



THE **RELIABLE** WIRE



QUARTER 2, 2020 EDITION



THE RELIABLE WIRE NEWSLETTER



TABLE OF CONTENTS

A MESSAGE FROM THE CEO

There are some crucial conversations regarding systemic racial injustice occurring throughout the country this month, and hopefully for many months to come. While I am certainly doing more listening than talking these days, since I have the privilege to breathe freely, I want to put some of my breaths to work.

My first child was just born and, for the first few days of his life, he was having some trouble breathing—all my wife and I wanted was for him to be able to breathe normally. We had to endure this for three difficult days. I cannot imagine having to worry about our son being able to breathe freely out in this world for his entire life. I'm also privileged enough to confidently know that I will provide my son with an optimal environment to thrive and the opportunities necessary to succeed. I've always been a strong believer that we are all products of our environment but, more recently, started to realize that our environments still do not always provide equal opportunity.

Like many, my understanding and perspective on racism in America in 2020 is continually changing and being revised—the metrics and stories I have recently learned of have forced me to realize that many things are not right. I want to encourage everyone to challenge their belief system and ways of thinking. In the words of Jeff Bezos, “the smartest people are constantly revising their understanding, reconsidering a problem they thought they'd already solved.

While GridSME is certainly far from perfect, the guiding principles our company was founded upon are relevant for the tough and very important conversations regarding racial injustice occurring throughout the country this month, and hopefully for many months to come. While I am certainly doing more listening than talking these days, I feel that sharing these guiding principles may help others navigate these waters, so I want to do my part and add to the conversation.

GridSME's 3 Laws:

1. No jerks
2. Always add value
3. Win-win-win

#1 is everyone's favorite, especially since we say it differently within the halls of GridSME! It's also one of the most fundamental human moral laws. We require a workplace in which everyone is respected, heard, and treated fairly. We do not tolerate those who do not treat others as they wish to be treated. We apply this law to all employees, contractors, and even our clients. We will not tolerate violation of this law, and it has resulted in terminations of employees, as well as clients who were abusing our employees. However, simply not being a jerk isn't enough anymore, and we all (GridSME especially) need to do more to proactively create the positive change we want to see in the world.

#2 is to remind everyone at GridSME why we exist as a company, which is to improve our employees' lives and our clients' businesses. If, for some reason, we find ourselves in a position where we are not adding value to our clients or employees, we force ourselves to re-examine the situation and make the necessary changes to get back to a place of value. I encourage everyone to continually look in the proverbial mirror and check-in with ourselves to ensure we are always adding value, especially when discussing, listening, and learning about what is going on around us in America right now.

#3 is just our colloquial way of saying “each deal must be fair and equitable for all involved” (i.e. a win for the client, a win for GridSME as a company, and a win for the GridSME resources completing the work). I strongly believe that we need to do better as a collective country to provide equity in every aspect and walk of life.

Additionally, we operate as a meritocracy. We compensate, promote, and reward our employees based on merit, not based on age, tenure, or political/industry connections. There are good and bad people in every race, country, and community. Let's strive to reward those whose merit warrants it, regardless of any other attribute.

Last and certainly not least, we strive for open and candid communication—again, with both our employees and clients. We encourage having those tough conversations at GridSME—whether it's providing direct and constructive criticism on employee performance or telling a client a truth that may be tough to swallow. Of course, this is easier said than done. Even Warren Buffett admittedly struggles with this. In his words on having disciplinary conversations, “it's pure agony, and I usually postpone it and suck my thumb and do all kinds of other things before I finally carry it out.” But we all know that it is not beneficial to anyone involved to delay these tough conversations.

On that note, here's to having those tough conversations that will help advance our society and improve the lives of all the good people who deserve it. #BlackLivesMatter



John Franzino

John Franzino
Chief Executive Officer

NERC & FERC REGULATORY NEWS



Recent NERC News

- On June 2nd, 2020, NERC announced that its 2020 Summer Reliability Assessment ([link here](#)) found projected resources are at or above the levels needed to satisfy summer peak demand under anticipated weather in nearly all assessment areas.
- The Align Project released the Registered Entity Newsletter on 5/18/20, reviewing the key takeaways from the Let's Get Aligned meeting. The full Registered Entity Newsletter may be found ([here](#)). On 5/14/20, NERC also released the announcement, Board Holds Virtual Meeting; Approves Updated Align Timeline, SEL Strategy. The full post may be found ([here](#)) and more information about the Align webpage may be found ([here](#)).
- On May 14th, 2020, NERC released an article titled "Resource Developed to Help Organizations Update Pandemic Response Plans" ([full article here](#)). The plans discuss the Epidemic/Pandemic Response Plan Resource ([link here](#)).

Recent FERC News

- On June 18th, 2020, FERC issued a staff white paper on Cybersecurity Incentives Policies ([link here](#)). This paper follows the Commission stating that cybersecurity is an important part of reliability and indicated that it would address cybersecurity incentives independently in a separate, future proceeding. This staff white paper discusses a potential new framework for providing transmission incentives to utilities for cybersecurity investments.
- On June 3rd, 2020, FERC released a 2020 Energy Primer: A Handbook of Energy Market Basics ([link here](#)). This primer provides a high-level review of the markets in the US, how they're operated, and how entities interact with them.

Q&A WITH THE EXPERTS CYPRESS CREEK RENEWABLES SERC O&P AUDIT

WRITTEN BY CYPRESS CREEK RENEWABLES



Cypress Creek Renewables (CCR) recently passed an Operations & Planning (O&P) Reliability Standards audit conducted by SERC. GridSME sat down with CCR to discuss the experience, the results of the audit, lessons learned, and key takeaways. Here is the Q&A:

1. Can you provide a high-level summary of the audit?

We were first notified by SERC in July 2019 that Cypress Creek was on the audit schedule for 2020 with a proposed audit date in May 2020. The official audit engagement began when we received the Audit Notification Letter (ANL) in January 2020. The ANL identified the specific Reliability Standards and Requirements included in the scope, as well as data requests related to organizational information and internal controls. Our audit scope included Operations and Planning (O&P) standards specific to the Generator Operator (GOP) registration and was conducted remotely by SERC. There were five audit team members, including a Point of Contact (POC) and an Audit Team Lead. Audit documentation was delivered via the SERC portal and the audit team reviewed our compliance evidence in a timely fashion and were very communicative throughout the process. SERC issued just one follow-up data request and finished their review ahead of schedule with zero findings. Overall, the audit went smoothly and was a great learning experience for our entity as one of the first solar specific GOPs to be audited in the SERC region.

2. What was the audit process like? Was there anything that took Cypress Creek by surprise? Was the process clear?

The audit process was straightforward with deliverables, due dates, additional information requests, and responses communicated to us in a timely manner. We saw this process divided into 5 basic steps following Appendix 4C of the NERC Rules of Procedure:

First, Cypress Creek was notified by SERC of our inclusion in the 2020 annual audit plan in July 2019 and was requested to confirm the proposed dates.

Second, the Audit Notification Letter (ANL) was received about 4 months before the scheduled audit dates. Along with the ANL, there was also a Request for Information, and Certification Letter. The ANL identified the specific Reliability Standards and Requirements for evaluation and the regional entity's preferred formatting on the Reliability Standard Audit Worksheets (RSAWs). The Request for Information (RFI) included a questionnaire on the organization's internal control practices, and the Certification Letter requested general company information such as business organizational charts. The audit team scheduled an introductory call soon after delivery of the ANL to introduce themselves and to discuss the process.

Third, the requested audit material was provided to SERC within 30 days. This upload included the completed RSAWs, associated evidence files, and responses to the RFI and Certification Letter.

Fourth, the audit team reviewed the submitted information for compliance with the Reliability Standards. Following this review, SERC provided Cypress Creek with an audit update which included a preliminary determination status for the in-scope Reliability Standards. All standards had been assessed a status of "No Finding" except one, for which additional information was required and a corresponding data request was issued. Cypress Creek had approximately a week and a half to respond to the data request and upload additional evidence for their review of that Requirement. Cypress Creek received a second audit update in late March that confirmed all requirements were moved to a "No Finding" status.

Fifth, SERC conducted an exit presentation, provided the draft audit report for Cypress Creek's review, and delivered the final signed report to Cypress Creek. As communicated by the audit team during our opening presentation, if a potential non-compliance had been identified, the SERC audit team would have turned the proceedings over to the enforcement team following the exit presentation.

We were pleased with how communicative the auditors were and how the audit was concluded ahead of schedule. Our Exit Presentation was held the last week of March, almost 2 months before our originally scheduled audit date in May. Our audit was also largely uninterrupted by COVID-19 as the audit had already been determined as off site and the initial evidence gathering had already been completed prior to travel restrictions being implemented.

3. What would Cypress Creek recommend to entities prior to an audit to prepare?

We have a couple recommendations based on our experience and which worked well for us. (1) Conduct a mock audit. We recommend inclusion of all the applicable Reliability Standards to your registration and for your Subject Matter Experts to sit for mock interviews. This exercise is helpful to fine tune organization and presentation, RSAW narratives and citations, and most importantly, to confirm and obtain feedback on evidence. The objective is to prepare the RSAWs and evidence in advance as close to final form as possible. A mock audit will help confirm that your organization is ready for the audit or identify any areas of concern ahead of time. (2) Involve your management team early and often. Cypress Creek's senior leadership was very supportive and prioritized being present and available to the compliance team throughout the audit. For example, the senior leadership team was present on the Opening and Exit Presentations and asked questions to the audit team, demonstrating engagement. The Regional Entities may notice touchpoints like this since there is a section in the Audit Report about Compliance Culture. (3) Review your Regional Entity's audit resources. At Cypress Creek, we placed a priority on attending Open Forums and Compliance Seminars, and we were able to refer to internal notes and published recordings and presentations which helped us identify how the Regional Entity conducts their audits. This included identifying how SERC prefers evidence to be organized, including citation format and folder structure, which led to positive feedback from the audit team on our organization and presentation.

4. During the audit, what were Cypress Creek's interactions with the audit team like? How many of your team members interacted with SERC during the audit? Was the entire audit conducted remotely and did that introduce any unique challenges? What form of interaction and communication was most effective?

Our interactions with the audit team were positive and professional. The audit team members were responsive and, since the audit was designated as offsite from the initial notice, we went into the audit with a communication philosophy of "early and often" and did not face any unexpected challenges. While it is always a best practice to have designated Point of Contacts from each team, this was especially important for an off-site audit. Written communication was most effective and appropriate for correspondence related to material content while verbal conversations were most effective to establish a rapport with the auditors. For example, the introductory call and opening presentation were key opportunities for senior management to meet the auditors and demonstrate active engagement and for the compliance team to ask questions.

5. Did the audit result in any material changes to Cypress Creek’s compliance program, policies, or procedures going forward?

Since our audit results included no recommendations and no potential non-compliances, there were no material changes made to Cypress Creek’s compliance program. The results and audit experience confirmed that our program and focus areas for development align with NERC’s risk-based approach and encouraged Cypress Creek to continuously improve elements of our program, such as internal controls. We were pleased to hear that the auditors had positive feedback for an entity of our size regarding our program structure and about the material contents of our documentation.





RESPONDING TO THE EXECUTIVE ORDER ON SECURING THE UNITED STATES BULK-POWER SYSTEM

Written By John Franzino | CEO



Since the May 1st Executive Order, GridSME has received two common questions/concerns from our clients:

1. How will the Executive Order impact my operating assets and future projects?
2. What concerns and considerations should I have?

In this article, we will be taking a deeper dive into what the Executive Order includes and how entities within the power industry should respond.

Summary of the Executive Order

The Executive Order seeks to mitigate well known, and long-standing, cyber security supply chain risks. There is no doubt that cyber supply chain risk poses a real threat to the reliable operation of the U.S. bulk-power system (“grid”). After all, the industry has been talking about addressing this risk since 2016 when the Federal Energy Regulatory Commission (FERC) directed the North American Electric Reliability Corporation (NERC) to “develop a new supply chain risk management standard that addresses risks to information systems and related bulk electric system assets.” However, in the Executive Order’s defense, the NERC Critical Infrastructure Protection (CIP) standard that addresses cyber supply chain risks, CIP-013, does not go into effect until October 1, 2020, so there is definitely still a large, lingering risk that needs to be mitigated.

The Executive Order seeks to address cyber supply chain risks by establishing a joint task force, with members including the Secretary of Defense, Secretary of Homeland Security, and the Director of National Intelligence, that will work with the public and private sectors to restrict the acquisition or use of bulk-power system electric equipment designed, developed, manufactured, or supplied by foreign adversaries.



The BPS and the thousands of components necessary for it to function are integral to national security. With today's EO, the US is committed to eliminating the possibility any adversary or those beholden to them can pose undue risk to the indispensable services the BPS provides. [twitter.com/SecBrouillette...](https://twitter.com/SecBrouillette)

Dan Brouillette @SecBrouillette
Replying to @SecBrouillette

It is imperative our bulk-power system remains secure from exploitation and foreign threats. This Executive Order will lessen the ability of foreign adversaries to target our electrical grid.

6 10:59 AM - May 1, 2020



What's the scope of the EO?

During my first read through of the EO, I thought there was a major scope difference between it and the NERC CIP-013 Cyber Security Supply Chain Risk Management standard and was pleasantly surprised!

(h) Because attacks on the bulk-power system can originate through the distribution system, the Task Force shall engage with distribution system industry groups, to the extent consistent with law and national security. Within 180 days of receiving the recommendations pursuant to subsection (c)(i) of this section, the FAR Council shall consider proposing for notice and public comment an amendment to the applicable provisions in the Federal Acquisition Regulation to implement the recommendations provided pursuant to subsection (c)(i) of this section.

Sec. 4. Definitions. For purposes of this order, the following definitions shall apply:

(a) The term "bulk-power system" means (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. For the purpose of this order, this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

Section 3 (h) acknowledges the fact that distribution system poses a risk to the overall reliable operation of the grid. However, FERC and NERC have no jurisdiction over the distribution system and, as a result, CIP-013 (or any NERC Reliability Standard for that matter), is not applicable or enforceable on the distribution system.

Confusingly, Section 4 (a) goes on to define "bulk-power system," the primary basis of applicability for the EO, and explicitly excludes "facilities used in the local distribution of electric energy."

If this EO does not apply at the distribution level, there will only be incremental benefits above and beyond CIP-013. However, if this EO does in fact apply at the distribution system level, I see real potential value in this initiative--the traditional FERC-NERC construct leaves a major hole in security for the grid. As Joe Weiss points out in his blog, Control, "electrons, like the hackers don't have organization charts to follow or regulations to meet. Yet, the defenders have refused to address this obvious cyber security gap."

Another common question I received over the last few weeks was how to interpret the definition of "foreign adversary."

"I need to understand if we are using any equipment or software manufactured by a "foreign adversary" at my facilities"

For better or worse, your guess that this Executive Order is primarily directed at China is as good as mine. The U.S. has other foreign adversaries that have been known to conduct cyber attacks against our critical infrastructure, such as, Russia, Iran, and North Korea--however none of these countries produce large amounts of components used to operate and monitor the grid like China does. Also, it's no secret that the current Commander in Chief has a trade-war-bone-to-pick with China and this is arguably just another lever to pull.

Enough with political speculation and attribution. Playing that game is a waste of time, in my humble opinion.

Should I do anything?

Since the Executive Order is written in such an open-ended, vague, and even somewhat contradictory way, I recommend that taking this time to evaluation of your current cyber security posture.

In the coming months, the DOE will be performing an evaluation to identify what equipment will be prohibited under this executive order. Now, if equipment at your facility were to be declared prohibited during the DOE evaluation, that doesn't necessarily mean you need to replace it, as most installed prohibited items will be allowed to remain in the system with appropriate mitigation.

Should every asset owner and operator evaluate their supply chain risks?

Absolutely! However, that should not be the priority for your organization, unless you have already implemented and continuously monitor more foundational cyber security controls. My preferred framework for fundamental cyber security controls is the Center for Internet Security (CIS) Top 20 Critical Security Controls (CSC). This is a great starting point if you are unsure about the state of your cyber security posture.

You should note that supply chain risk management controls are NOT present in the CIS Top 20 CSC. This is not to say that supply chain risk management isn't extremely important for the reliable operation of the grid, just that there are many fundamental controls that should be implemented first and foremost.



CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.



→ CIS Controls V7 separates the controls into three distinct categories:

Basic:
Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational:
Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational:
These controls are more focused on people and processes involved in cybersecurity.

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

“Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process.”

Zurich Insurance Group
Blue Boxes: Overview by cyber risk?
Economic benefits and costs
of alternate cyber futures
Switzerland

Assuming you have already addressed all (or at least a good portion) of the CIS Top 20 CSC, then your focus should be turned to managing supply chain risks. For those that are responsible for CIP medium and high impact BES cyber systems, you hopefully have already developed a cyber security supply chain risk management program to meet the CIP-013 requirements. For those with only low impact or “no-impact” systems and do not know where to start, below are some good resources to get you started thinking about what a cyber supply chain risk management program might look like for your organization:

- North American Transmission Forum (NATF) CIP-013-1 Implementation Guidance
- Cyber Security Supply Chain Risk Management Plans Implementation Guidance for CIP-013-1
- NIST Best Practices in Cyber Supply Chain Risk Management
- DOE Cyber Security Procurement Language for Control Systems
- NERC FAQ Supply Chain – Small Group Advisory Sessions

While I would love to share two additional supply chain risk management resources, they are restricted NERC Alerts that cannot publicly be shared. The public can see a listing of all NERC Alerts, including the two that are focused on supply chain--one issued in October of 2017 and the other in July of 2019. If you are a registered entity, you have access to the details of these NERC Alerts (ask your resident NERC compliance expert if you do not already have access).



DO YOU WANT HELP?

Understanding & Managing Cyber Risk at Your Generator/Control Center?
OR
Developing & Implementing Your CIP-013 Program?

CONNECT WITH ONE OF OUR SUBJECT MATTER EXPERTS



SUBSTATION PHYSICAL SECURITY INITIATIVES

Written By Ernie Hayden MIPM CISSP CEH GICSP(Gold) PSP
Executive ICS Security Consultant



Have you ever been curious about what events lead to the increase of regulations towards increasing physical security protection of your electric substations? In this article we will take a dive into the events that lead to the standards and how those standards effect your substations.

In the electric energy industry, a predominant compliance driver has focused on cyber security of the bulk electric system controls. In 2013, the focus on cyber security compliance issues for electric utilities was augmented with some new physical security requirements. In this article, I'll introduce you to the events that led to the development of these new regulations and how you can development and implement your new physical security protocol that meets these new guidelines.

Metcalfe Substation Attack

The Executive Order seeks to mitigate well known, and long-standing, cyber security supply chain risks. There is no doubt that on the night of April 15, 2013, several very well-informed attackers caused physical damage to Pacific Gas & Electric's large 500 kv/230kv Metcalfe Transmission Substation located south of San Jose, California. Beginning at about 1:00 AM, the attackers cut two fiber communication lines. After they were finished, they resealed the telecom vaults and spread garbage in the area to help draw attention away from their actions.

At 1:31 AM the attackers began shooting at the substation transformers and circuit breakers. Ten of the 11 transformers were struck. It appeared that the attackers only shot at the "hot" transformers (one was down for maintenance). By 1:45 AM the transformers had begun to shut down, presumably, due to low cooling oil levels and low oil pressures.

The subsequent investigation after the shooting identified 116 impact points on 22 pieces of equipment and 52,000 gallons of transformer oil was spilled onto the base of the substation foundation. It was also determined during the investigation that the slow response time of the employees and inaccessibility of the substation allowed the perpetrator(s) enough time to get escape before the police arrived on scene.

TIMELINE OF THE EVENTS

1:00 AM	Attacker(s) cut two fiber communication lines
1:31 AM	Attacker(s) began to shoot transformers and circuit breakers
1:41 AM	911 called
1:48 - 1:50 AM	Investigators estimated the attacker(s) stopped shooting
1:51 AM	Police arrived on scene but couldn't enter substation due to the gates being locked.
3:25 AM	Utility electrician arrived on scene

Metcalfe Attack Regulatory Response

After the attack, there was a buzz within the electric energy and security industries, which was filled with conjecture as to the true motivation(s) behind the attack. The local transmission system operators were able to effectively bypass Metcalf, which resulted in no reported electricity outages in the surrounding area.

The “buzzing” reached a crescendo on March 7, 2014 when the Federal Energy Regulatory Commission (FERC) – the government entity regulating the interstate transmission of electricity, natural gas, and oil in the US – directed the North American Electric Reliability Corporation (NERC) to submit a proposed physical security reliability standard for electric transmission substations within 90 days.

The focus of this proposed standard was to “Identify and protect facilities that if rendered inoperable or damaged could result in widespread transmission grid instability, uncontrolled electric network separation, or cascading failure within a transmission inter-connection.”

Such a demand from FERC is not abnormal; however, their mandate for a rapid turnaround and production by NERC standards committees was unheard of. Everyone realized FERC was taking the Metcalf event seriously.

The response from NERC was the development of NERC Critical Infrastructure Protection (CIP) Standard 014, “Physical Security.” The final ballot closed on May 5, 2014 – passing at 85%. The NERC Board of Trustees adopted CIP-014 on May 13, 2014. FERC approved this new standard on July 17, 2014 resulting in an effective implementation date of October 1, 2015.

This may seem slow; however, in the regulatory environments of FERC and NERC this was “SUPERFAST!”

CIP-014, Substation Physical Security Standard

The CIP-014 requirements are summarized in the table shown below but the you can view the full CIP-014 standards by visiting NERC.com or by ([clicking here](#)).

REQUIREMENT	GOAL
R1	Initial Risk Assessment – Critical Facility Identification
R2	Independent Review of Initial Risk Assessment (R1)
R3	Coordination Between Grid Operator (e.g., ISO) and Owner/Utility
R4	Threat and Vulnerability Assessment
R5	Development and Implementation of Physical Security Plan for Critical Substations
R6	Qualified Third-Party Assessment of Plans Developed in R4 and R5

Since the initial introduction of CIP-014, all North American electric utilities have implemented plans to address the requirements specified within the legislation and most have been audited to ensure the effectiveness of their plans.

California Doesn’t Want to Be Left Behind

While FERC and NERC were busy developing new physical security standards for large electric transmission substations, California lawmakers also showed their concern regarding the Metcalf attack by passing new legislation in June 2015 called Senate Bill 699 (aka, SB-699).

The new legislation addressed two major areas when it effective on January 1, 2016:

- Directed the California Public Utilities Commission (CPUC) to explore policies and practices related to physical security of electric distribution assets (not transmission – that is FERC/NERC’s jurisdiction!)
- Directed the CPUC to consider adoption of new standards and rules to address any physical security risk to the distribution system of California’s electric corporations so as to ensure “high-quality, safe, and reliable service.”

SB-699 Development

The actual legislation included in SB-699 is not very detailed. The document is only a few paragraphs long. So, to develop the detailed response to SB-699, the CPUC held three workshops to gather information from the affected California utilities and get a sense of the necessary parameters to include in the actual rules.

The first workshop was held on May 2, 2017 and was focused on information sharing, sensitive data protection, and confidentiality of critical energy infrastructure information. The workshop also established proceeding rules of engagement for input and testimony on sensitive subjects.

The second workshop was held on May 31, 2017 where the discussions were about state, federal, and industry standards and responses including CIP-014.

On June 21, 2017, the final workshop was held to address how SB-699 informs CPUC response and responsibilities. The meeting also included discussions on threat assessment, critical substation protections, and incident response resiliency.

Of note, on July 12, 2017, as part of the SB-699 response development process, an administrative law judge issued a ruling requesting straw proposals from the stakeholders on what the SB-699 rules should include.

January 2018 – CPUC Staff White Paper

After digesting the workshop notes and straw proposals the CPUC issued a very informative white paper entitled Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB-699. The primary topics in the paper included:

- Electric utility physical security in the Post-Metcalf era
- Distribution asset security and resiliency in California
- Incident reporting and tracking best practices
- Exchange of and access to highly confidential and sensitive information
- Utility general rate cases informing physical security efforts, and
- Recommendations

This white paper gives you an excellent sense of the State of California electric distribution grid and the challenges with keeping the critical infrastructure information secured from general knowledge – especially from the terrorists and threat actors.

January 22, 2019 – Physical Security Decision

Almost a year after the CPUC white paper was issued – the CPUC approved the “Physical Security Decision (D.19-01-018).” This made California the first U.S. state to adopt rules to guard the electric distribution grid against terrorist attack.

The decision established general criteria for the identification phase and criteria for the assessment phase, which clearly defined what parameters are used when deciding what distribution substations should be tagged as critical, and what are the rules that should be followed for the physical security assessments of the identified subs.

Identification Criteria

The general rules in the Physical Security Decision for identifying and declaring which distribution substations are critical include those that:

- Are needed for crank path, black start, restoration of the regional grid
- Are an electric power source for a military installation
- Serve a regional water and wastewater facilities
- Serve a regional public safety (e.g., 911 center)
- Serve a major transportation facility (e.g., Los Angeles International Airport)
- Serve a Level 1 Trauma Center
- Serve > 60,000 electric meters

Assessment Phase Criteria

Once the more critical distribution substations are identified – as noted above – the assessment phase will look at such issues as:

- Existing system resiliency and/or redundancy solutions
- Spare assets to restore a particular load
- Existing physical security protections
- Potential for emergency responders to identify and respond to an attack in a timely manner
- Location/proximity to gas pipelines, geographical challenges, impacts of weather, etc...
- History of criminal activity affecting the substation

Cost Recovery

The decision does allow for the investor-owned utilities to file separate applications for cost recovery associated with their respective distribution security programs. Although the Distribution Security Program documents are considered security-sensitive and cannot be publicly released, the investor-owned utilities may file a public version of the unaffiliated third-party review and CPUC approval in their cost recovery requests.


Security Decision Timeline

According to the Security Decision, each utility's Security Plan Report is due to the CPUC within 30 months of the approval of the Decision (estimated to be July 2020). The third-party reviews should be completed by April 2021.

Conclusion

The events of the Metcalf substation shooting were profound and a bit rattling to the electric energy utilities and regulators. CIP-014 came out of the event thus affecting most major North American electric transmission utilities. Now California Senate Bill 699 and the derivative Security Decision of January 2019 has been issued thus affecting most electric utilities in California. These two events show a trend towards increased physical security protection of electric substations.

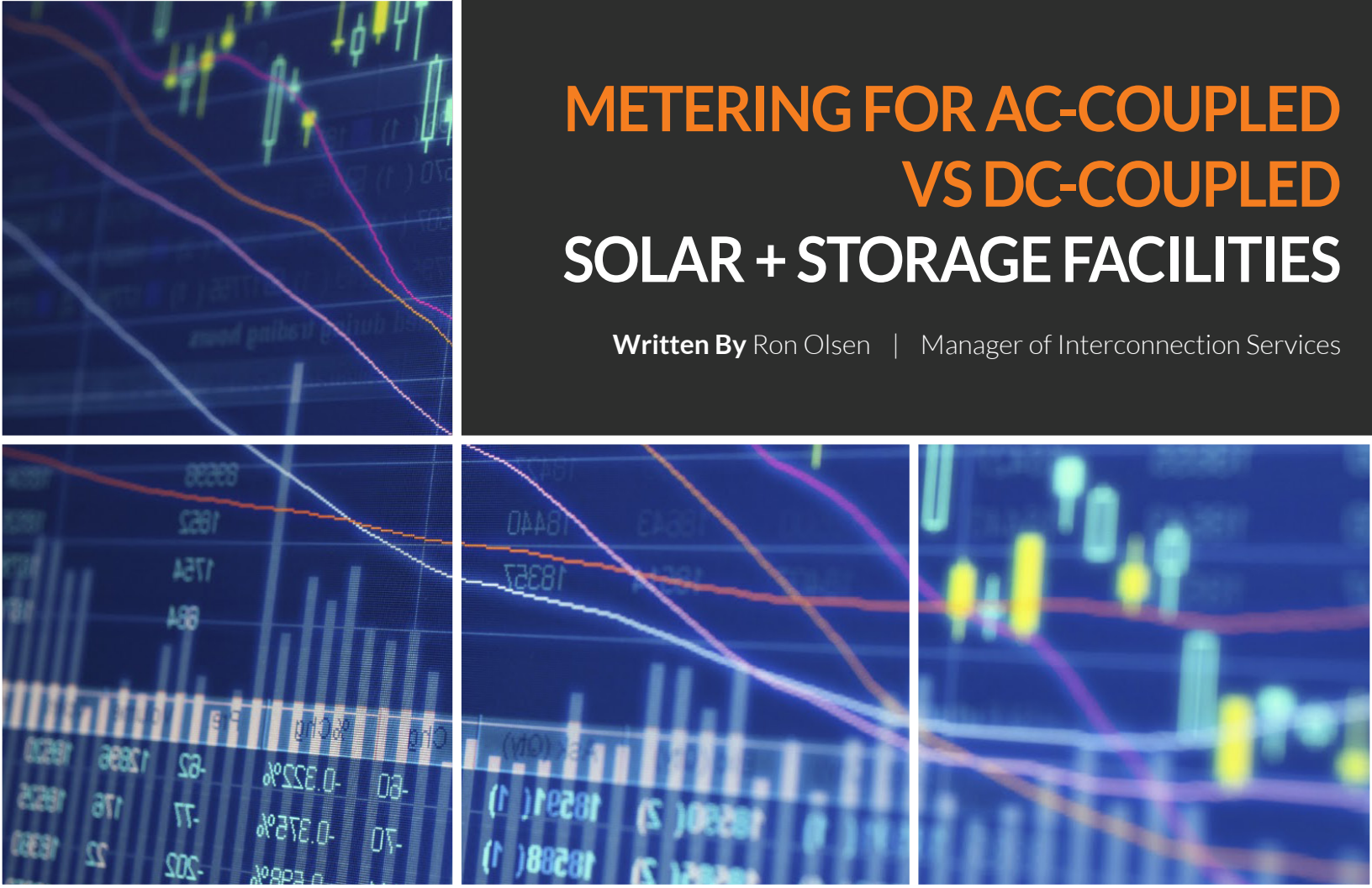
DO YOU NEED HELP WITH YOUR PHYSICAL & CYBER SECURITY?



GridSME has a team of experts that can help you build a secure physical and digital operation.

Contact Us at

Customerservice@gridsme.com
or +1 (916) 800-4545



METERING FOR AC-COUPLED VS DC-COUPLED SOLAR + STORAGE FACILITIES

Written By Ron Olsen | Manager of Interconnection Services

Introduction

As the grid evolves, there is an increasing need and motivation for existing renewable resources (e.g., solar PV) to add storage behind the same point of interconnection. With the coupling of storage to generators come many new challenges, including various challenges to coupling a storage resource on the direct current (DC) side of a renewable resource (i.e., behind the inverters). Now the hard part, how to do that within the rules and protocols of an ISO market, such as CAISO, and is it possible to separate the storage resource from the generation resource even if they are physically intertwined?

This article compares two different metering options for a solar+storage facility:

1. AC-coupled Storage with AC Low-Side Feeder Metering: AC low-side metering on the low-side of the step-up transformer placed on separated fuel type (e.g., one for PV and one for storage) feeders thus creating two resource ID's; and
2. DC-coupled Storage with AC High-Side and Low-Side Metering: AC high-side and low-side AC metering and DC-side metering where the storage is coupled with the solar feeder. This allows for two resource ID's and two fuel types even though the storage is on the DC-side.

In April 2017, the CAISO put into place metering enhancement rules within the CAISO Metering Business Practice Manual (BPM) applicable within its Balancing Authority area (BAA). These rules set the stage for metering solar+storage facilities in a way that gives the resource owner and off-taker maximum flexibility.

The metering enhancement rules and Metering BPM give entities inside of the CAISO control area the option to use a Scheduling Coordinator Meter Entity (SCME) to submit settlement quality meter data (SQMD) into the CAISO settlement system. This change to the Metering BPM allows an entity to calculate or extract 5-minute settlement meter data without a CAISO-approved meter by collecting settlement quality data from an approved and accurate device either on the DC-side or AC (alternating current) side of the solar+storage facility.

The CAISO metering enhancement rules are designed to allow SQMD energy submissions into the ISO Market Result Interface Settlement (MRI-S) system directly without an ISO-poled meter. To do this, an entity will need to comply with the CAISO AC-side metering accuracy as directed by the CAISO Metering BPM. The same CAISO metering accuracy, if applied to other interconnection facility hardware (e.g., an inverter), can be used to collect data that can derive 5-minute settlement interval data. The SQMD 5-minute intervals will be submitted into MRI-S system by the selected Scheduling Coordinator.

AC-coupled Storage with AC Low-Side Feeder Metering

Concept: The AC low-side metering is the most common metering settlement concept when a solar+storage facility must have multiple CAISO resource identifiers (“resource ID’s”) for purposes of separately accounting for the solar and storage resources and allowing for two different fuel types (i.e., solar PV and non-generator resource), perhaps because there exist multiple power purchase agreements (PPAs), there is a need for the solar resource to be considered an Eligible Intermittent Resource (EIR), to account for renewable energy credits (RECs), or for the storage resource to provide ancillary services.

Interconnection Planning Model: AC-coupling storage to a solar PV facility uses a separate feeder for each storage layout without changing the interconnection engineering study and planning design of the solar facility. The CAISO production system will model each resource ID as its own fuel type (e.g., solar and storage separate and distinct). In addition, the two resource ID’s will be treated independently in CAISO’s EMS and market models. CAISO will not view the two resource ID’s as a co-located or hybrid resource.

Interconnection Planning Model Considerations: If the solar PV facility was not studied as a co-located fuel type (i.e., solar+storage), then adding storage will require the interconnection agreement to go through the material modification assessment (MMA) process.

Revenue Settlements: Storage and renewable resources electrically connected but on separate feeders on the AC low-side of the step-up transformer can be complex if the entity owner selects polled CAISO metering for the different resource ID fuel types. In order to not violate the CPUC’s Eligible Intermittent Resource (EIR) ruling, these two fuel types must be kept separate (i.e., each have their own resource IDs). To achieve this low-side AC metering on each feeder, or collection of busses under a feeder, a resource must have a CAISO-approved meter. Then each resource ID’s meter, or group of meters, are associated with a single fuel type resource ID. CAISO can aggregate the same fuel type resource meters (e.g., multiple solar PV meters associated with the same fuel type).

DC-coupled Storage with AC High-Side and Low-Side Metering:

Concept: AC high-side metering with a DC-coupled storage resource on the same DC collection bus as the renewable resource and distributed across one or multiple inverters.

Interconnection Planning Model: DC-coupling storage to a renewable resource uses the DC buses and feeders’ electrical connection infrastructure to couple the storage resource without changing the interconnection engineering, study, and planning design of the generator interconnection facility. There may be a need to study the short circuit capabilities when adding storage to a solar DC bus to ensure the inverter can handle the bidirectional power flow, it takes less time for this type of restudy than AC coupled storage.

Revenue Settlements: The storage and the solar resources must be settled separately using an SQMD plan for each resource ID fuel type (e.g., storage and solar separate). The SQMD must be submitted by a SCME. The data in the SCME submission is derived from:

- A. single high-side revenue quality metering,
- B. low-side revenue quality metering, and
- C. DC metering of the solar and storage output.

With this setup, the DC metering will interface with the low-side AC metering to logically separate the solar and storage production, thereby allowing for the solar resource to appear as its own resource and therefore qualify as an EIR.

Summary

As the saying goes, “the devil is in the details.” There are, of course, a number of complexities here but the important takeaway is to know, no matter the site’s physical configuration (i.e., DC or AC-coupled storage), it is possible to separate your solar resource from your storage resource in the CAISO market. It is just a matter of identifying and implementing the right metering solution within the CAISO rules. If you have any thoughts or questions on this topic, feel free to give us a call or send an email. We’d love to chat.

Interested in learning more

GridSME will be co-hosting a webinar on Operating Hybrid Resources in CAISO on July 15th at 10:30am PT. Join Customized Energy Solutions (CES), Buchalter, and us for an in-depth discussion on metering, telemetry, market participation, and ITC considerations for solar+storage resources operating in CAISO.

RECENT CPUC NEWS

RESOURCES ADEQUACY AND SOLAR + STORAGE

WRITTEN BY TOM WATSON | PRINCIPAL CONSULTANT

One topic of particular interest in the PV and solar+storage community is California's Resource Adequacy (RA) program. As described by the CPUC ("the Commission"), the RA program has two goals:

1. To ensure the safe and reliable operation of the grid in real-time providing sufficient resources to the California Independent System Operator (CAISO) when and where needed.
2. To incentivize the siting and construction of new resources needed for future grid reliability.

As the program continues to evolve, new challenges emerge, such as how to best integrate the newest generation (pun intended) of renewable facilities. The inherent daily and seasonal variability in solar production introduces some interesting factors in the context of RA, and the Net Qualifying Capacity (NQC) value calculations applied to solar and co-located solar+storage resources is a hot topic of late. Co-located solar+storage projects often seek to maximize Investment Tax Credit incentives, commonly known as the "ITC." Capturing this credit requires a solar+storage facility to source its storage charge energy from the on-site solar generation.

Depending on the sizing difference between solar and storage components at a given facility, limitations on available solar energy can impact storage NQC calculations. In its RA Oversight/Enhancements proceeding, the CPUC previously adopted an interim methodology to calculate NQC for ITC-constrained storage, based on the solar generation capacity reduced by an Effective Load Carrying Capacity (ELCC) factor. The ELCC values vary monthly, with non-summer factors as low as zero.

The Commission's May 22nd Proposed Decision (PD) in the RA proceeding defines a new solar+storage resource (whether one resource ID or two) NQC calculation methodology. It includes a daily solar energy profile, reflecting charge capability until two hours before the net load peak, in addition to an ELCC-adjusted estimate for remaining renewable capacity beyond what is required to charge the battery. The daily profiles are to be developed by the CPUC's Energy Division. The PD also authorizes the Energy Division to "further explore a marginal ELCC approach for consideration in this proceeding."

Among other things, the PD also aligns the CPUC's definitions of "co-located" and "hybrid" resources with the CAISO's existing definitions. This small but critical change will help eliminate potential confusion when referring to the different types of facilities.

The PD could be voted on by the full Commission as early as June 25th. For more information, see <https://www.cpuc.ca.gov/ra/>

AN INTRODUCTION TO ADMS & DERMS

WRITTEN BY ERIC WHITLEY | GRIDSME CO-FOUNDER, CHAIRMAN

There is a growing interest among utilities and industry stakeholders in modernizing the distribution systems beyond the automation efforts of metering infrastructure field switches. This has led to an increase in procurement of vendor-supplied Advanced Distribution Management System (ADMS) by a growing list of load-serving entities. ADMS solutions integrate SCADA, Outage Management (OMS), and Distribution Management (DMS) functionality in a common database and user interface.

What is interesting is the “A” in the ADMS product solutions. This “advanced” denotation refers to the ability to perform power load flows, contingency analysis, and outage management on top of the normal DMS functions. Regardless of vendor claims, this is a considerable challenge due to the distribution modeling and field SCADA necessary to allow these transmission-type applications to be accurate and useful. This is a daunting task for many utilities that have not had a need to provide all the data relationships that a detailed network model requires.

Along with ADMS, some utilities are integrating newer functionality called Distributed Energy Resource Management Systems (DERMS). DERMS support such functionality as: Volt-VAR control, Dynamic Network Topology, DER Load Forecasts, DER situational awareness, DER susceptibility, network constraint management using DERs, energy arbitrage, and DER fleet management. The market is still deciding if DERMS will be independent systems, integrated with an ADMS, or an extra application



Microgrid



Wind



Solar



Storage



EV
charging



Load
control



Smart
buildings

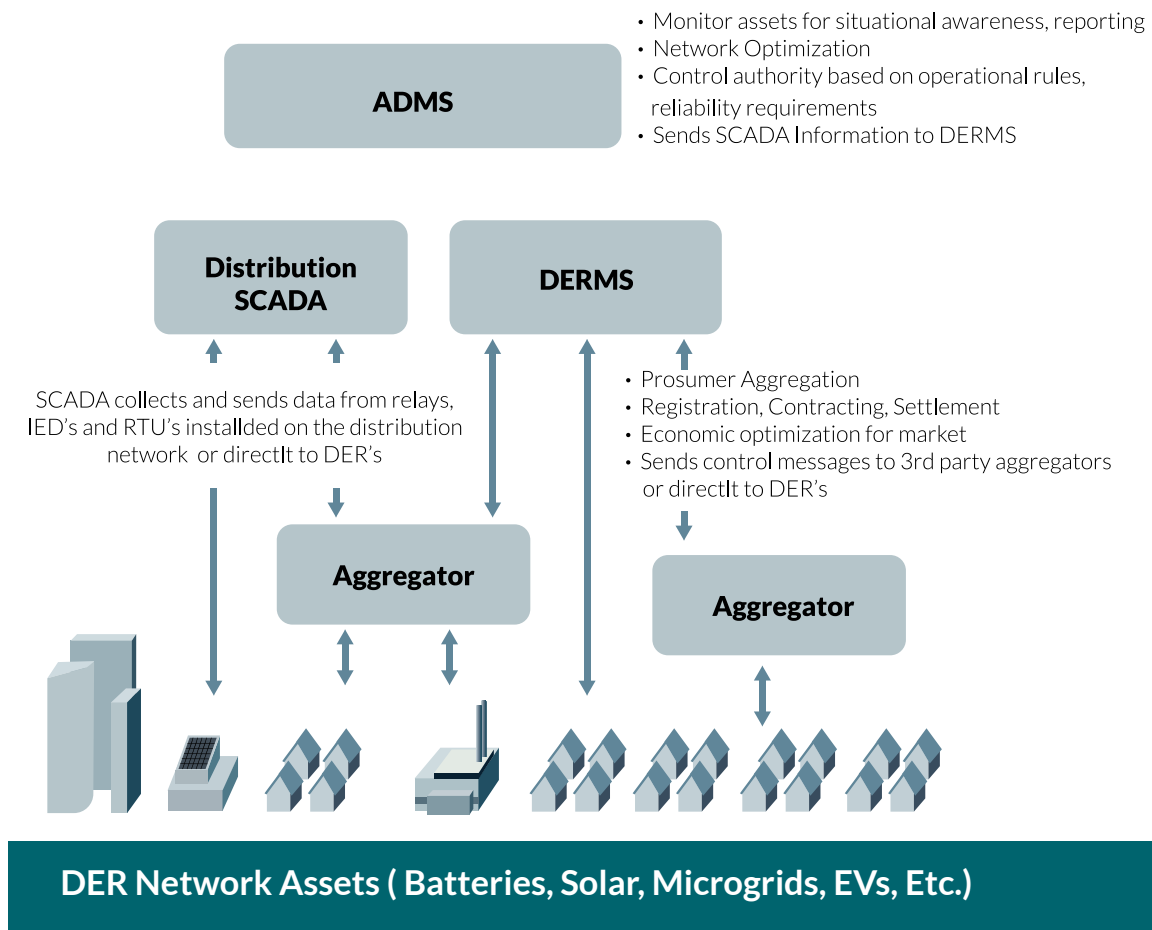


Prosumers

within the “advanced” part of an ADMS. However, to be useful, DERMS requires much more data than just a power flow model to equitably dispatch distributed generation and charging resources. To be accurate, each generation and storage resource must be modeled along with the controls implemented for those resources that are or need to be dispatchable. Some DERMS systems support modeling of Demand Response (DR) contracts, and integration with Demand Response (DR) applications for data and possibly controls, increasing Distribution system operators’ situational awareness of utility-initiated impacts to the grid – optimizing the use of DR and Distributed Energy Resource (DER) to relieve constraints on the grid. A very advanced technology being incorporated into combination ADMS/DERMS systems is an integration of energy arbitrage with reliability optimization, which ensures grid reliability while maximizing the economics of DER management (minimize Green House Gas and cost, interfacing with spot and forward market prices where available).

Several vendors are offering new approaches to DERMS that piece together the technologies required to give intelligence to a DERMS solution. These new approaches represent flexibility whereas most DMS, let alone ADMS, vendor solutions are pretty much SCADA systems with bolt on applications. This is a new arena in which some non-ADMS vendors are participating, such as OSIsoft (solutions such as PXISE and DERNetSoft, with partners) and mPrest. For example, if a utility utilizes OSIsoft PI, the data collection and analytical tools for the solutions based on PI come out of the box and the solutions take advantage of that to bring in distribution specific analytics and tools. There are many details in all of this, but it is a chance to actually implement a DERMS solution that can grow and adapt as the utility’s knowledge, needs, and grid complexity expands.

Safe to say, distribution’s time in the sun is now here (literally) and the amount of changes heading its way are enormous on two fronts: distributed generation and dispatchable storage (think EVs, too). Not having a coordinated and manageable set of tools to handle both these areas will be unfortunate for utilities struggling to deal with more and more distribution demands.



UPCOMING EVENTS

Due to COVID-19, these events are subject to change. Check host website to confirm.

JUNE

June 23, 2020

FERC Increasing Real-Time and Day-Ahead Market Efficiency and Enhancing Resilience Through Improved Software Technical Conference
([Webinar Registration Here](#))

June 25, 2020

Texas RE NERC Standards Review Forum
([Webinar Registration Here](#))

June 26, 2020

MRO Third Party Vendor Cyber Process Webinar
([Webinar Information Here](#))

JULY

July 1, 2020

SRCA - Supply Chain Risk Management Webinar
([Webinar Registration Here](#))

July 8-9, 2020

FERC COVID Impacts to Energy Industry Conference
([Conference Information Here](#))

July 21, 2020

CES, GridSME & Buchalter Co-host Webinar - Operating Hybrid Resources in CAISO
([information Coming Soon](#))

July 20, 2020

RF Reliability and Compliance Open Forum
([Conference Information Here](#))

July 23, 2020

FERC Technical Conference regarding Hybrid Resources
([Conference Information Here](#))

July 27, 2020

SERC Q3 2020 Open Forum
([Conference Information Here](#))

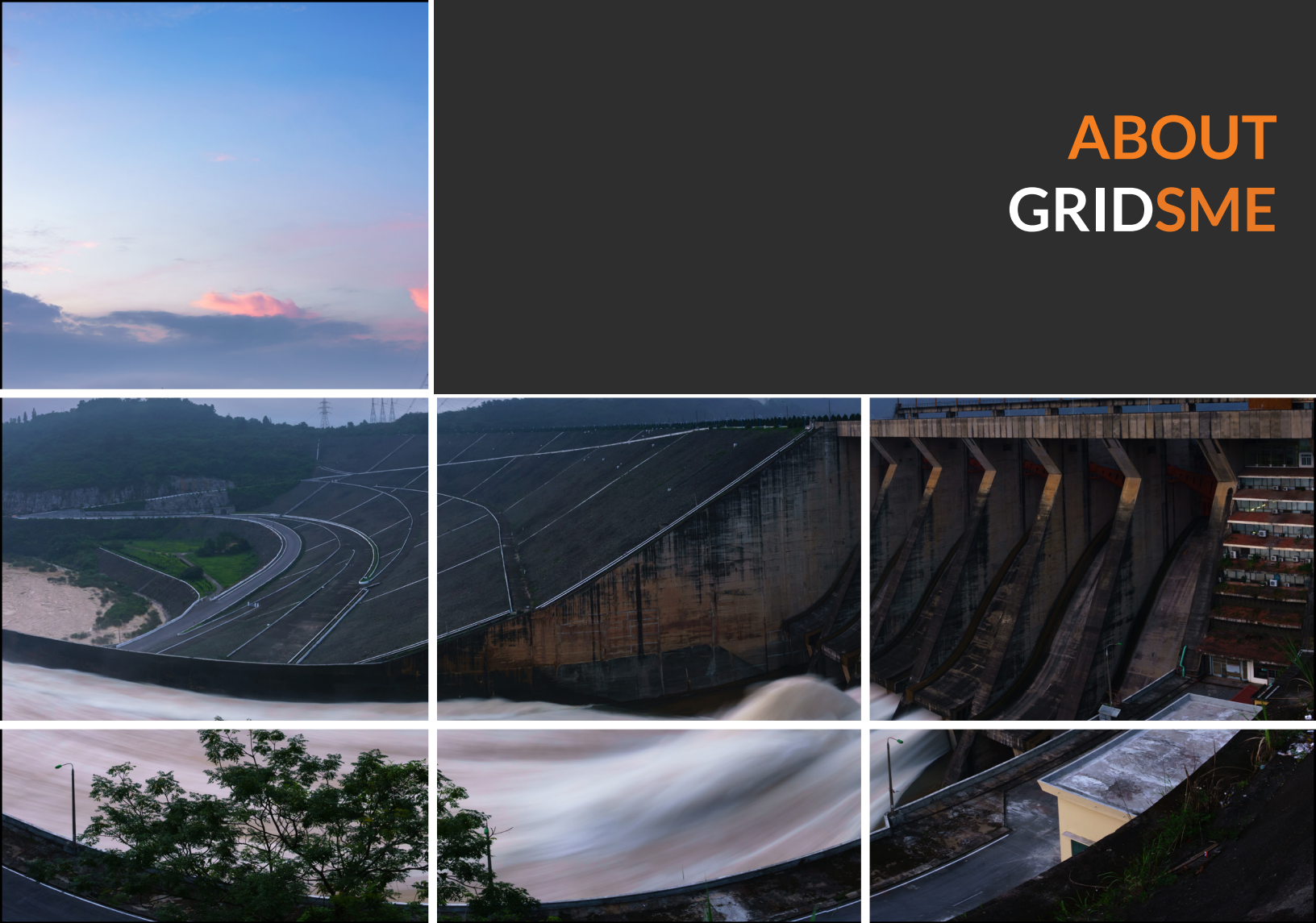
July 30, 2020

Texas RE NERC Standards Review Forum
([Webinar Registration Here](#))

UPCOMING EFFECTIVE DATES

Reliability Standard	Title	Effective Date
CIP-005-6	Cyber Security - Electronic Security Perimeter(s)	July 1, 2020
CIP-010-3	Cyber Security - Configuration Change Management	July 1, 2020
CIP-013-1	Cyber Security - Supply Chain Risk Management	July 1, 2020
PER-006-1	Specific Training for Personnel	October 1, 2020
PRC-027-1	Coordination of Protection Systems for Performing During Faults	October 1, 2020
CIP-008-6	Cyber Security – Incident Reporting and Response Planning	January 1, 2021
TPL-007-4	Transmission System Planned Performance for Geomagnetic Disturbance Events	January 1, 2021
PRC-027-1	Coordination of Protection Systems for Performing During Faults	October 1, 2020

ABOUT GRIDSME



GridSME is a results-focused consulting firm, representing a diverse group of talented electric industry experts ready to help guide our clients through the fast-changing landscape of the industry.

Our clients make up a very diverse group, ranging from small renewable energy companies to large regional utilities and everything in-between—our subject matter experts (SME) provide pragmatic solutions on a wide range of operational, technical, and business challenges, leveraging industry best-practice knowledge gleaned over the many decades of collective experience amassed by our team. While GridSME's core competencies lie in NERC compliance, cybersecurity, electrical engineering, and grid technology, we provide a number of additional grid support services to our clients, such as electricity market expertise, operations training, and IT services.

EXPLORE MORE WAYS THAT WE CAN HELP YOU
POWER YOUR WORLD WITH CONFIDENCE



GRIDSECURITY

We offer a wide range of state-of-the-art cyber security solutions for your company's server or power grid.



ENGINEERING & INTERCONNECTION

Our Engineering & Interconnection team is staffed by registered P.E.'s with experience in transmission planning, operations engineering, and power/control systems design.



NERC & REGULATORY COMPLIANCE

We assist all types of registered entities with both the Operations and Planning standards, as well as the Critical Infrastructure Protection (CIP) standards.



POWER SYSTEMS SERVICES

We have experience and expertise as project managers, technical leads, engineers, architects, and more.



REQUEST ADDITIONAL INFORMATION
WWW.GRIDSME.COM | (916) 800-4545