, building on the scope of the SIO-CS. This Phase 2 group would again be comprised of the California DSOs and DER stakeholders to review and update the SIO-CS Phase 1 Primary DER Cybersecurity Requirements based on input from the DOE/NARUC "*Cybersecurity Baselines for Electric Distribution and DER*", the UL 2941 Outline of Investigation, the "SunSpec Cybersecurity Certification" document, the new CPUC-SCE VGI effort,[32] SAE J3400, and other cybersecurity requirements sources. The updated Phase 2 DER Cybersecurity Requirements would include qualifications on where they are (or are not) applicable and flexibility on where they would be deployed since cybersecurity threats are expected to change over time.

    b. **Path G2: The CPUC initiates and/or supports the establishment of a Cybersecurity Coordination Forum** comprised of cybersecurity experts from different organizations. Although a longer process, this effort could provide additional input into the Phase 2 DER Cybersecurity Requirements.

H. **Path H. The CPUC endorses the establishment of testing and certification programs** that would meet the SIO-CS Phase 1 (and eventually Phase 2) DER cybersecurity testing and certification needs, such as those being developed by UL and SunSpec. This is like the testing and certification requirements for Rule 21 functions which were developed as UL 1741 Supplement A and more recently Supplement B. Compliance timing for meeting the Phase 1 cybersecurity measures would reflect the time to develop such testing and certification programs plus the time to allow DER implementors to test their products. This approach would provide the necessary cybersecurity certification of DER vendors. This path is necessary for any the implementation of any of the other Paths.

[32] *Southern California Edison Company's (U 338-E) Vehicle-grid Integration Strategies Annual Report for 2022, March 15, 2023 in Rulemaking R.18-12-006 to Continue the Development of Rates and Infrastructure for Vehicle Electrification*

5.4 Paths Rejected by the SIO-CS Subgroup

The following paths were deemed not appropriate for the CPUC cybersecurity effort and were therefore rejected by the SIO-CS Subgroup:

- **Paths A, B, or C (wait for governmental groups):** If the CPUC were to follow the regulatory Paths A, B, or C, the wait for governmental groups to develop appropriate DER cybersecurity requirements (*not just baselines*) could be lengthy or might not occur at all, and the results might not meet the cybersecurity requirements for California's High DER future. The DSOs are already requiring some cybersecurity requirements and DER vendors do not want to wait longer for regulatory direction.
- **Path D (Leave cybersecurity requirements up to each DSO):** If the CPUC were to follow Path D, the status quo would be maintained, allowing each DSO to determine their own, uncoordinated set of cybersecurity requirements. The lack of coordination would result in higher costs for DER vendors.
- **Path E (CPUC undertakes the development of cybersecurity requirements):** If the CPUC were to follow Path E, they would be taking on a new burden. The path would likely be expensive and would put the CPUC into the standards business, and potentially the testing and certification business. With this path the CPUC would also need a mechanism to modify and add more requirements in the future, which is why this report is titled "*Phase 1 Primary Cybersecurity Requirements*". In the fast-moving cybersecurity environment, the CPUC would need to add and change requirements in future phases.

5.5 Recommended CPUC Paths

5.5.1 Recommended Paths F, G, and H

Ultimately the SIO-CS subgroup recommends that the CPUC pursue paths F, G, and H in parallel, namely:

- **Path F:** The CPUC ***recommends*** (but does not mandate) that the DSOs use the SIO-CS Phase 1 Primary DER Cybersecurity Requirements in the short term as part of their cybersecurity requirements for DER facilities.
- **Path G:** The CPUC initiates the **development of Phase 2 DER Cybersecurity Requirements** for the California DSOs. This could be split into 2 efforts:
  - **Path G1:** The CPUC initiates a Phase 2 cybersecurity working group, similar to the SIO-CS, comprised of the California DSOs and DER stakeholders to review and update the SIO-CS Phase 1 Primary DER Cybersecurity Requirements based on input from the DOE/NARUC "*Cybersecurity Baselines for Electric Distribution and DER*", the UL 2941 Outline of Investigation, the "SunSpec Cybersecurity Certification" document, the new CPUC-SCE VGI effort, SAE J3400, and other cybersecurity requirements sources. The updated Phase 2 Primary DER Cybersecurity Requirements would include qualifications on where they are (or are not) applicable and flexibility on where they would be deployed since cybersecurity threats are expected to change over time.

- **Path G2:** The CPUC initiates and/or supports the establishment of a Cybersecurity Coordination Forum comprised of cybersecurity experts from the different organizations.

- **Path H**: The CPUC endorses the establishment of testing and certification programs that would meet the SIO-CS Phase 1 (or Phase 2) DER cybersecurity testing and certification needs, such as those being developed by UL and SunSpec.

These paths are described in more detail in the following sections.

5.5.2 Path F: The CPUC recommend (but does not mandate) that the DSOs use the SIO-CS Phase 1 Primary DER Cybersecurity Requirements

{Immediately as Interim} If the CPUC follows Path F, the DSOs can continue to **define** their cybersecurity requirements, but the CPUC would recommend that they include the "*Phase 1 Primary DER Cybersecurity Requirements*" in their own set of cybersecurity requirements. This approach would provide more certainty for DER vendors and other stakeholders. This path is the quickest to implementing additional requirements since DSOs already identify specific cybersecurity requirements in add-ons to their contractual agreements, but not coordinated requirements. The DSOs would need on-going coordination via additional phases for cybersecurity requirements.

DSOs currently impose cybersecurity requirements on suppliers and partners. These contracts can include interconnection agreements, but also include any other contractual relationship such as pilots, service agreements, etc. However, there is considerable variability between the DSOs on the exact requirements for the various types of contracts. The DSOs could incorporate the Phase 1 Requirements in their approval processes for such contracts. DSOs would be free to add additional requirements on top of Phase 1 requirements.

This is similar to the CPUC developing the DER smart inverter functional requirements in Rule 21 but recognizes that the testing of DERs to ensure they were meeting the Rule 21 requirements necessitated testing expertise with third-party certification through UL 1741.

However, the SIO-CS Phase 1 DER Cybersecurity Requirements have not been adequately "reworded" or refined to act as definitive, basic cybersecurity requirements. Therefore, additional effort will be needed to clarify these Phase 1 requirements, so Path G is also needed.

5.5.3 Path G: The CPUC initiate Phase 2 DER Cybersecurity Requirements Based on SIO-CS Phase 1

{Requiring a few months to a year} In parallel with Path F, if the CPUC follows Path G, then for Path G1, the CPUC would initiate a **Phase 2 cybersecurity working group**, similar to the SIO-CS, comprised of the California DSOs and DER stakeholders to review and update the SIO-CS Phase 1 Primary DER Cybersecurity Requirements to become Phase 2 DER Cybersecurity Requirements. The updates to Phase 2 would be based on input from the DOE/NARUC "*Cybersecurity Baselines for Electric Distribution and DER*", the UL 2941 Outline of Investigation, the "SunSpec Cybersecurity Certification" document, the new CPUC-SCE VGI effort, SAE J3400, and other cybersecurity requirements sources. The updated Primary DER Cybersecurity Requirements would include qualifications on where they are (or are not) applicable and flexibility on where they would be deployed since cybersecurity threats are expected to change over time.

If the CPUC follows Path G2, then the CPUC would sponsor a **Cybersecurity Collaboration Forum.** The results of the SIO-CS *Phase 1 Primary DER Cybersecurity Requirements* would become an important contribution to the overall effort of developing DER cybersecurity requirements, possibly in. Although asking multiple organizations to collaborate on such an effort could require additional time to resolve differences, ultimately this approach could lead to a single set of effective and widely implemented DER cybersecurity requirements. This approach could reduce the burden on DER manufacturers and implementers by eliminating the possibility of multiple, conflicting cybersecurity requirements. Such a Cybersecurity Collaboration Forum could be managed by an independent party such as a standards organization or a nationally recognized corporation.

This set of cybersecurity requirements might need to be augmented for specific situations. Additional cybersecurity requirements could be added to address the cybersecurity needs in particular situations or for areas not covered by the Phase 1 Primary DER Cybersecurity Requirements (e.g., risk assessment, vendor personnel security, reporting specifics, etc.).

5.5.4 Path H: The CPUC Endorse Testing and Certification Programs

{As part of developing final requirements} In parallel with Path G, if the CPUC follows Path H, testing and certification programs can be established for Phase 1 and eventually Phase 2 DER Cybersecurity Requirements. This approach is similar to the UL 1741 SA testing requirements for the smart inverter functions of Rule 21. Once such testing and certification programs are set up, and time is allocated for testing and certification organizations to test DERs, DER implementations can quickly get to market. Agility to meet new cybersecurity threats can also be best handled by testing programs.

This path necessitates collaboration between third-party testing and certification programs and the CPUC. A prime example of previous collaboration between these organizations is represented by the CPUC's requirement that DER manufactures and aggregators follow UL 1741 Supplement A for DER testing and certification to meet Rule 21 Phase 1 requirements. UL has continued to develop the testing and certification requirements in the UL 1741 Supplement B as Rule 21 added the Phase 2 and Phase 3 requirements, and now the IEEE Std 1547-2018 requirements.

Based on this example, the SIO-CS Subgroup believes that the CPUC should take the lead in urging the development of third-party certification programs, such as by UL, and then hand over responsibility to the third parties when their testing and certification programs meet the needs of the CPUC and are operational.

5.6 Next Steps on Cybersecurity

As next steps on cybersecurity issues, the CPUC could either (1) continue this SIO-CS Subgroup with an expanded scope, (2) create another group that involves at least the same stakeholders or (3) initiate/support a Cybersecurity Coordination Forum involving these stakeholders and other cybersecurity experts. This new working group could then address additional cybersecurity-related questions for DSOs and the DER industry, such as:

- What cybersecurity functions do utilities already have and what challenges might they have in conforming to the requirements ("Shall") in Annex A?
- What "rewording" is needed to achieve full agreement on the SIO-CS Phase 1 DER Cybersecurity Requirements and what group will be charged with undertaking this effort? (Tied into Path G)

- How ought the IEEE 1547.3 “should” recommendations (as opposed to the “shall” requirements) be handled? Ought some of these “should” recommendations become “shall” requirements if reworded and/or qualified as only needed for specific situations?
- What are the timeframes for requiring DERs to meet which cybersecurity requirements (as either included in the Phase 1 document or as developed by the external group)?
- What requirements would need testing and certification as opposed to attestation?
- What are the other cybersecurity requirements DSOs would like to see in a testing and certification program?
- How can we make modifications to the Phase 1 requirements based on program experience and new developments?
- How do we make certification programs more useful to enterprise cybersecurity teams? Currently certifications are viewed as compliance, but hardly sufficient to protect against threats. Certification programs need to be seen as more value add to cybersecurity response teams.
- How should certification programs adapt to address supply chain and bill of materials threats? These concerns are a high priority for the Federal Government and the largest breaches today involve the supply chain.
- How should the industry develop cybersecurity infrastructure that enables sharing of real time data and improving incident response? Currently each organization is siloed and there is little inter-organization cooperation. This is problematic in an interconnected ecosystem like the distributed grid.
- What is the role of system and site testing in DER cybersecurity requirements (see Phase 1 Requirements Document).

6 Non-Consensus Statements and Qualifications on “Phase 1 Primary DER Cybersecurity Requirements” Document

6.1 General Qualifications

By agreement of the SIO-CS Subgroup, the contents of Annex A: *Phase 1 Primary DER Cybersecurity Requirements* reflect the agreement by ALL parties on the inclusion of the specific cybersecurity requirements extracted from the IEEE 1547.3 recommendations. However, there were also qualifications where the parties agreed in general with the inclusion of a requirement but felt that additional rewording or qualifications by DER type and/or size must be included. In general, these caveats or qualifications were added to the items in the document, but additional qualifications are expected to be needed, particularly if a joint Cybersecurity Collaboration Forum is created to harmonize the varying cybersecurity requirements from different efforts.

Although SCE agreed with the contents of Annex A, SCE does not agree with Path F in which the CPUC would recommend the use of Annex A by DSOs on a short term basis until the results from Path G updates to the cybersecurity requirements were fully developed.

All non-consensus and qualification statements in this section are verbatim as provided by each organization.

6.2 SunSpec Non-Consensus and Qualifications

SunSpec wishes the following words to be included, "*SunSpec is convinced that the state of California should not attempt to define its own cybersecurity standard using the IEEE 1547.3 guide as input. SunSpec agreed to prefix certain requirements in this document with the word "SHALL" only to indicate that California should seek third-party cybersecurity standards that include well-defined, testable requirements that are similar to the ones presented.*"

6.3 SCE Non-Consensus and Qualifications [placeholder language subject to revision based on final report due date confirmation]

SCE wishes to add the following non-consensus statements and qualifications.

6.3.1 SCE Feedback to Proposed Regulatory Recommendations

SCE does not support the rejection of Paths B, C, and D. SCE also provides additional comments on proposed paths F, G and H.

For Path B, the NARUC effort is a nationwide effort that is currently underway and also based on existing NIST cybersecurity framework (consistent with IEEE efforts) and that a CA specific effort would benefit from alignment with Federal cybersecurity efforts and provide consistency within the marketplace. The proposed NARUC effort involves greater representation from nationwide parties and is consistent with White House cybersecurity guidance issued last year speaking to common baselines. Work completed under this effort would be an important input to aid with proposed controls developed within the NARUC process.

Path C – SCE believes Path C should not be rejected as IEEE 1547.3 is a national guideline and additional revision would allow for a more mature work product The existing IEEE "standard" discussed within this report was developed in a guidance format as discussed within this report. Additional time may also allow for coordination with ongoing Federal efforts and experience gained from Smart Inverter implementation highlights benefits from starting from a clearly defined starting point.

Path D - SCE is currently addressing cybersecurity risk via several efforts including performance of risk assessments and cybersecurity appendices as discussed within the working group.

Path F – As discussed above, a CA specific effort departs from development of national baselines that would be proposed for adoption and it would be more appropriate at this time to allow a national effort whether that be the updated 1547.3 standard that is drafted as requirements and/or NARUC in support of nationwide grid security. If the CPUC believes it is prudent to move forward with a CA specific effort, it should be limited to a trial process as discussed within SDG&E's comments to gain experience and allow for flexibility.

Path G – SCE believes it would be more efficient and productive to allow for the expected NARUC/IEEE revision process to move forward as compared to additional development of a CA specific standard as compared to providing important input to these other efforts based on the work performed within this working group.

Path H – While SCE doesn't oppose entities like UL and SunSpec performing certification and testing, SCE supports further discussion regarding how cybersecurity requirements should be implemented. The model of Smart Inverter requirements being implemented through Rule 21 interconnection agreements may not be appropriate for meeting cybersecurity requirements. Alternative approaches that provide for generators being directly responsible for cybersecurity requirements (vs. through an IOU interconnection agreement) should be considered.

Although SCE conceptually supports moving forward with development of initial cybersecurity baselines for DERs, as the 1547.3 standard recommendations were drafted as guiding recommendations, and additional efforts are underway and should be reviewed before such recommendations could be placed within a contractual arrangement.. It was outside the WG scope to develop refined language that would be necessary in support of specific tariff requirements, and/or agreements. As noted below, additional discussion is warranted to how such requirements would be applied to projects individually or in aggregate. It would be premature at this time to move forward with specific contract/tariff development until these key questions are answered but this effort should support development of initial cybersecurity certification programs. Finally, as previously highlighted, the IEEE 1547.3 effort was drafted as recommendations only and did not itself propose any actual mandatory recommendations. It is anticipated that an updated standard for 1547.3 will be issued to incorporate feedback based on the proposed guiding recommendations. **Going forward utilizing 1547.3 may also conflict with Federal efforts at the national level which runs against recommendations put forward in the national cybersecurity strategy put forward that speaks to national standards as the broader NARUC effort captures. In addition, a number of questions remain in future efforts of this work:**

The following areas merit additional detailed stakeholder discussion. SCE supports a Phase 2 of this effort to assist with the review:

- Project size individual application or aggregation size
- Clarification of use applications that proposed requirements would apply to
- Specific control wording that would support contract/tariff inclusion as compared to conceptual guiding recommendations (this could be assisted with standard certification process development)
- Contractual placement (Rule 21 processes or contact based on grid services provided to facilitate more comprehensive adoption)
- Potential implementation timelines and how existing systems could be incorporated into proposed conceptual requirements
- Enforcement mechanisms (certification, contractual attestation, physical verification)
- Application to Existing Systems

6.3.2 SCE High Level Feedback to 1547.3 Standards

Unfortunately, IEEE STD 1547.3-2023 is not a standard[33]—it is a set of guidelines. There is a considerable amount of work required to convert IEEE 1547.3 into testable requirements, and recent priorities at the federal level have highlighted the need for additional requirements.

In addition, the proposed requirements based on 1547.3 will need to be further reviewed, revisited, and tailored before those requirements should be rolled out in specific tariffs. For this Phase 1 effort, only basic cybersecurity controls are included, but even these will require modifications and exemptions based on the types and sizes of DER, the electrical and physical locations of the facilities, the legal and regulatory situations, and combinations of legacy and new types of DER management systems. As stated previously, SCE is supportive of the types of controls proposed but not specifically utilizing the 1547.3 proposed guidelines/proposed regulations. If the CPUC elects to move forward with this effort, SCE agrees with SDG&E comments regarding the need for flexibility and view this as a trial effort as one way to utilize this effort but with the backdrop of outstanding issues and coordination with Federal efforts so as to not create confusion to the marketplace and overall national security.

6.4 PG&E Non-Consensus and Qualifications

PG&E is in agreement with moving forward with **regulatory Path F** and implementation of baseline cybersecurity requirements identified in Annex A: *Phase 1 Primary DER cybersecurity requirements*. PG&E already has established agreements with DER vendors and is already implementing cybersecurity requirements. It is essential that state baseline cybersecurity requirements are established as DSOs continue to onboard and integrate DER vendors in support of statewide clean energy goals.

PG&E is aware that there are efforts at the federal level, as well as through other groups working to identify DER cybersecurity standards and requirements, but waiting for those efforts to conclude or legislation to be passed in a timely manner is not feasible and is unrealistic. Regarding these efforts, it will be important to ensure harmonization at the state and federal level, at least through shared guiding principles, so as to avoid jurisdictional, operational, and compliance challenges. Wildly different approaches by different states or jurisdictions would not be ideal. That said, the CPUC has an opportunity to lead in this space, having identified DER baseline requirements that could use by others.

As DSOs continue to integrate in real-time, PG&E supports moving forward with the identified baseline cybersecurity requirements by the SIO-CS working group and acknowledges the need for flexibility to tweak in the future rather than waiting for other efforts to conclude.

PG&E's expectation is that we reserve the flexibility and right—based on changing risks and our unique system, and architecture—to require DERs to meet other additional requirements. Additional requirements would be applied in a transparent and fair manner to DER vendors.

Additionally, PG&E has the expectation that in response to changes in use cases, telemetry and controls of DER assets would require additional capabilities from a cybersecurity perspective beyond the baseline requirements identified by the working group.

PG&E supports a risk-based approach to cybersecurity requirements, informed and in response to the changing DER landscape and threats which are constantly evolving. As such, PG&E expects to require

[33] *As a clarification, IEEE Std 1547.3-2023 is defined as a standard by the IEEE but does not contain any mandatory requirements.*

additional requirements in addition to just baseline security needs. For example, “should” items that are part of Annex B Section 5 could be additional requirements that are asked of DER vendors.

Regarding the proposed **regulatory Path G:** waiting for multiple groups to convene, such as what is being proposed, runs the risk of trying to create a one size fits all path. An additional working group made up of a larger group of stakeholders may be ideal in concept but, in implementation, it could take years for multiple groups to come up with anything beyond a baseline which the current working group has already done. This idea assumes that a larger group would come up with a more perfect solution in a short time frame. Furthermore, CPUC and DSOs may not be the appropriate entities to convene nationwide stakeholders. That said, such a Cybersecurity Collaboration Forum as is being proposed could be something that can align and/or springboard from the current DOE and NARUC effort. A Federal effort or entity/entities leading this may be more appropriate and have the resources to convene multiple stakeholders.

6.5 SDG&E Non-Consensus and Qualifications

SDG&E acknowledges the critical necessity of robust cybersecurity measures for DER installations, recognizing that consistent, secure practices are paramount for the safe, efficient, and sustainable integration of DERs. In alignment with this recognition, SDG&E supports a trial adoption of the comprehensive set of requirements outlined in Annex A of this report as a next step forward.

SDG&E is aware of the dynamic nature of DER technologies, the diverse use cases they encompass, and the continuously evolving industry standards. This awareness is grounded in the insights and discussions presented in this report’s Phase 1 analysis. Given the rapid technological advancements and the diverse applications of DERs, SDG&E believes a trial adoption process should be monitored and evaluated. This evaluation would focus not only on achieving a fundamental baseline of cybersecurity but also on identifying potential challenges, gaps, and areas for enhancement. Furthermore, if a Phase 2 effort was pursued, it could aim to systematically evaluate the experiences from a trial adoption of the requirements. Recognizing that the DER landscape is characterized by its complexity and variability, SDG&E advocates for the retention of full autonomy by DSOs to implement additional, case-specific cybersecurity contractual requirements. This flexibility ensures that unique risks and scenarios can be addressed effectively, maintaining the highest level of security and reliability.

Annex A Phase 1 Primary DER Cybersecurity Requirements

A.1 Introduction

A.1.1 Qualifications and Caveats

The development of universal cybersecurity requirements for DERs is very challenging and will need to be further reviewed, revisited, and tailored before those requirements should be rolled out in specific tariffs. For this Phase 1 effort, only basic cybersecurity requirements are included, but even these will require modifications and exemptions based on the types and sizes of DER, the electrical and physical locations of the facilities, the legal and regulatory situations, and combinations of legacy and new types of DER management systems.

Once the CPUC process is finalized (see the SIO-CS Working Group Report and Staff Proposal [pending]), it is expected that each DSO will use the Phase 1 Primary DER Cybersecurity Requirements as core to their overall DER cybersecurity requirements. When DER systems are submitted to the DSO for interconnection, the DSO will state which devices, systems, networks, protocols, and sites will be required to meet their cybersecurity requirements, specifically including qualifications on which equipment must meet which requirements, based on clear and consistent criteria agreed upon by all stakeholders.

Specifically, there is always a risk for any size or type of equipment, but cybersecurity must balance the cost of solutions against the likelihood of a security event taking place and the impact of such an event. A simple but useful way of looking at risk is Cost of Risk = Likelihood of Event “times” the Impact of Event. Then the Cost of Risk must be balanced against the Cost of the Solution:

- **Size/importance** of DER: Small, Medium, Large, Plant, Critical, Large Aggregation of DER
- **DER Unit**: Distributed Energy Resource (DER) unit, such as a photovoltaic system, a battery storage system, a wind turbine, or any inverter-based resource.
- **DER system**: as defined in IEEE 1547-2018, including a group of DER units
- **PCS**: Power Control Systems or energy management systems (also known as a facility EMS, a microgrid EMS, or a Plant Management System)
- **DSO Gateways**: Gateways to DSO DER Energy Management System (DERMS)
- **Aggregator Gateways**: Gateways to Aggregator DER Energy Management System
- **Network devices**: such as gateways, routers, and firewalls

Although the CPUC stakeholder process will identify the DER cybersecurity testing and certification requirements, the cybersecurity testing may be performed by authorized independent testing organizations and confirmed by approved certification bodies. These are still under development so it is expected that revisions to both the cybersecurity requirements wording and to the testing protocols will occur over time.

A.1.2 Document Contents

The following sections comprise the Phase 1 Primary DER Cybersecurity Requirements. These are organized using the same numbering scheme as IEEE 1547.3 but with an “a” added to the numbering to indicate the item has been modified. Specifically, the word “shall” has been inserted, and, in some cases, additional qualifications, comments, and questions have been added.

Annex A includes the table used by the SIO-CS Subgroup to review, comment, and select the IEEE 1547.3 Section 5 items.

A.2 RA: Risk Assessment and Management

No cybersecurity requirements were identified in the Risk Assessment and Management section, so the IEEE 1547.3 RA items remain as "Should” recommendations.

A.3 NE: Network Cybersecurity Requirements

The following network items from IEEE 1547.3 have been agreed to be “**Shall**” mandatory cybersecurity requirements:

A.3.1 Network Segmentation and Defining Security Boundaries

The cybersecurity requirements are:

- NE-4a. Logical network segmentations **Shall** be based on trust levels, access, and function. Network segments with low trust levels such as the Public Internet **Shall** use IEEE 1547-2018 specified communication protocols that support TLS 1.2 or TLS 1.3 since access to the network is unrestricted.
  - Higher trust segments **should** include access control to the network and may implement additional defensive measures such as IDS/IPS where end devices may operate over insecure protocols. ICS equipment **should** be treated as less secure and therefore **should** reside within a network segment with higher level of trust.

A.3.2 Managing Security Boundary

The cybersecurity requirements are:

- NE-20a. The types of communication protocols and ports **Shall** be limited to the minimum set required for functional operations.
- NE-21a. Multi-homed devices (**please confirm how Multi-homed devices will be defined)** without security **Shall** not connect to a DSO network.

A.3.3 Network Traffic Monitoring

The cybersecurity requirements are:

- NE-28a. DER **Shall** log security events.

A.3.4 Network Security Equipment

The cybersecurity requirements are:

- NE-36a. Unused ports and services **Shall** be disabled, and enabling **Shall** be logged.
- NE-37a. Equipment **Shall** require unique username and password, programmed on commissioning.
- NE-38a. Access control **Shall** be implemented on all equipment.

A.3.5 Physical Access to Networks

The cybersecurity requirements are:

- NE-42a. Unused external communications ports on critical hardware **Shall** be disabled in software when possible.
- NE-43a. Unused communication connections including wireless on installed equipment **Shall** be removed as feasible.
- NE-44a. Modifications to settings through physical equipment panels [**switchbox?**] **Shall** be monitored and logged.

A.4 AC: Access Control Cybersecurity Requirements

A.4.1 User Access Requirements

The cybersecurity requirements are:

- AC-3a. User (human) accountability and non-repudiation – User actions **Shall** be logged so events can be traced, time-synchronized with other events, and/or audited.
- AC-5a. User-created passwords **Shall** follow a set of rules that are adhered to in the creation of each password. Passwords **Shall** be at least eight characters in length and **Shall** be case sensitive. They **Shall** not use common dictionary words and/or consecutive and repeatable characters. When encoding passwords in plain text, the password characters **Shall** contain the following as a minimum: **this proposal as drafted is consistent with existing NIST best practices for passwords, we should look to phrasing that speaks to best practices)**
  - At least one uppercase and one lower case letter
  - At least one number
  - At least one non-alphanumeric character (e.g., @, %, &, *)
- AC-6a. Any attempt to create a password that violates these rules **Shall** be captured at the time of attempted creation, and the user **Shall** be notified and prompted to choose another password that conforms to the rules. Individual DER (< 1 MW?) and individual EVs may be exempted.
- AC-7a. Access failures **Shall** support adjustable account lockout thresholds and durations. Individual DER (< 1 MW?) and individual EVs may be exempted.

- AC-8a. Passwords and other security tokens **Shall** never be displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.

A.4.2 System Access Requirements

The cybersecurity requirements are:

- AC-11a. System authentication – Systems, software applications, and devices **Shall** be authenticated for access to other systems, software applications, and devices through cybersecurity authentication mechanisms, such as certificates, tokens, white lists, etc.
- AC-12a. System authorization – Systems, software applications, and devices **Shall** be assigned permissions to access data, services, resources, or objects granted by the security policy. These permissions **Shall** also be constrained to one or more of the following: reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.
- AC-13a. System authentication **Shall** be performed as closely as possible to the end system, software application, and/or device.
- AC-14a. System accountability and non-repudiation – Systems, software applications, and device actions **Shall** be logged so events can be traced, time-synchronized with other events, and/or audited.

A.4.3 Access Management Recommendations

The cybersecurity requirements are:

- AC-15a. Default shared passwords **Shall** be required to be changed upon installation or any change of ownership or location of equipment or systems.
- AC-17a. Secure interfaces **Shall** provide an open and documented method for adding and updating user accounts, passwords, and assignment to roles.
- AC-18a. All access changes **Shall** be logged.

A.4.4 Role-Based Access Control (RBAC) Requirements

The cybersecurity requirements are:

- AC-19a. Role-Based Access Control (RBAC) **Shall** be supported for all interactions between users, systems, software applications, and devices.
- AC-20a. Users **Shall** be assigned to one or more roles which have the permissions necessary for the users to perform their tasks. Individual DER (< 1 MW?) and individual EVs may be exempted.
- AC-21a. Systems, software applications, and devices **Shall** be assigned to one or more roles as needed for them to perform their functions. Individual DER (< 1 MW?) and individual EVs may be exempted.

- AC-23a. The DER and other objects **Shall** have the capability of defining multiple user-defined roles. Each role **Shall** have the capability of having any combination of rights including: Individual DER (< 1 MW?) and individual EVs may be exempted.
- AC-26a. All RBAC changes **Shall** be logged.

A.5 DS: Data Security Requirements

The following data security items from IEEE 1547.3 have been agreed to be "**Shall**" mandatory cybersecurity requirements:

A.5.1 Security for Data-at-Rest

The cybersecurity requirements are:

- DS-1a. RBAC methods **Shall** be used to authorize any viewing, read, write, create, or delete access to stored data, particularly where different organizations have different types and levels of authority to access the same stored data. Individual DER (< 1 MW?) and individual EVs may be exempted.
- DS-2a. Cryptography used to secure data **Shall** not use any deprecated methods.
- DS-3a. On removing, disposing, or repurposing devices, a sanitization process **Shall** be used to remove any confidential data at rest on the device, such as a factory reset option or securely recycled. Individual DER (< 1 MW?) and individual EVs may be exempted.
- DS-5a. All devices **Shall** have their security certificate credentials securely stored in a Secure Element (SE) such as Trusted Platform Module (TPM) chips or equivalent solutions to secure the software components of the device. Individual DER (< 1 MW?) and individual EVs may be exempted. A phased implementation timeline may be used.
- DS-6a. Verification **Shall** be done to help ensure sensitive information no longer exists on the device following factory reset. Individual DER (< 1 MW?) and individual EVs may be exempted.

A.5.2 Security for Data-in-Transit

The cybersecurity requirements are:

- DS-7a. Every communication session **Shall** require authentication of both the source (system, device, database, and/or software application) of the data and the recipient (system, device, database, and/or software application) of the data. Local EPS networks with communications using Modbus may be exempted.
- DS-8a. Communication sessions **Shall** have time limits and **Shall** require the renegotiation and reauthentication of new communication sessions. Individual DER (< 1 MW?) and individual EVs may be exempted.
- DS-11a. Data-in-transit **Shall** be time-stamped so that it may be stored and possibly logged with accurate time information. Individual DER (< 1 MW?) and individual EVs may be exempted. Communications using Modbus may be exempted.

- DS-14a. Key management **Shall** be used as required by mutually-agreed security policies.

A.6 SM: Security Management Requirements

A.6.1 Lifecycle Management

The cybersecurity requirements are:

- SM-1a. Asset inventories **Shall** include all physical devices.
- SM-2a. Asset inventories **Shall** include all installed firmware, software and applications with version information including external systems.
- SM-3a. Asset inventories **Shall** include all external services such as cloud services and third-party managed services.
- SM-6a. Time synchronization, of adequate precision and accuracy, **Shall** be implemented across all key DER components, networks, logs, and interfaces to external stakeholders, (e.g. as per IEEE 1588, RFC 5905 (NTP)). Protection **Shall** be implemented against attacks on clocks and the time synch protocol, to help ensure that the timestamps of audit logs capture a series of events truly chronologically with the necessary time resolution. Individual DER (< 1 MW?) and individual EVs may be exempted. Adequate precision and accuracy of time synchronization **Shall** be, at a minimum within + 1 minute of UTC and time resolution is at least 1 ms, with exceptions determined by mutually-agreed security policies.
- SM-7a. Operating system management **Shall** include: Operating systems installed on security devices **Shall** be within vendor support window; Operating systems on industrial equipment outside of vendor support windows **Shall** be assessed, isolated and/or recommended for replacement. Individual DER (< 1 MW?) and individual EVs may be exempted.
- SM-8a. Hardware, software and security upgrades **Shall** be noted in the asset inventories, along with any updated identities.
- SM-9a. Decommissioning or disposal of any asset **Shall** be noted in the asset inventories, including the current status of that asset.

A.6.2 Supply Chain Management

The cybersecurity requirements are:

- No supply chain requirements were identified

A.6.3 Patch Management

The cybersecurity requirements are:

- SM-16a. DER and associated systems **Shall** support the ability to be updated.
- SM-17a. DER and associated systems **Shall** support the ability for remote updates.
- SM-18a. DER and associated systems **Shall** support the ability for automated updates, if mutually-agreed by security policies.

- SM-20a. DER and associated systems **Shall** check periodically, within [7?] days, whether there is an available update. **(industry best practice?)**
- SM-21a. DER and associated systems **Shall** verify the authenticity and integrity of software updates.
- SM-22a. DER and associated systems **Shall** be commissioned with the most recent firmware version.
- SM-23a. DER product suppliers **Shall** document the firmware patching policy.
- SM-24a. DER product suppliers **Shall** provide a policy on product support including firmware updates.
- SM-25a. DER product suppliers **Shall** provide software updates that are non-repudiable. Software update non-repudiation **Shall** provide the product supplier with proof of patch delivery and the recipient **Shall** be provided with proof of the product supplier's identity.
- SM-26a. DER product suppliers **Shall** use an appropriate standard to approve the selection of cryptography modules. DER product supplier may use a FIPS 140-2 Level 2 or greater cryptography modules for all keys used in code signing processes, with equivalent certifications recognized as acceptable. NIST 800-52 Guidelines may also be used.
- SM-27a. DER product suppliers **Shall** inform integrators, aggregators, and owners in a recognizable and apparent manner (e.g., on a website) that a security update is available.
- SM-28a. DER product suppliers **Shall** provide information on applicability, compatibility, and risks mitigated by the patch.
- SM-29a. DER product suppliers **Shall** notify the aggregator, owner, or operator when the application of a software update will disrupt the basic functioning of the DER.
- SM-30a. DER product suppliers **Shall** provide, in an accessible way that is clear and transparent to the aggregator, owner, or operator, the defined DER device support period.
- SM-31a. DER product suppliers **Shall** publish a list of all patches and their approval status.
- SM-32a. When technically feasible, DER product suppliers **Shall** provide a patch or alternative risk mitigation for security vulnerabilities within 60 days of notification or internal discovery by the DER product supplier.
- SM-33a. DER product suppliers **Shall** use mechanisms that prevent firmware downgrade attacks, i.e., prevent updates to previous software versions.
- SM-43a. DER owners **Shall** document patch management process for tracking, evaluating, and installing DER security patches. The tracking portion **Shall** include the identification of source(s) of DER security patches.
- SM-48a. DER owners **Shall** maintain a record (log) of all previously installed firmware versions for each device.

A.6.4 Security Event Logging

The cybersecurity requirements are:

- SM-56a. Systems **Shall** be able to store security log events locally if they are unable to export them. At a minimum if unable to export / send the logs to cloud or external system, systems **Shall** store security event logs for 90 days, power system logs for 90 days, and network traffic for 14 days and if able to export / send logs to cloud or external system for up to 7 days.
- SM-57a. Systems **Shall** include timestamps in all logs including security logs with sufficient resolution to be useful, as determined by mutually-agreed security policies.
- SM-58a. System internal clocks **Shall** be kept in sync with appropriate time sources of adequate precision, such as the Network Time Protocol (NTP).
- SM-59a. Write access to security logs **Shall** be restricted to only adding information and **Shall** prevent modification and/or deletion of events.
- SM-60a. Power system logs **Shall** include: Power system logs for output anomalies; When a function is enabled or disabled; When a function is activated and has an impact on output power; May include data validation of incoming packets such as checksums. Firmware updates **Shall** be validated and verified prior to installation.
- SM-61a. Power system and security logs **Shall** be monitored on a recurring basis.
- SM-62a. Security logs **Shall** be securely, but easily, remotely retrievable and remotely accessible in real time.
- SM-64a. The ability to aggregate security logs in a centralized Security Information and Event Management (SIEM) systems **Shall** be supported. Individual DER (< 1 MW?) and individual EVs may be exempted.
- SM-65a. Power system and security log storage allocation **Shall** be sufficient to store event data for the minimum required timeframe.
- SM-66a. For power system and security logs with limited memory allocations, warnings on overwriting log entries **Shall** be provided.
- SM-67a. Power system and security logs **Shall** be periodically backed up to another system

A.6.5 Data Backups

No cybersecurity requirements were identified.

A.7 CM: Coping and Recovery Requirements

A.7.1 Pre-Event Coordination Planning and Cross-Organization Security Studies

No cybersecurity requirements were identified.

A.7.2 During-Event Security Event Notification, Coping, and Coordination with Stakeholders

The cybersecurity requirements are:

- CM-15a. Logging **Shall** capture and accurately timestamp all actions by all stakeholders. Multiple logs from different organizations **Shall** be able to be correlated with each other based on the timestamps.

A.7.3 Post-Event Cross-Organization Review of Impact of Security Situation

No cybersecurity requirements were identified.

Annex B IEEE 1547.3 Table of Section 5 Items

B.1 Purpose of Table of Section 5 Items

This table was used by the SIO-CS to assess the IEEE 1547.3 items to determine which ones could become Shall requirements with just slight wording updates, and possibly qualifications for which devices the requirements would be applicable. SIO-CS members entered "Should" or "Shall" (or left an entry blank to indicate Should) along with qualifications on which equipment the requirement ought to apply. In addition, some members added comments, some quite extensive, indicating why they made the judgment that they did. In most cases, only the "necessary recommendations" were addressed, since the "optional recommendations" were not perceived as potential "Shall" requirements.

The table reflects the discussions and the final results of the group (the sausage-making) but has deliberately not been "cleaned up" for editorial purposes, since the various qualifications and comments could be useful in subsequent phases of this cybersecurity effort. The SIO-CS used this table to work through all the security items and come to agreement on which should be included in Annex A. It was included because this is a WG report.

B.2 Table of IEEE 1547.3 Section 5 Cybersecurity Requirements and Recommendations

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
B.2.1 5.1 Risk Assessment and Management (RA) Recommendations **5.1.2 Risk Assessment Across Organizations (Inter-organizational)**						**Should** Phase One/**Shall** Future Phases /Implementation Discussion **Should** be discussed in greater detail within potential additional phases of this effort/implementation review and could be addressed in direct contractual negotiations between parties; as compared to an initial certification effort existing interconnection agreements due have emergency provisions and DSO will gain greater experience with ongoing pilots				SCE Draft Comments: Risk assessments must be aligned to an in-scope reference architecture, so that all parties are operating from a common baseline understanding to support the overall system. DSOs already have long standing governance over internal and external interactions with third parties. In this effort DSOs will need further discussions to determine potential risk impacts.
Necessary Recommendations										
RA-1. All organizations participate in cross-organizational agreements as they affect the cybersecurity of their operations.			**Should**	**Should**		Same as 5.2.Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	**Should** a template for cross-organizational agreements include a list of the cybersecurity items that **Should** be addressed? Security Certification requirement for devices (When available) that directly connect to DSO could be part of the above template agreement: DER Gateway Inverter OR Organizational certification like ISO 270001, SOC II etc., could be specified in the agreement template.	**Should** a template for cross-organizational agreements include a list of the cybersecurity items that **should** be addressed? Security Certification requirement for devices (When available) that directly connect to DSO could be part of the above template agreement: DER Gateway Inverter FDEMS Aggregator GW OR Organizational certification like ISO 270001, SOC II etc., could be specified in the agreement template. SCE Draft Comments a Cybersecurity incident within any of the participating organizations has the potential to affect another organization, it must be supported under common agreement like an incident response plan concept that could be discussed within future phases. If looking a future certification approach ,may want to see areas of common baselines that could support agreement development as this may looks to be beyond and initial certification proposal

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
RA-2. All organizations expect and understand that agreements and/or risk assessments may require revision to update or include more specific details as projects progress and throughout the system lifecycle.				NA					This is not an actionable recommendation. This can be part of service contract between organizations and such contract can specify what additional details are required. It **Should** be left to organizations to decide based on their specific cyber security policy. AJ: Agree.	This is not an actionable recommendation. This can be part of service contract between organizations and such contract can specify what additional details are required. It **should** be left to organizations to decide based on their specific cyber security policy. SCE Draft Comment: Agreed, it is not actionable but must be understood as part of the overall lifecycle given changes…and thought **should** be given as to if there is a need for update if a material change is triggered or negotiation of new terms.
RA-3. Updates to risk assessments and agreements are communicated to all relevant stakeholders.				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment -Practically, further discussion is warranted on how the update would be defined
RA-4. Agreements between organizations include assignment of responsibility for ameliorating cross-organizational risks.				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment Additional discussion is warranted perhaps brining into discussion what types of methods best support this effort o to understand area of responsibility levels of input and output.
RA-5. Agreements between organizations require each to perform an assessment of *threats* – what are the potential inadvertent threats (mistakes, failures, natural disasters) and deliberate threats (hackers, industrial espionage, nation-state hackers, disgruntled employees)?				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment Additional discussion is warranted as it may be difficult to expect a level of operational confidence without understanding the inadvertent and deliberate "threat scape"
RA-6. Agreements between organizations require each to perform an assessment of *vulnerabilities* – where are the vulnerabilities, including the systems themselves, applications, databases, and the communications between them, including legacy systems?				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	AJ: DSOs & partners **Should** agree to share IOC (Indicator of compromises) within an agreeable period of time from its occurrence	SCE Draft Comment: Vulnerability assessment **should** be considered for what has the potential for negative impact based on its criticality to the system as identified in the reference architecture
RA-7. Agreements between organizations require each to perform an assessment of *impact* – what types of impacts might there be for each type of attack, failure, or event, including safety, electrical reliability, financial, reputation, societal?				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment: Impact ratings could be a starting point to classify the level of security needed both to protect the component itself and any cross organizational impact it might have.
RA-8. Agreements between organizations require each to perform an assessment of *likelihood* (probability) of and attack, failure, or event – how attractive would a successful deliberate attack be, and to whom? What is the probability of wormable malware or ransomeware affecting operations? How probably is a failure or a natural disaster event occurring that would impact cybersecurity mechanisms?				**Should**		Same approach as 5.2 Overview	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment: Likelihood and Impact are inseparable, they must both be done for the appropriate criticality and potential development of risk rankings

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
Optional Recommendations										
RA-9. Agreements between organizations require each to combine these risk items into risk exposure: The risk exposure of a threat is the likelihood (probability) of an attack "times" or weighted by the impact if such an attack were to take place, offset perhaps by the ability to cope during an attack, and taking into account the time and cost for eventual recovery.						SCE has concentrated its review on the "Required" Standard Proposals as part of this WG				.
RA-10. Agreements between organizations include mutual access to risk assessment results of assets that could impact each organization (e.g. threats, vulnerabilities, likelihoods, and impacts) and a means of timely communication of new identified threats and vulnerabilities.										
RA-11. Risk prioritization is agreed upon by all relevant stakeholders.										.
5.1.3 Risk Management Across Organizations (Inter-organizational)										
Necessary Recommendations										
RA-12. Identified risks are mitigated, accepted, tolerated, or transferred to other stakeholders with agreement of risk management strategy between stakeholders.				Should		**Should/Shall** (Future Phases) SCE believes this is a critical concept, but additional discussion is warranted how this could be incorporated within a certification process and supporting agreements– future phases of this effort **should** further review this item	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		These Risk Management issues are not testable or certifiable but would be auditable. These comments could be added as additional comments on the 1547.3 recommendations in the WG Report
RA-13. Agreements between organizations include required time lines for notification of changes in identified risks.				Should		Refer to RA-12 Under 5.2.3 recommendation	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment: This must be done based on risk impact. Not all risks require the same level of response. Additional discussion is warranted how this is incorporated within a certification process
RA-14. Agreements between organizations clearly define the responsibilities of each organization for identifying and coping with each type of potential cybersecurity event. (Additional recommendations for indentifying and coping with security incidents is included in section 5.7)				Should		Refer to RA-12 Under 5.2.3. recommendation	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comment: Additional discussion is warranted to determine the impacted stakeholder feels the need for an internal response plan, and potentially a broader group of stakeholders

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
RA-15. Agreements between organizations identify what types of possible cybersecurity events would require notification to other parties and how such notifications will be provided.				Should		Refer to RA-12 Under 5.2.3 recommendation	All	All		
RA-16. Agreements between organizations identify what actions would be taken for different types of cybersecurity events (e.g. disconnect DER from the grid, shutdown communications, reset security parameters, etc.).			Should there be a template for what actions could be taken?	Should		Refer to RA-12 Under 5.2.3 recommendation	All	All		
Optional Recommendations										
RA-17. Agreements between organizations define the risk tolerance across organizations, in particular those affecting critical infrastructures.						SCE has concentrated its review on "required" recommendations but has provided comments to aid future discussions				SCE Draft Comment: Critical Infrastructure could be considered a broad term and may be best if the focus is tied to a reference architecture. This seems to be duplicative from the above assessment items.
RA-18. Agreements take into account the different cybersecurity maturity levels of different organizations.										SCE Draft Comment: This concept supports other proposals within this section as looks to establishment of the internal posture to help determine the community weakest link.
5.1.4 Intra-organizational Risk Issues										
Necessary Recommendations										
RA-19. Organizations use the existing risk management standards, such as ISO/IEC 27005, NIST Risk Management Framework, NIST SP 800-53, NISTIR 7628, etc., to manage their own risks, taking into account the need to cope with the risks associated with other DER stakeholder organizations.				Should		Should/Shall for future phases of this effort	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comments: Taking RA-18 into account, if a common reference architecture is established, the system/component critical is defined and supported through an approach that could include functional roles, and levels of input/output…From the established baseline and levels of criticality, the community coping levels can be established for all stakeholders to support and from those their internal review mechanisms can be established for their environment. SOC II audits should pick up on an entity's ability to cope with an event/incident.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
Optional Recommendations										
RA-20. Risk assessments include a review of services, applications and ports necessary for system functionality and an assessment of Defense in Depth strategies to secure those services. Standards such as IEC 62443 deal extensively with this topic.						As it is an optional recommendation, not providing a ranking but highlight that this is an important recommendation as we look to potential additional Phase 2 discussions				SCE Draft Comments: any potential pathway to engage any element of the reference architecture without authorization must be assessed for its impact on the operational requirements. IEC62443 and the CSF are great resources, and to be complimentary, two of the industries leaders produced a white paper identifying the following five critical controls: 5. Incident Response 2. Defensible Architecture 3. Network Visibility Monitoring 4. Secure Remote Access 5. Risk-Based Vulnerability Management
RA-21. Risk assessments may take into account relative likelihood of individual attack vector exploitation and focus Defense in Depth strategies on parts of the system that are considered the most likely targets based on current Tactics Techniques and Procedures used by attackers.										SCE Draft Comments: The MITRE ATT&CK ICS provides for tactics and techniques insight, the ICS Cyber Kill Chain provides phases pursued in an attack, and in conjunction with NIST's Common Vulnerability Scoring System, the risk and impact can be established. These are all available and supported tools.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
B.2.2 5.2 Communication Network Engineering (NE) Recommendations										
5.2.1 Network Segmentation and Defining Security Boundaries										
Necessary Recommendations										
NE-1. Network topologies are thoroughly documented and their purposes clearly described in order to determine what level of security they require.			**Should**	**Should**	AJ: **Should**	**Should**	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Interconnection Agreements or Service Agreements would include these requirements Certification can be made via SunSpec or other Attestation and/or testing, including inspection	Interconnection Agreements or Service Agreements would include these requirements, but further review may be warranted " Certification can be made via SunSpec or other Attestation and/or testing, including inspection SCE Draft Comment : Additional discussion maybe warranted on the interaction with DERMS system, and it is important to note that a certification relates to a specific protocol not network topology How do we also define terms such thoroughly documented?
NE-2. The bandwidth of network components are sized for the level of traffic expected and the required maximum traffic latency, including during emergency conditions, in order to help ensure adequate availability.			**N/A** **Not include as a cybersecurity requirement either Should or Shall**	**Not Applicable**					Performance requirement	Performance requirement
NE-3. Network data exchanges between network systems and devices are documented.			**Should**	AJ: **Should**	**Should (additional discussion maybe warranted as well)**	DER Gateways Inverters	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	How detailed **Should** the documentation be? Is the protocol one of the protocols in IEEE 1547? Or documentation on just what protocol is being used? E.g. Tesla is proprietary but at least documented AJ: Though protocol help inter-operability to a large extend, there are other connection specific details taken care – E.g. - Cipher	How detailed **should** the documentation be? Is the protocol one of the protocols in IEEE 1547? Or documentation on just what protocol is being used? E.g. Tesla is proprietary but at least documented! SCE Draft Comment: Similar Comments as NE-1

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-4. Logical network segmentations are based on trust levels, access, and function. Low trust levels such as the internet require higher level of security within the protocol since access to the network is unrestricted. Higher trust segments include access control to the network and may implement additional defensive measure such as IDS/IPS where end devices may operate over insecure protocols. ICS equipment is treated as less secure and therefore reside within a network segment with higher level of trust.	NE-4a. Logical network segmentations **Shall** be based on trust levels, access, and function. Network segments with low trust levels such as the Public Internet **Shall** use TLS 5.2 or TLS 5.3 within communication protocols since access to the network is unrestricted. Higher trust segments **Shall** include access control to the network and may implement additional defensive measure such as IDS/IPS where end devices may operate over insecure protocols. ICS equipment **Shall** be treated as less secure and therefore **Shall** reside within a network segment with higher level of trust.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation All other DERs **Shall** use Secure Protocols like DNP3 SAV5, IEEE 2030.5 or IEC 61850. If Modbus is used over public Internet, it **Shall** be over a TLS 5.2/5.3 secure tunnel or SSL VPN.	All data exchange over public internet **Shall** use TLS 5.2/5.3 based communication.	All data exchange over public internet **Shall** use TLS 5.2/5.3 based communication. SCE Draft Comment: We may want to consider if particular protocols are not specified, there could be an increased level of risk – but appreciate that generally R21 has agnostic approach
NE-5. Communication networks for internal communications (facility, DER controllers, SCADA systems, DERMS, etc.) are isolated from communication networks for external communications (the Internet, cellular systems, AMI, etc.).	NE-5a. Communication networks for internal communications (facility, DER controllers, SCADA systems, DERMS, etc.) **Shall** be isolated from communication networks for external communications (the Internet, cellular systems, AMI, etc.). Applicable to DER > 1 MW.	**No**	**Should** since this is a site requirement rather than a device requirement (type testing)	**Shall**	AJ: **Shall**	**Shall**	All	All except very small DERs and EVs	Considering internet sharing by small DER and EVs.	Considering internet sharing by small DER and EVs. SCE Draft Comment: How would aggregations be Considered?
NE-6. If including geographically isolated resources within the same VLAN connected through VPN or other secure remote connection, VLAN size is limited and areas of the network segmented to the extent practical to limit risk of network and security issues.				**NA**				Specific for certain implementations		
Optional Recommendations										
NE-7. Critical systems, applications, software, and equipment which pose a greater risk to safe operation of DER are isolated from less critical functions when possible.						For SCE, as these are presented an Optional Recommendation, SCE has concentrated on required recommendations but has provided comments for future reference.				SCE Draft Comment: System critical components and functions must be identified to apply appropriate controls.
NE-8. Equipment that controls critical operations reside within a high trust network segment.										SCE Draft Comment: Additionally, any lesser critical components would need to be secured commensurate to the critical components so as not to present risk.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-9. OT communications are separate from administrative communications used for supporting the network and hardware when possible.										SCE Draft Comment All communications in and out of the system must be identified to the respective functional requirements to include risk impact to determine network design and deployment.
NE-10. Network segments are reduced to core equipment to limit impact and probability of network compromise.										SCE Draft Comment: This is the focus of NE-8 and 9.
NE-11. Communications in and out of a control network are routed through a demilitarized zone (DMZ).										SCE Draft Comment: There is a previous reference to this in RA-18 variable levels of cybersecurity capability maturity. There are many advancements in boundary protection to where ingress/egress communications can be authenticated to a network, given authorization to a network destination after having been inspected for unauthorized manipulation which is a great detection mechanism, however it can be expensive and resource intensive. The optimum situation would mandate such capability to ensure a high level of confidence once deployed. The Risk Impact assessment will clarify the network boundary impacts to consider.
NE-12. A centralized DMZ may be considered for aggregated resources that are connected over a VLAN if a DMZ at each physical location is not feasible.										SCE Draft Comments: This may part of the community impact assessment that will also produce the local impact analysis results.
NE-13. Directories used for user authentication and/or authorization are unique to the control network and are not shared across the DMZ to enterprise and cross-organizational networks.										SCE Draft Comments: Directories must be impact assessed as per the stakeholder agreed upon reference architecture, sharing of an authentication/authorization "directory" over a network is a bad practice internally and or externally. This might be in part to a specific use case?
NE-14. Inbound and outbound traffic may be managed through separate gateway devices and other means of integrating downstream DER controls with upstream networks to allow for more restrictive rulesets and increased security. Specifically, traffic going one way is separated from traffic going the other way.										SCE Draft Comments: This is not clear, is it attempting to present a "data diode"? Any tcp/ip session is going to require bi-directional communication. Unless this is meant to separate single to many networks through individual gateways, which is the better requirement but again depending on the impact assessment. Additionally, if physical separation is not possible then logical is the next best thing to pursue.
NE-15. Databases with RBAC control may segregate which roles may write what data, and which roles may have view and read access to what data.										SCE Draft Comment: The NIST CSF can guide towards appropriate RBAC, however for this requirement, it seems to be better tied to establishing a database

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-16. Low latency critical functions do not rely on WAN communications.									Ride-through functions, droop, volt-var, etc. do not require WAN communications Unintentional islanding may be an example of where WAN communications may be needed.	SCE Draft Comment: it is possible to see the operational down side of having to run all comms through the WAN, but it depends on how the overall network is set up. There needs to be more insight to the level of unacceptable latency and evaluate it for impact against the available network paths within the reference architecture.
5.2.2 Managing Security Boundary										
Necessary Recommendations										
NE-17. Security boundaries are clearly defined and documented.				**Should**	AJ: **Should**	**Should** (Phase One)/**Shall** (Future Phases)	DER Gateway Inverters	All except very small DERs and EVs	Considering internet sharing by small DER and EVs. AJ: Firewall functionalities are foundational	Considering internet sharing by small DER and EVs. Reference Architecture. SCE Draft Comment: Unclear if this effort would be applied to inverters as well
NE-18. All communication paths through the security boundary are monitored for anomalous traffic patterns and malformed protocol packets.			**Should**	**Should**	AJ: **Should**	**Should** (Phase One/**Shall** (Future Phases)	DER Gateway Inverters	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comments: Complimentary to NE-11 in part to the impact analysis.
NE-19. Well configured and managed security devices are included on each data path through the boundary (manufacturer recommendations, and IEEE 1686 for device configuration guidance).				**Should**	AJ: **Should**	**Should**	DER Gateway Inverters	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comments: IEEE 1686 is currently in DRAFT, it is focused on IED's and not "security devices", additionally the standard goes into more detail requiring Control and monitoring of physical access to the secure perimeter housing the IED... Additional discussion may be required to provide further clarity to "security devices"?
NE-20. The types of communication protocols and ports are limited to the minimum set required for functional operations.	NE-20a. The types of communication protocols and ports **Shall** be limited to the minimum set required for functional operations.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	DER Gateway Inverters Networking Devices Maybe All	All	AJ: Minimal hardening is expected as best practice	SCE Draft Comments: Ports and Services **Shall** have well documented operational use requirements. Additional discussion is warranted on what a "minimum set for functional operations" is defined
NE-21. Multi-homed devices which have interfaces connected to multiple network segments include additional security measures equal to or greater than the security devices between those boundaries.	NE-21a. Multi-homed devices without security **Shall** not connect to a DSO network.	**Yes**	**Shall**	AJ: **Shall**	**Shall**	DER Gateway Inverters Networking Devices Maybe All	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Multihomed systems without security **Shall** not connect to DSO network.	SCE Draft Comments: Multihomed systems **Shall** not connect to DSO network. If a multi homed device is not identified and permitted to access any stakeholder network, a new potential threat path exists without impact assessment, this is a blind spot.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-22. Protection mechanisms are able to filter network traffic based on the protocol, source, and destination of each packet to determine if they are permitted based on predefined rules.				Should	AJ: Should	Should (this phase)/should be reviewed as part of future discussions	DER Gateway Networking Devices	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comments: If a stakeholder is not capable of implementing basic network boundary protections, they not only present a risk to their assets but any other stakeholder that is connected to them is also impacted, therefore it is important to cover the individual stakeholder as well as the community.
Optional Recommendations										
NE-23. Boundary devices such as web application firewalls are installed to include application and protocol aware rulesets for better filtering.						SCE Comments: SCE has focused review on "mandatory" requirements but has been provided to aid future discussions				SCE Draft Comments: It may be better to understand the impact reduction capability of web app as part of standard review fw before considering to be optional.
NE-24. Incoming control function communications from a low impact system are denied by default on boundary devices.										SCE Draft Comments: If this is permitted there could be significant impacts if an unauthorized control function is permitted to travers a network boundary, the impact analysis will help validate.
NE-25. Communications are unidirectional out of critical control networks with boundary devices configured to default deny incoming traffic.										SCE Draft Comments: Analysis of what stakeholder must poll, input, view etc. To help determine the respective boundary protection rule sets...DSOs currently do not have a need for direct connectivity to a DER behind an aggregator, therefore it **Shall** be denied. Is there a need for aggregator staff to engage in the DER network containing the smart inverter or any other DER network segment? Additional discussion is warranted as part of future standard updates
NE-26. Geoblocking techniques may be implemented to restrict international IP traffic.										
5.2.3 Network Traffic Monitoring										
Necessary Recommendations										
NE-27. Workstation or device security logs are enabled and stored.	NE-27a. Workstation or device security logs **Shall** be enabled and stored. Qualifications: 1. This applies to DER Gateways, Inverters, Workstations / Servers, Aggregators {but use more industry-specific language} 2. The size and duration of storage **Shall** be a minimum of 7 days ---- on the device or uploaded with exceptions handled through mutual agreement.	Yes	Shall	Shall	AJ: Shall	Shall	DER Gateways Inverters Workstations / Servers Aggregators	All	Need to define the duration / size of logs to be stored;	Need to define the duration / size of logs to be stored; Any event log to be captured and processed must be identified with a need and is further supported by the AOR's in a review in terms of who reviews, responds, consults etc.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-28. Security device logs are collected and stored.	NE-28a. DER **Shall** log security events.	**Yes, pending PG&E and SCE agreement**	**Shall**	**Shall.** If not implying a Network Security Device, then **Shall**	AJ: **Should** –	**Should**	Network Security Device	Medium DERs, Large DERs or Critical DERs or Aggregators managing more than 10 MW in Aggregated Generation or Aggregated Controllable Load (Rule 2, 15, 16 Proceeding)	Assumption, there is a separate security device AJ: Security logs generated by DER/related devices need to be harvested by a separate security device	SCE Draft Comment: Assumption, there is a separate security device. Duplicative, unless further expanded to include reference to the incident response plan?
NE-29. Logs collected from network security equipment are centrally collected and automatically analyzed against known threat signatures.			**Shall ((except for automatic analyzing against known threat signatures)**	**Should** If not implying a Network Security Device, then **Shall**	AJ: **Should**	**Should**	Network Security Device	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Concern about "centrally" collected.	SCE Draft Comment: Seems like 2 requirements here: 5. Centrally collected, would lend itself to a Security Event and Mgmt System (SEIM), and that would be linked to the incident response plan and activities. Automatically analyzed, event log analysis requires several elements to be established to determine the course of action to the desired point of return to service.
NE-30. Baseline network traffic, consisting of the source, destination, protocols and ports (TCP or UDP, mTLS, application protocol), timing, and typical data flow volumes, is captured and made available for incident response teams in the event of a compromise.			**Shall (Actually we took this out of SunSpec Phase 1)**	**Should** If not implying a Network Security Device, then **Shall**	AJ: **Should**	**Should** (Current Phase)/**Shall** Future Phases	Network Security Device	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	AJ: Assumes there are security technologies / devices part of the DER network	SCE Draft Comments: Baselined traffic with data flows are key elements for the reference architecture
Optional Recommendations										
NE-31. Intrusion Detection and/or Protection Systems (IDS/IPS) are used for monitoring traffic on higher trust networks.						SCE has focused on "Necessary" Recommendations for purposes of this review but have left comments to assist with future discussions				SCE Draft Comments: In most instances of IDS/IPS are implemented with the intent to progress from a passive monitoring to a reactionary capability that includes ensuring the response activities are aligned to the business internally or cross org impacts.
NE-32. If IPS are used, actions do not compromise the safe operation of the DER device.										
NE-33. Network and system management monitoring and alarming technologies (e.g. SNMP) are implemented to provide situational awareness (see IEC 62351-7 for further guidance).										
NE-34. Traffic is monitored at interfaces for unusual or unexpected patterns to provide situational awareness.										
NE-35. Critical network traffic is monitored 24/7 with personnel capable of taking corrective actions immediately after a detected compromise to limit the impact of an attack.										

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
5.2.4 Network Security Equipment										
Necessary Recommendations										
NE-36. Unused ports and services are disabled, and enabling is logged.	NE-36a. Unused ports and services **Shall** be disabled, and enabling **Shall** be logged.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		
NE-37. Equipment require unique username and password, programmed on commissioning.	NE-37a. Equipment **Shall** require unique username and password, programmed on commissioning.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		
NE-38. Access control is implemented on all equipment. See Section B.2.3 for detailed recommendations.	NE-38a. Access control **Shall** be implemented on all equipment.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		SCE Draft Comment: In future drafting process **should** better understand differences with NE 20/27 "All equipment" is very broad – confirmation or clarification will be required to keep the **Shall**
Optional Recommendations										***Boundary protection is a must, as per the clarified business impacts that require boundary protection.***
NE-39. The system include security and network devices which may be upgraded.						SCE has concentrated on "Necessary Recommendations" for this review				
NE-40. Firewall rules are configured by qualified personnel and are protected by RBAC methods against changes by unqualified personnel.										
NE-41. Boundary hardware have sufficient processor speeds such that significant latency delays are not introduced that would impact efficient operation of the DER.										
5.2.5 Physical Access to Networks										SCE Draft Comments: Physical ports can be logically disabled in support of physically blocking the port. Communication mediums must be evaluated for stakeholder impact. Logging is already covered, but nothing wrong with re-iterating the requirements for specific domains like boundary protection etc...
Necessary Recommendations										
NE-42. Unused external communications ports on critical hardware are disabled in software when possible.	NE-42a. Unused external communications ports on critical hardware **Shall** be disabled in software when possible.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
NE-43. Unused communication connections including wireless on installed equipment are removed.	NE-43a. Unused communication connections including wireless on installed equipment **Shall** be removed.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		
NE-44. Modifications to settings through physical equipment panels are monitored and logged.	NE-44a. Modifications to settings through physical equipment panels **Shall** be monitored and logged.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All	AJ: Physical security implementations	
Optional Recommendations										
NE-45. Unused external communications ports on critical hardware are physically blocked.	NE-45a. Unused external communications ports on critical hardware **Shall** be physically blocked.	**??**	**Should**	**Shall**		SCE has concentrated review on proposed "Necessary Recommendations" for purposes of this review	All	All		
NE-46. Where possible, equipment resides within a locked room or cabinet.										
NE-47. Only authorized personnel have access to network and control equipment.										
NE-48. Physical access to network equipment are monitored and logged.										
NE-49. Critical installation sites include 24/7 video monitoring.										
5.2.6 Cloud Computing										
B.2.3 5.3 Access Control (AC) Recommendations										
5.3.1 User Access Recommendations										
Necessary Recommendations										
AC-1. Authentication – All electronic access to systems and devices, whether locally through a control panel or diagnostic port, or remotely through communications media, are protected with an authentication mechanism that identifies a user with a unique user identification (ID) and password combination.	AC-1a. Authentication – All electronic access to systems and devices, whether locally through a control panel or diagnostic port, or remotely through communications media, **Shall** be protected with an authentication mechanism that identifies a user (human) with a unique user identification (ID) and password combination.	**Yes, pending PG&E agreement**	**Shall**	**Shall**	AJ: **Should**	**Shall**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
AC-2. User authorization – Users are assigned permissions to access data, services, resources, or objects granted by the security policy. These permissions are also constrained to one or more of the following: viewing (seeing), reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.	AC-2a. User authorization – Users (humans) **Shall** be assigned permissions to access data, services, resources, or objects granted by the security policy.	**No, the Shall would be RBAC for users**	**Should**	Shall	AJ: Should		EMS DERMS Aggregator Remote Management Applications to manage DER devices For "managed" devices	All	It cannot be expected for devices like an Inverter or a DER Gateway or a Controller to have multiple users, access, and security policies. They may be managed from a management service	It cannot be expected for devices like an Inverter or a DER Gateway or a Controller to have multiple users, access, and security policies. They may be managed from a management service SCE Draft Comment: for "managed services" – it appears to be confirmed on existing draft – subject to final confirmation
AC-3. User accountability and non-repudiation – User actions are logged so events can be traced, time-synchronized with other events, and/or audited.	AC-3a. User (human) accountability and non-repudiation – User actions **Shall** be logged so events can be traced, time-synchronized with other events, and/or audited.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All	AJ: and non-repudiation – User actions are logged – some explanation may help on this. See SM-6 on Time synchronization	
Optional Recommendations										
AC-4. User authentication – Users provide one or more proofs of identity to help ensure they are who they claim to be. Legitimate users are either required to know something (username/password, key code, etc.), have something (access card), be something (fingerprints, biometric scans, etc.), or—in the case of multifactor authentication—use a combination of these items to prove their identity. Recent implementations are also incorporating geolocation techniques to authenticate legitimate users based on where they are.	AC-4a. User (human) authentication – Users **Shall** provide one or more proofs of identity to help ensure they are who they claim to be. Legitimate users **Shall** be either required to know something (username/password, key code, etc.), have something (access card), be something (fingerprints, biometric scans, etc.), or—in the case of multifactor authentication—use a combination of these items to prove their identity. Recent implementations **may** also incorporate geolocation techniques to authenticate legitimate users based on where they are.	**No, because this is beyond the scope of DSOs to certify this item**	**Should**	Shall		SCE has focused review on "Necessary Recommendations" but have provided comments to aid future review	All	All	At least username/password	SCE Draft Comment: **Should** or **Shall**, needs to be determined by risk impact. Geolocation can provide protection against foreign adversaries, but not the silver bullet. Each stakeholder and as a community must clearly understand the potential for business impact from a remote attacker. There are legal challenges with foreign adversaries which makes it hard to apprehend them, however geolocation/blocking is a beneficial capability to be included in the business impact mitigations.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
AC-5. User-created passwords follow a set of rules that are adhered to in the creation of each password. Passwords are at least eight characters in length and are case sensitive. They do not use common dictionary words and/or consecutive and repeatable characters. When encoding passwords in plain text, the password characters contain the following as a minimum: • At least one uppercase and one lower case letter • At least one number • At least one non-alphanumeric character (e.g., @, %, &, *)	AC-5a. User-created passwords **Shall** follow a set of rules that are adhered to in the creation of each password. Passwords **Shall** be at least eight characters in length and **Shall** be case sensitive. They **Shall** not use common dictionary words and/or consecutive and repeatable characters. When encoding passwords in plain text, the password characters **Shall** contain the following as a minimum: • At least one uppercase and one lower case letter • At least one number • At least one non-alphanumeric character (e.g., @, %, &, *)	**Yes**	**Shall**	**Shall**			All	All		
AC-6. Any attempt to create a password that violates these rules is captured at the time of attempted creation, and the user is notified and prompted to choose another password that conforms to the rules.	AC-6a. Any attempt to create a password that violates these rules **Shall** be captured at the time of attempted creation, and the user **Shall** be notified and prompted to choose another password that conforms to the rules. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Shall**	**Shall**	AJ: **Shall**		All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	For "managed" devices	SCE Draft Comment: The risk impact to consider is from the ability to access the system/component with weak guessable passwords?
AC-7. Access failures support adjustable account lockout thresholds and durations.	AC-7a. Access failures **Shall** support adjustable account lockout thresholds and durations. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Shall**	**Shall**	AJ: **Shall**		All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	For "managed" devices	SCE Draft Response: Account lockouts are a stop gap, intended to support delaying the adversary from further repeated attempt at exploitation. It is also understood that in some operational capacities the account cannot withstand a lockout, in such instances the impacts are evaluated to adjust adherence to the requirement.
AC-8. Passwords and other security tokens are never displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.	AC-8a. Passwords and other security tokens **Shall** never be displayed through any means, including local display panel, configuration software (local or remote; offline or online), web browser, and terminal access.	**Yes**	**Shall**	**Shall**	AJ: **Shall**		All	All		
AC-9. User access capabilities include a timeout feature that automatically logs out a user who has logged in after a period of user inactivity.	AC-9a. User access capabilities **Shall** include a timeout feature that automatically logs out a user who has logged in after a period of user inactivity.	**Yes**	**Shall**	**Shall**	AJ: **Shall**		All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
AC-10. For user access to critical devices, applications, or systems, multifactor authentication is used.			Should	Should (In practice may not be easily available for technicians in the field)	AJ: Shall		All	All	MFA is default off late / considered minimal cyber hygiene	SCE Draft Response: Network, System and Component levels are the vantage points for deploying 2FA, this is another stop gap to be assessed for its mitigation capability.
5.3.2 System Access Recommendations										
Necessary Recommendations										
AC-11. System authentication – Systems, software applications, and devices are authenticated for access to other systems, software applications, and devices through cybersecurity authentication mechanisms, such as certificates, tokens, white lists, etc.	AC-11a. System authentication – Systems, software applications, and devices Shall be authenticated for access to other systems, software applications, and devices through cybersecurity authentication mechanisms, such as certificates, tokens, white lists, etc.	Yes	Shall	Shall	AJ: Shall	Shall	EMS DERMS Aggregator Remote Management Applications to manage DER devices	All	System authentication for systems rather than devices	
AC-12. System authorization – Systems, software applications, and devices are assigned permissions to access data, services, resources, or objects granted by the security policy. These permissions are also constrained to one or more of the following: reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.	AC-12a. System authorization – Systems, software applications, and devices Shall be assigned permissions to access data, services, resources, or objects granted by the security policy. These permissions Shall also be constrained to one or more of the following: reading (downloading), writing (uploading), issuing control commands, creating new items, or deleting items.	Yes	Should	Shall	AJ: Shall	Shall	DER Gateways Inverters EMS DERMS Aggregator Remote Management Applications to manage DER devices	All	System authentication for systems, controllers for devices, and smart devices. Need granular RBAC authorization to individual applications and databases within systems and to individual devices. Perhaps default roles and default access for those roles See section 5.4.4 on RBAC for adding clarifications	
AC-13. System authentication is performed as closely as possible to the end system, software application, and/or device.	AC-13a. System authentication Shall be performed as closely as possible to the end system, software application, and/or device.	Yes	Shall	Shall	AJ: Shall			All	"As closely as possible" is not testable. However, this is really a way of stating the authentication for granular RBAC. The details of such granularity needs further definition See section 5.4.4 on RBAC for adding granularity requirements	"As closely as possible" is not testable

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
AC-14. System accountability and non-repudiation – Systems, software applications, and device actions are logged so events can be traced, time-synchronized with other events, and/or audited.	AC-14a. System accountability and non-repudiation – Systems, software applications, and device actions **Shall** be logged so events can be traced, time-synchronized with other events, and/or audited.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	DER Gateways Inverters EMS DERMS Aggregator Remote Management Applications to manage DER devices	All	The accuracy of time-sync is open AJ: Typically, these events are not cached, pushed to SIEM in real-time – network latency ok See SM-6 on Time synchronization	Time-synchronized to what min accuracy?
5.3.3 Access Management Recommendations										
Necessary Recommendations										
AC-15. Default passwords are required to be changed upon installation or any change of ownership or location of equipment or systems.	AC-15a. Default passwords **Shall** be required to be changed upon installation or any change of ownership or location of equipment or systems.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All		
AC-16. Multiple users and multiple software applications with different access permissions are supported by systems.			**Should**	**N/A**	AJ: **Shall**	Should		Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Need to define "system". Applicable to systems that support multiple roles. Each RBAC role has an individual set of permissions AJ: Scope of this document is the device in the system that generates/	Need to define "system" Network, System, Component in part to the reference architecture.
AC-17. Secure interfaces provide an open and documented method for adding and updating user accounts, passwords, and assignment to roles.	AC-17a. Secure interfaces **Shall** provide an open and documented method for adding and updating user accounts, passwords, and assignment to roles.	**Yes**	**Should**	**Shall**	AJ: **Shall**	Shall	EMS DERMS Aggregator Remote Management Applications to manage DER devices	All		
AC-18. All access changes are logged.	AC-18a. All access changes **Shall** be logged.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
5.3.4 Role-Based Access Control (RBAC) Recommendations						SCE reinforces that these are initial standard guidance recommendations and should not be viewed as the only strategy				***Access control requirements enable accountability and make it difficult for an adversary to have complete control.*** ***With a RACI the RBAC can be supported at various levels in a consistent manner.*** ***To require an IEC 62351-8 token assumes that there is respective infrastructure in place, those elements need to be referenced to support the implementation.***
Necessary Recommendations										
AC-19. Role-Based Access Control (RBAC) is supported for all interactions between users, systems, software applications, and devices.	AC-19a. Role-Based Access Control (RBAC) **Shall** be supported for all interactions between users, systems, software applications, and devices.	**Yes, the concept is Role-Based Access Control, but the techniques for implementing this could be different**	**Should**	**Shall**	AJ: **Shall**	Additional discussion is warranted regarding level of implementation	DER Gateways, DAS, EMS, DERMS Aggregator Remote Management Applications to manage DER devices	All		
AC-20. Users are assigned to one or more roles which have the permissions necessary for the user to perform their tasks.	AC-20a. Users **Shall** be assigned to one or more roles which have the permissions necessary for the users to perform their tasks. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes, need to figure out which systems this applies to**	**Should**	**Shall for larger** **Should for small**	AJ: **Shall**		All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Is a **Shall** for larger systems or aggregations of many systems more than xx watts in total Size needs further discussion	
AC-21. Systems, software applications, and devices are assigned to one or more roles as needed for them to perform their functions.	AC-21a. Systems, software applications, and devices **Shall** be assigned to one or more roles as needed for them to perform their functions. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes, need to figure out which systems this applies to**	**Should**	**Shall for medium** **Should for small**	AJ: **Shall**		DER Gateways DAS, EMS, DERMS Aggregator Remote Management Applications to manage DER devices	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		
AC-22. All entities responding to requests for access verify that the requests are permitted for the roles making the requests. The requests are rejected if the roles do not have the correct permissions. Rejected requests are logged.	AC-22a. All entities responding to requests for access **Shall** verify that the requests are permitted for the roles making the requests. The requests **Shall** be rejected if the roles do not have the correct permissions. Rejected requests **Shall** be logged. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes, need to figure out which systems this applies to**	**Shall**	**Shall for medium** **Should for small**	AJ: **Shall**		DER Gateways DAS, Network Security Devices, EMS DERMS Aggregator Remote Management Applications to manage DER devices	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
AC-23. The DER and other objects have the capability of defining multiple user-defined roles. Each role has the capability of having any combination of rights including: Reading DER nameplate or configuration information, measurement data (voltage, current, power, energy, status, alarms, etc.), and control mode settings; Writing control mode settings that alter the operational characteristics of the DER; Additional functionality is documented	AC-23a. The DER and other objects **Shall** have the capability of defining multiple user-defined roles. Each role **Shall** have the capability of having any combination of rights including: Reading DER nameplate or configuration information, measurement data (voltage, current, power, energy, status, alarms, etc.), and control mode settings; Writing control mode settings that alter the operational characteristics of the DER; Additional functionality **Shall** be documented. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes, may need to combine or correlate with other access control requirements**	**Should**	**Shall for medium** **Should for small**	AJ: **Shall**		All	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Role based access control	
AC-24. The DER and other objects support the "push" RBAC model and accept valid role tokens.	AC-24a. The DER and other objects **Shall** support the "push" RBAC model and accept valid role tokens. Individual DER (< 1 MW?) and individual EVs may be exempted.	**No, too prescriptive**	**Should**	**Should**	AJ: **Shall** (for medium/large) **Should** for small		DER Gateways, DAS, Network Security Devices, EMS, DERMS, Aggregator Remote Management Applications to manage DER devices	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		
AC-25. A role is assignable in the DER and other objects using an IEC 62351-8 Profile A token. Additional methods of assigning roles to subjects/users are permitted.	AC-25a. A role **Shall** be assignable in the DER and other objects using an IEC 62351-8 Profile A token. Additional methods of assigning roles to subjects/users **Shall** be permitted. Individual DER (< 1 MW?) and individual EVs may be exempted.	**No, too prescriptive**	**Should**	**Should**	AJ: **Shall** (for medium/large) **Should** for small		DER Gateways DERMS Aggregator	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		
AC-26. All RBAC changes are logged.	AC-26a. All RBAC changes **Shall** be logged.	**Yes**	**Shall**	**Shall**	AJ: **Shall**		All	Small DER, Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
B.2.4 5.4 Data Security (DS) Recommendations										
5.4.1 Security for Data-at-Rest										
Necessary Recommendations										
DS-1. RBAC methods are used to authorize any viewing, read, write, create, or delete access to stored data, particularly where different organizations have different types and levels of authority to access the same stored data. See clause 5.x for more details.	DS-1a. RBAC methods **Shall** be used to authorize any viewing, read, write, create, or delete access to stored data, particularly where different organizations have different types and levels of authority to access the same stored data. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Should**	**Shall for medium** **Should for small**	AJ: **Shall** (for medium/large) **Should** for small	**Should**	DER Gateways, DAS Network Security Devices, EMS, DERMS Aggregator Remote Management Applications to manage DER devices	Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Applicable for confidential data	SCE Draft Comments: For this item to remain a **Should**, the stakeholders need to agree on the data class and handling in transit and at rest. It must be made clear to the DER asset owner who has access to their PII.
DS-2. Cryptography used to secure data do not use any deprecated methods	DS-2a. Cryptography used to secure data **Shall** not use any deprecated methods	**Yes**	**Should**	**Shall**	AJ: **Shall**	**Shall**	All	All	AJ: This can be a custom item based on deployment clarified via IC agreement	
DS-3. On removing, disposing, or repurposing devices, a sanitization process is used to remove any confidential data at rest on the device, such as a factory reset option or securely recycled.	DS-3a. On removing, disposing, or repurposing devices, a sanitization process **Shall** be used to remove any confidential data at rest on the device, such as a factory reset option or securely recycled. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes, but confirm with AJ and ensure no specific sanitization process is implied**	**Shall**	**Shall for medium** **Should for small**	AJ: **Should**	**Should**	All	Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		SCE Draft Comments: There are services to support electronic equipment disposition, such as hard drives where the drive is shredded to ensure data is not recoverable. Given a hard drive may have anything from device configuration, network communications and asset owner information, it is highly recommended to require "**Shall**" hard drives and any other storage media to be destroyed based on data classification and business impact.
DS-4. Hard drives storing sensitive data are encrypted.	DS-4a. Storage **Shall** have the capability of encrypting confidential (PII, financial) data. Individual DER (< 1 MW?) and individual EVs may be exempted.	**No, covered by other regulations**	**Should**	**Shall for medium** **Should for small**	AJ: **Should**	**Should**	All	Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	AJ: If there is a TPM implementation, telemetry data may not be of any value that need to be encrypted	

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
Optional Recommendations										
DS-5. All devices have their security certificate credentials securely stored in a Secure Element (SE) such as Trusted Platform Module (TPM) chips or equivalent solution to secure the software components of the device.	DS-5a. All devices **Shall** have their security certificate credentials securely stored in a Secure Element (SE) such as Trusted Platform Module (TPM) chips or equivalent solutions to secure the software components of the device. Individual DER (< 1 MW?) and individual EVs may be exempted. A phased implementation timeline may be used.	**Yes**	**Should**	**Shall for medium** **Should for small**						
DS-6. Verfication is done to help ensure sensitive information no longer exists on the device following factory reset.	DS-6a. Verification **Shall** be done to help ensure sensitive information no longer exists on the device following factory reset. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Shall**	**Shall for medium** **Should for small**	AJ: **Shall**	Concentrated "Necessary Recommendations" for purpose of this review. Have provided comments to aid discussions	DER Gateway Inverters	Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Better handled in a roadmap from CPUC like Phase 1/2/3 requirements – defining a phase wise implementation so that TPM etc., can be incorporated and certified into all devices used in DER	
5.4.2 Security for Data-in-Transit										
Necessary Recommendations										
DS-7. Every communication session requires authentication of both the source (system, device, database, and/or software application) of the data and the recipient (system, device, database, and/or software application) of the data.	DS-7a. Every communication session **Shall** require authentication of both the source (system, device, database, and/or software application) of the data and the recipient (system, device, database, and/or software application) of the data. Local EPS networks with communications using Modbus may be exempted.	**Yes**	**Shall**	**Should for DNP3, remote Modbus, Shall for IEEE 2030.5** **Shall for Proprietary**	AJ: agree		All DSO communications. All communication with Aggregators (both to DERs and to DSO) All communication through public Internet		Since Modbus is the most prevalent protocol used in DERs, and is specified in 1547-2018, this cannot be applied to local communication between Inverters, DAS, Meters, DER Gateway, EMS etc., DNP3 has security but is not often used	Since Modbus is the most prevalent protocol used in DERs, and is specified in 1547-2018, this cannot be applied to communication between Inverters, DAS, Meters, DER Gateway, EMS etc., SCE Draft Comments If unauthenticated sessions were permitted by the DSOs to communicate with their EMS system, it would present significant risk not only to the DER but to the other assets within EMS purview.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
DS-8. Communication sessions have time limits and require the renegotiation and reauthentication of new communication sessions.	DS-8a. Communication sessions **Shall** have time limits and **Shall** require the renegotiation and reauthentication of new communication sessions. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Shall**	**Shall for medium** **Should for small**	AJ: **Shall**		All	Medium DER, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Re-negotiating the communication over cellular network increases data usage.	Re-negotiating the communication over cellular network increases data usage.
DS-9. RBAC methods are used to authorize any viewing, read, write, create, or delete access to data-in-transit, particularly where different organizations have different types and levels of authority to access the same data. See section B.2.3 for RBAC recommendations.	DS-9a. RBAC methods **Shall** be used to authorize any viewing, read, write, create, or delete access to data-in-transit, particularly where different organizations have different types and levels of authority to access the same data. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Should**	**Shall for medium** **Should for small**	AJ: **Shall**		All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		
DS-10. Time-sensitive data is checked to determine if it has arrived within the expected time window.				**NA**					AJ: DER data time interval requirements may vary .	
DS-11. Data-in-transit is time-stamped so that it may be stored and possibly logged with accurate time information.	DS-11a. Data-in-transit **Shall** be time-stamped so that it may be stored and possibly logged with accurate time information. Individual DER (< 1 MW?) and individual EVs may be exempted. Communications using Modbus may be exempted.	**Yes, with the exceptions noted**	**Shall**	**Should**	AJ: **Should**	**Should**	All	Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	Modbus does not support timestamp. This is applicable for protocols that support timestamp.	Modbus does not support timestamp. This is applicable for protocols that support timestamp. How accurate?
DS-12. TLS v5.3 is used where practical, as specified in IEC 62351-3 recognizing that some installations may still need to use TLS 5.2.				**Should**	AJ: **Should**		All			SCE Comment TBD
DS-13. X.509v3 digital certificates are used as specified in IEC 62351-9	DS-13a. For IEEE 2030.5, digital certificates **Shall** follow the CSIP requirements. Where supported by the communications protocol, X.509v3 digital certificates **Shall** be used as specified in IEC 62351-9.	**No, already defined in communication protocols or associated documents**		**Follow CSIP**					AJ: **Should** adhere to IEEE 2030.5	SCE Draft Comment Certificates have provided a good layer of defense against unauthorized access, however some implementations like self-signed certificates have been exploited. In following the industry best practice provided by NIST (Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (nist.gov)) is not to be expected as set it and forget it, there will need to be good key management established and it bodes well when certificates can be leveraged for more than authentication, like deep packet inspection.

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
DS-14. Key management is used as specified in IEC 62351-9.	DS-14a. Key management **Shall** be used as required by mutually-agreed security policies. Where possible, key management **Shall** follow the requirements specified in IEC 62351-9.	**Yes, as reworded in green**	**Should**	**NA**	Some kind of key management is required, but different DSOs and vendors manage their keys differently		??		Intra-DER communications do not use keys currently. Applicable only when IEC 61850 is supported as a 1547 protocol. Not sure of status of key management for DNP3 SA	Intra-DER communications do not use keys currently. Applicable only when IEC 61850 is supported as a 1547 protocol. Not sure of status of. key management for DNP3 SA
Optional Recommendations										
DS-15. Data-in-transit include "quality" information to reflect the validity and potentially the source of the data										
DS-16. If data-in-transit is encrypted, deep packet inspection techniques are available to verify the integrity of the data										
DS-17. For sessionless communications (e.g. streaming data), individual data-in-transit packets include source authentication and RBAC permissions information and are encrypted to support transit over zero-trust networks			Shall	**NA**			All	All	Where might streaming data be used?	
B.2.5 5.5 Security Management (SM) Recommendations										
5.5.1 Lifecycle Management										
Necessary Recommendations										
SM-1. Asset inventories include all physical devices.	SM-1a. Asset inventories **Shall** include all physical devices.	**Yes**	**Shall**	**Shall but needs more guidance on details – to be left up to contractual agreements**	AJ: **Shall**	**Shall**	All	All	AJ: to be maintained by respective asset owners	Virtual Cloud resources are likely to be incorporated to support the scale of growth, therefore virtual needs to be added to device/component asset list.
SM-2. Asset inventories include all installed firmware, software and applications with version information including external systems.	SM-2a. Asset inventories **Shall** include all installed firmware, software and applications with version information including external systems.	**Yes**	**Shall**	**Shall but needs more guidance on details – to be left up to contractual agreements**	AJ: **Shall**	**Shall**	All	All	AJ: A mature approach will be to enumerate SBoM and associated vulnerabilities	
SM-3. Asset inventories include all external services such as cloud services and third party managed services.	SM-3a. Asset inventories **Shall** include all external services such as cloud services and third party managed services.	**Yes**	**Shall**	**Shall but needs more guidance on details – to be left up to contractual agreements**	AJ: **Shall**	**Shall**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-4. All assets have identities that are securely associated with them, such as fastened to a physical device, or included in a TPM chip, or linked to a cryptographic certificate.			**Depends on the asset…**	**Should**	AJ: **Should**	**Should**	DER Gateways Inverters DAS Network Security Devices Aggregator	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	AJ: Such capabilities demonstrate vendor maturity and will be encouraged by DSOs	SCE Draft Comment At a minimum **SHALL** have an identity on the reference architecture and be identified in the asset list by some form of authorized serial number etc.
SM-5. Security procedures, processes, and technologies are evaluated on an recurring basis (or when triggered by system changes or industry events) and updated accordingly.				**Should**	AJ: **Should**	**Should**	All	All	Better handled through Organizational Security Policies and managed through certifications like ISO 27001	Better handled through Organizational Security Policies and managed through certifications like ISO 27001
SM-6. Time synchronization, of adequate precision and accuracy, is implemented across all key DER components, networks, logs, and interfaces to external stakeholders, (e.g. as per IEEE 1588, RFC 5905 (NTP)). Protection is implemented against attacks on clocks and the time synch protocol, to help ensure that the timestamps of audit logs capture a series of events truly chronologically with the necessary time resolution.	DS-13a. For IEEE 2030.5, digital certificates **Shall** follow the CSIP requirements. Where supported by the communications protocol, X.509v3 digital certificates **Shall** be used as specified in IEC 62351-9.	**No, already defined in communication protocols or associated documents**	Shall	Shall for Time Synchronization Should for protection of clocks	AJ: Should	Should	DER Gateways Inverters	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation	"Adequate precision and accuracy" needs to be defined. Non-Internet time synchronization can be via GPS, WWVB, cellphone networks, local time server, etc.	SCE Draft Comments The risk impact to the "key DER components" from out of sync time must be evaluated to determine where this must be a SHALL.
SM-7. Operating system management include: Operating systems installed on security devices must be within vendor support window; Operating systems on industrial equipment outside of vendor support windows are assessed, isolated and/or recommended for replacement.	DS-14a. Key management **Shall** be used as required by mutually-agreed security policies. Where possible, key management **Shall** follow the requirements specified in IEC 62351-9.	**Yes, as reworded in green**	**Should**	**Shall**	AJ: **Shall**	**Shall**	All	Medium DERs, Large DERs or Critical DERs or Aggregators with more than 10 MW in Aggregated Generation		
SM-8. Hardware, software and security upgrades are noted in the asset inventories, along with any updated identities.	SM-8a. Hardware, software and security upgrades **Shall** be noted in the asset inventories, along with any updated identities.	**Yes**	**Should**	**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-9. Decommissioning or disposal of any asset is noted in the asset inventories, including the current status of that asset.	SM-9a. Decommissioning or disposal of any asset **Shall** be noted in the asset inventories, including the current status of that asset.	**Yes**	**Should**	**Shall**	AJ: **Shall**	**Shall**	All	All		
5.5.2 Supply Chain Management										
Necessary Recommendations										***Under Review***

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-10. Risk management plans include supply chain security as part of the risk assessment and risk amelioration procedures.			Should	Should	AJ: Should		All	All	AJ: Applicable for respective asset owners Difficult for DSOs to enforce compliance of vendors. Unlike some other industries, there are a large number of stakeholders and vendors, making enforcement difficult at this time. However, DOE and others are pushing for more supply chain enforcement	
SM-11. Supplier security audits or third party certifications are required of vendors to help ensure adequate cyber security policies are in place.			Should	Should	AJ: Should		All	All	AJ: DSOs may encourage vendors for this	
SM-12. All asset identities are validated as they are received and as they are implemented, installed, or used in updates or patches.			Should	Should	AJ: Should		All	All	DSOs may encourage vendors for this	
SM-13. Appropriate language on supply chain sources and validation procedures is added to specifications and agreements.			Should	Should	AJ: Should		All	All		
SM-14. Shipping and handling of equipment comply with security policy requirements.			Should	Should	AJ: Should		All	All		
SM-15. A process is in place to help ensure that software posesses expected security and robustness characteristics. For example, the vendor supplies evidence of following applicable coding best practices frameworks or the software can be evaluated against applicable standards if not vendor supplied (such as open source software).			Should	Should	AJ: Should		All	All		
5.5.3 Patch Management										
Necessary Recommendations										
SM-16. DER and associated systems support the ability to be updated.	SM-16a. DER and associated systems **Shall** support the ability to be updated.	Yes	Shall	Shall	AJ: Shall	Shall	All	All		
SM-17. DER and associated systems support the ability for remote updates.	SM-17a. DER and associated systems **Shall** support the ability for remote updates.	Yes	Shall	Shall	AJ: Shall	Shall	All	All		
SM-18. DER and associated systems support the ability for automated updates.	SM-18a. DER and associated systems **Shall** support the ability for automated updates, if mutually-agreed by security policies.	Yes	Shall	Should	AJ: Should	Should	All	All	Only if contractually required because automated updates may impact other systems	

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-19. DER and associated systems support the ability to be configured for and disable automated updates.	SM-19a. DER and associated systems **Shall** support the ability to be configured for and disable automated updates, if mutually-agreed by security policies.	No	Should	Should	AJ: Should	Should	All	All	Only if contractually required	
SM-20. DER and associated systems check periodically whether there is an available update.	SM-20a. DER and associated systems **Shall** check periodically, within 7 days, whether there is an available update.	Yes	Shall	Shall	AJ: Shall	Shall	All	All	Every 7 days [SunSpec] AJ: implementation specific	Every 7 days [SunSpec]
SM-21. DER and associated systems verify the authenticity and integrity of software updates.	SM-21a. DER and associated systems **Shall** verify the authenticity and integrity of software updates.	Yes	Shall	Shall	AJ: Should	Shall	All	All	AJ: Mitigate supply chain risk "**Shall**" Confirm patches are from the correct source, but "**Should**" not necessarily confirm that the source does not have a supply chain risk.	
SM-22. DER and associated systems are commissioned with the most recent firmware version.	SM-22a. DER and associated systems **Shall** be commissioned with the most recent firmware version.	Yes	Shall	Shall	AJ: Shall	Shall	All	All		
SM-23. DER product suppliers document the firmware patching policy.	SM-23a. DER product suppliers **Shall** document the firmware patching policy.	Yes		Shall	AJ: Shall	Shall	All	All		
SM-24. DER product suppliers provide a policy on product support including firmware updates.	SM-24a. DER product suppliers **Shall** provide a policy on product support including firmware updates.	Yes		Shall	AJ: Shall	Shall	All	All		
SM-25. DER product suppliers provide software updates that are non-repudiable. Software update non-repudiation provides the product supplier with proof of patch delivery and the recipient is provided with proof of the product supplier's identity.	SM-25a. DER product suppliers **Shall** provide software updates that are non-repudiable. Software update non-repudiation **Shall** provide the product supplier with proof of patch delivery and the recipient **Shall** be provided with proof of the product supplier's identity.	Yes, pending PG&E agreement	Shall	Shall	AJ: Should	Shall	All	All	AJ: Mitigate supply chain risk "**Shall**" Confirm updates are from the correct source, but "**Should**" not necessarily confirm that the source does not have a supply chain risk. Still need compensating measures.	
SM-26. DER product suppliers use an appropriate standard to approve the selection of cryptography modules. DER product supplier may use a FIPS 140-2 Level 2 or greater cryptography modules for all keys used in code signing processes, with equivalent certifications recognized as acceptable.	SM-26a. DER product suppliers **Shall** use an appropriate standard to approve the selection of cryptography modules. DER product supplier may use a FIPS 140-2 Level 2 or greater cryptography modules for all keys used in code signing processes, with equivalent certifications recognized as acceptable. NIST 800-52 Guidelines may also be used.	Yes		Shall	AJ: Shall	Shall	All	All	Review NIST 800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations for key strength requirements to see if more applicable. Then review **Should** vs **Shall**.	

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-27. DER product suppliers inform integrators, aggregators, and owners in a recognizable and apparent manner (e.g., on a website) that a security update is available.	SM-27a. DER product suppliers **Shall** inform integrators, aggregators, and owners in a recognizable and apparent manner (e.g., on a website) that a security update is available.	**Yes**		**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-28. DER product suppliers provide information on applicability, compatibility, and risks mitigated by the patch.	SM-28a. DER product suppliers **Shall** provide information on applicability, compatibility, and risks mitigated by the patch.	**Yes**		**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-29. DER product suppliers notify the aggregator, owner, or operator when the application of a software update will disrupt the basic functioning of the DER.	SM-29a. DER product suppliers **Shall** notify the aggregator, owner, or operator when the application of a software update will disrupt the basic functioning of the DER.	**Yes**		**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-30. DER product suppliers provide, in an accessible way that is clear and transparent to the aggregator, owner, or operator, the defined DER device support period.	SM-30a. DER product suppliers **Shall** provide, in an accessible way that is clear and transparent to the aggregator, owner, or operator, the defined DER device support period.	**Yes**		**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-31. DER product suppliers publish a list of all patches and their approval status.	SM-31a. DER product suppliers **Shall** publish a list of all patches and their approval status.	**Yes**	**Should**	**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-32. When technically feasible, DER product suppliers provide a patch or alternative risk mitigation for security vulnerabilities within 60 days of notification or internal discovery by the DER product supplier.	SM-32a. When technically feasible, DER product suppliers **Shall** provide a patch or alternative risk mitigation for security vulnerabilities within 60 days of notification or internal discovery by the DER product supplier.	**Yes**		**Shall**	AJ: **Shall**	**Shall**	All	All		
SM-33. DER product suppliers use mechanisms that prevent firmware downgrade attacks, i.e., prevent updates to previous software versions.	SM-33a. DER product suppliers **Shall** use mechanisms that prevent firmware downgrade attacks, i.e., prevent updates to previous software versions.	**Yes, pending SCE agreement**	**Shall**	**Shall**	AJ: **Shall**	**Should**	All	All	SunSpec has such a test and could be a contractual **Shall**. That document **Should** be reviewed.	
SM-34. DER product suppliers write segmented/modular software and complete UL 1998 or UL 60730 certification of all DER firmware to reduce product re-evaluations.			**Should**	**Should**	AJ: **Should**	**Should**	All	All		
SM-35. DER product suppliers provide adequate warning (at least two years in advance) when components are reaching 'end of life' or if cyber security patches will no longer be made available.			**Should**	**Should**	AJ: **Should**	**Should**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-36. DER product suppliers include a Software Bill of Materials (SBOM) NTIA Minimum Elements in a machine-readable format. It is recommended to use SPDX, CycloneDX, SWID Tags or other industry compliant formats.			Should	Should	AJ: Should	Should	All	All	"Ball of Hair"	
SM-37. DER aggregators document the patching policy.			Should	Should	AJ: Should	Should	All	All		
SM-38. DER aggregators maintain a patching schedule which includes a planned interval for evaluation of new patches.			Should	Should	AJ: Should	Should	All	All		
SM-39. DER aggregators provide the ability to opt-out of automated updating.				Should	AJ: Should	Should	All	All		
SM-40. DER aggregators maintain an up-to-date inventory of all electronic devices in the DER system with the associated patch version.			Should	Should	AJ: Should	Should	All	All		
SM-41. DER aggregators maintain a record of all previously installed firmware versions for each device.			Should	Should	AJ: Should	Should	All	All		
Optional Recommendations						SCE focused on the "Necessary Recommendations" for this review				
SM-42. DER owners document the firmware update policy.										
SM-43. DER owners document patch management process for tracking, evaluating, and installing DER security patches. The tracking portion include the identification of source(s) of DER security patches.	SM-43a. DER owners **Shall** document patch management process for tracking, evaluating, and installing DER security patches. The tracking portion **Shall** include the identification of source(s) of DER security patches.	**Yes, pending PG&E and SCE agreement**	Should	Shall			All	All	This item indicates that DER owners do the process, but presumably the process is done by the DER	This item indicates that DER owners do the process, but presumably the process is done by the DER
SM-44. For applicable DER patches, within the schedule established in the firmware update policy, the DER owners take one of the following actions: (a) apply the applicable patch(es), (b) create a dated mitigation plan, or (c) revise an existing mitigation plan. Mitigation plans include planned actions to mitigate the vulnerabilities addressed by each security patch within 35 days or a timeframe established by the update policy.										
SM-45. DER owners implement the mitigation plan within 35 days or a timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe is approved.										

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-46. DER owners check every 35 days or other fixed periodicity documented in the firmware update policy whether there is an available update.										
SM-47. DER owners maintain an up-to-date inventory of all electronic devices in the DER system with the associated patch version.										
SM-48. DER owners maintain a record of all previously installed firmware versions for each device.	SM-48a. DER owners **Shall** maintain a record (log) of all previously installed firmware versions for each device.	**Yes, pending PG&E and SCE agreement**	**Should**	**Shall**			All	All		
SM-49. DER owners test the installation of patches in a way that accurately reflects the production environment.										
SM-50. DER owners update records as indicated in the firmware patch policy to include installed, authorized, effective, and released firmware versions.										
SM-51. DER devices support local updates.									Only remote updates are mentioned by SunSpec	Only remote updates are mentioned by SunSpec
SM-52. DER product suppliers publish the firmware patching policy publicly.										
SM-53. DER product suppliers inform asset owners within 30 days after a patch is released for third-party software operating within the DER.										
SM-54. DER patches may include patch data in a IETF RFC 4108-compliant patch manifest.										
5.5.4 Security Event Logging										
Necessary Recommendations										
SM-55. Systems include a security event log which includes, at a minimum: Successful and unsuccessful login attempts; Detected malicDSOs code; Detected failure of event logging; Changes to device settings; Software updates and changes; Changes to access controls such as RBAC permissions and roles, account creation, updates, and deletion	SM-55a. Systems **Shall** include a security event log which includes, at a minimum: Successful and unsuccessful login attempts; Detected malicious code; Detected failure of event logging; Changes to device settings; Software updates and changes; Changes to access controls such as RBAC permissions and roles, account creation, updates, and deletion	**Yes**	**Shall**	**Shall**	AJ: **Shall**	**Shall**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-56. Systems are able to store security log events locally if they are unable to export them.	SM-56a. Systems **Shall** be able to store security log events locally if they are unable to export them. At a minimum, systems **Shall** store security event logs for 90 days, power system logs for 90 days, and network traffic for 14 days.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All	Devices **SHALL** store security event logs for 90 days, power system logs for 90 days, and network traffic for 14 days. [SunSpec]	Devices **SHALL** store security event logs for 90 days, power system logs for 90 days, and network traffic for 14 days. [SunSpec]
SM-57. Systems include timestamps in all logs including security logs with sufficient resolution to be useful.	SM-57a. Systems **Shall** include timestamps in all logs including security logs with sufficient resolution to be useful, as determined by mutually-agreed security policies.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All	Some may require timestamp resolution of 1 millisecond (or ??)	Some may require timestamp resolution of 1 millisecond
SM-58. System internal clocks are kept in sync with appropriate time sources of adequate precision, refer to SM-6 for more details.	SM-58a. System internal clocks **Shall** be kept in sync with appropriate time sources of adequate precision, such as the Network Time Protocol (NTP).	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All	Adequate precision needs to be defined for different situations. Sync across DER are the most important. Should the capability to sync to NTP be required?	Adequate precision needs to be defined for different situations
SM-59. Write access to security logs is restricted to only adding information and prevent modification and/or deletion of events.	SM-59a. Write access to security logs **Shall** be restricted to only adding information and **Shall** prevent modification and/or deletion of events.	**Yes**	**Shall**	**Shall**	AJ: **Shall**	Shall	All	All		
Optional Recommendations										
SM-60. Power system logs recommendations include: Power system logs for output anomalies; When a function is enabled or disabled; When a function is activated and has an impact on output power; May include data validation of incoming packets such as checksums; Firmware updates are validated and verified prior to installation.	SM-60a. Power system logs **Shall** include: Power system logs for output anomalies; When a function is enabled or disabled; When a function is activated and has an impact on output power; May include data validation of incoming packets such as checksums. Firmware updates **Shall** be validated and verified prior to installation.	**Yes**	**Shall**	**Shall**	**Shall**		Manufacturer provides and test the capability for all DER; Aggregator and/or Implementor enables appropriate logging	All	Some sites may log more power system information than others. The details need to be resolved. Although power system logs may or may not exist, from a security perspective there needs to be a log of "anomalous" events.	Some sites may log more power system information than others. The details need to be resolved.
SM-61. Power system and security logs are monitored on a recurring basis.	SM-61a. Power system and security logs **Shall** be monitored on a recurring basis.	**Yes**	**Shall**	**Shall**			All	All	Monitoring of logs may vary by size and criticality of DER site	Monitoring of logs may vary by size and criticality of DER site
SM-62. Security logs are securely but easily remotely retrievable and remotely accessible in real time.	SM-62a. Security logs **Shall** be securely but easily remotely retrievable and remotely accessible in real time.	**Yes**	**Shall**	**Shall**			All	All	Logs are able to be retrieved by a remote site, including by push mechanisms. These logs are also able to be retrieved in near real time	

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-63. Security event log messages are capable of being prioritized based on user definable criteria.	SM-63a. Types of security event log messages **Shall** be capable of being categorized and/or prioritized based on user definable criteria. For larger systems?	**??, pending PG&E and SCE discussion**	**Should**	**Shall**			All	All		
SM-64. The ability to aggregate security logs in a centralized Security Information and Event Management (SIEM) systems is supported.	SM-64a. The ability to aggregate security logs in a centralized Security Information and Event Management (SIEM) systems **Shall** be supported. Individual DER (< 1 MW?) and individual EVs may be exempted.	**Yes**	**Shall**	**Shall**			DSO, Aggregator	Large, Plant, Critical, Large Aggregation		
SM-65. Power system and security log storage allocation is sufficient to store event data for the minimum required timeframe.	SM-65a. Power system and security log storage allocation **Shall** be sufficient to store event data for the minimum required timeframe.	**Yes**	**Shall**	**Shall**			All	All		
SM-66. For power system and security logs with limited memory allocations, warnings on overwriting log entries are provided.	SM-66a. For power system and security logs with limited memory allocations, warnings on overwriting log entries **Shall** be provided.	**Yes**	**Shall**	**Shall**			All	All		
SM-67. Power system and security logs are periodically backed up to another system.	SM-67a. Power system and security logs **Shall** be periodically backed up to another system	**Yes**	**Shall**	**Shall**			All	All		
5.5.5 Data Backups										
Necessary Recommendations										***The requirements are related to Business Continuity Planning and Disaster Recovery (BCP & DR) practices to support return to service in an orderly and efficient manner post an outage.*** ***Database security is key in ensuring data integrity and must be well maintained as noted in the respective operational plan.***
SM-68. All databases, software applications, and operating system data are backed up on a periodic or "when changed" basis to an offline, off premise location.			**Should**	**Should**		**Should**	All	All	Applicable for asset owners/operator for protection against ransomware, e.g. DSOs, aggregators for large plants, etc. **Should** be part of Organization Cyber security policy	**Should** be part of Organization Cyber security policy
SM-69. Restorable snapshots of all field device configurations **Shall** be stored off site and securely with notation of which site the backup is applicable to, when it was taken, and by whom.			**Should**	**Should**		**Should**	All	All		

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
SM-70. An up to date plan is documented and periodically reviewed for feasibility and completeness.			Should	Should		Should	All	All		
SM-71. Data backups are kept off line or disconnected from the network when not copying data to prevent loss of backup concurrent with the loss of network connected data such as in the event of a ransomware or similar malware attack.			Should	Should		Should	All	All		
Optional Recommendations										
SM-72. System restoration plans and associated backup media are periodically tested to restore the system to full operation from offline backups. Testing may include but not be limited to evaluation of timing, completeness, security of backups, procedures.										
5.5.6 Software Operating Systems and Application Security										
B.2.6 5.6 Coping with and Recovering from (CM) Security Events Recommendations										
5.6.1 Pre-Event Coordination Planning and Cross-Organization Security Studies										
Necessary Recommendations										
CM-1. Cross-organizational risk asessments are performed and inform incident analysis and response plans.										
CM-2. Plans are developed and clearly documented for coping and recovering from cybersecurity events and follow industry accepted best practices such as those included in NIST SP 800-61.										
CM-3. Response plans include allocation of responsibilities and decision authorities for actions and consider how responsibilites may change depending on the type of incident and the stakeholders involved.										

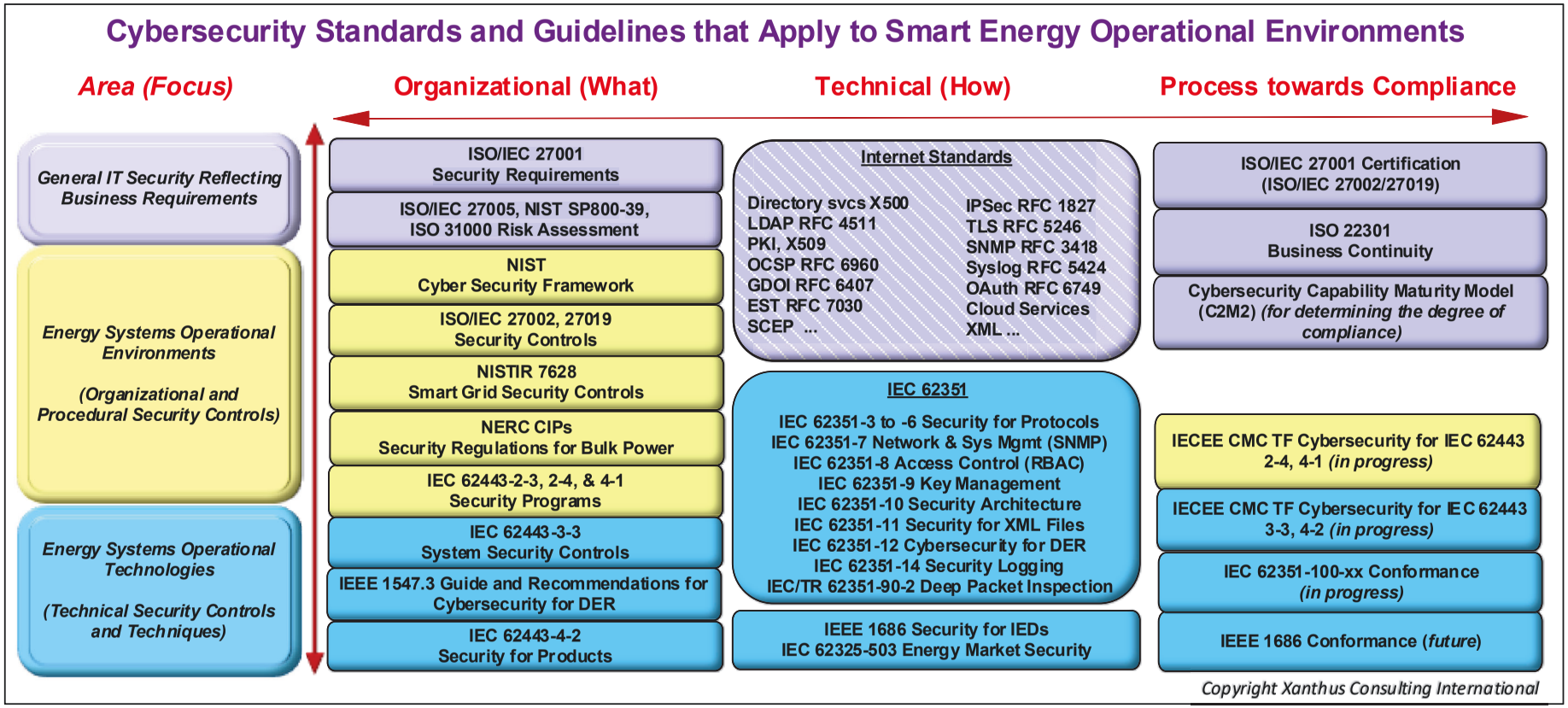
IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
CM-4. Baselines for network and system configurations, installed applications, user accounts, network traffic, and other useful information for incident response forensics are captured and updated as necessary.										
CM-5. Stakeholders agree and clearly document what would be considered a potential security event that would require immediate disclosure to all relevant stakeholders.										
CM-6. At a very minimum, all stakeholders have up to date contact details for all of the other applicable stakeholders for a given facility for the timely communication of cybersecurity related issues.										
CM-7. For each communicated potential security incident, the action that may be taken by the reporting party is reported to any other parties that might be impacted by such action.										
Optional Recommendations										
CM-8. Security event notification formats, time windows, and procedures are defined and implemented for all stakeholders.										
CM-9. Security staff is encouraged to establish and cultivate ongoing relationships and contact with national cyber security infrastructure support organizations.										
CM-10. Table top and training exercises including all relevant stakeholders may be performed to identify weak areas and strengthen the incident response planning across organizations.										
5.6.2 During-Event Security Event Notification, Coping, and Coordination with Stakeholders										
Necessary Recommendations										
CM-11. As appropriate, governmental organizations are contacted for disclosure of event and to request assistance if required.										
CM-12. During a security event, information is shared with relevant stakeholders on situations within timely and predetermined window.										

IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
CM-13. If a security event is taking place or has just taken place, the appropriate security event plan is executed.										
CM-14. Coordination of stakeholders during a security event is executed as planned, but with flexibility to modify details of the plan.										
CM-15. Logging capture and accurately timestamp all actions by all stakeholders. Multiple logs from different organizations are able to be correlated with each other based on the timestamps.	CM-15a. Logging **Shall** capture and accurately timestamp all actions by all stakeholders. Multiple logs from different organizations **Shall** be able to be correlated with each other based on the timestamps.	**Yes**	**Shall**	**Shall**		**Shall**	All	All		
CM-16. Information on coping actions, expected results, and timing of actions is shared with all impacted stakeholders.										
Optional Recommendations										
CM-17. Security events are reported to critical infrastructure cybersecurity support organizations such as CISA, E-ISAC or the FBI.										
5.6.3 Post-Event Cross-Organization Review of Impact of Security Situation										
Necessary Recommendations										
CM-18. All stakeholders agree on placing a system back into service, all changes recorded, and where applicable connection to the grid reestablished.										
CM-19. Reporting after the security event provides (authorized) stakeholders with relevant information on what occurred, what actions were taken, who (role) took what action, and the results of these actions.										
CM-20. Reports are used to review and possibly update plans for similar security events.										
CM-21. A mechanism is available for stakeholders to discuss what they learned from the incident and what future mitigation steps might be appropriate in the context of an incident review, which might lead to revisions of security monitoring, processes, configurations, and technologies.										

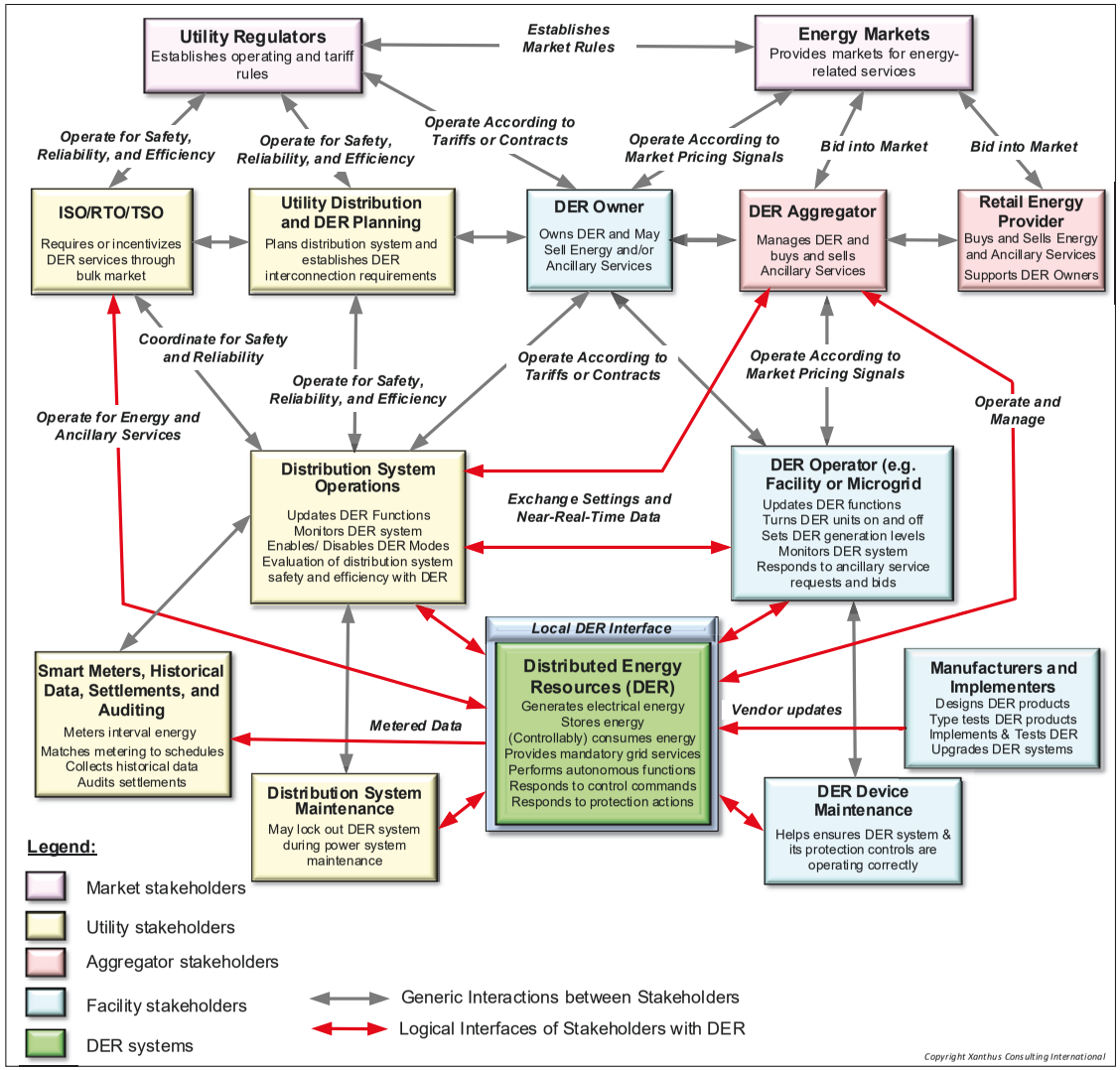
IEEE 1547.3 Section 5 Recommendations	Rewording and Qualifications of Shall Requirements. Also Phase 1 or Phase X for Should Recommendations	This IEEE 1547.3 recommendation SHALL be reworded to become a requirement	SunSpec/Frances Requirements Should, or Shall or N/A?	ASE Systems Prasanth Requirements Should or Shall	PG&E Abraham Jose Requirements Should or Shall	SCE Proposed Draft Recommendations	Equipment DER Unit, DER, PCS, Util Gateway, Agg Gateway, ChSt, EVs, Network devices	Size For Shall's, Applies to what Sizes? All, Small, Med, Large, Plant, Crit, Lg Agg?	Comments, Clarifications?	SCE Comments, Clarifications?
CM-22. An inventory of potentially compromised credentials is taken and these artifacts updated as soon as practical.										
CM-23. All stakeholders agree on closure of the incident investigation.										

Annex C Enlarged Versions of Some Diagrams

C.1 Cybersecurity Standards and Guidelines



C.2 DER Stakeholders



C.3 Utility DER Security Architecture