RADIAN GENERATION

TEXAS RE

Supply Chain Series: Renewables

Kellie Macpherson
Executive Vice President of Compliance & Security

Radian Generation

September 19, 2024

Antitrust Admonition

Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Upcoming Texas RE Events

October 2, 2024

Winter Weatherization Workshop

October 9, 2024

Electric and Oil & Natural Gas Coordination

October 16, 2024

Understanding New Generator Obligations

Upcoming ERO Enterprise Events

September 25, 2024

E-ISAC Physical Security Workshop

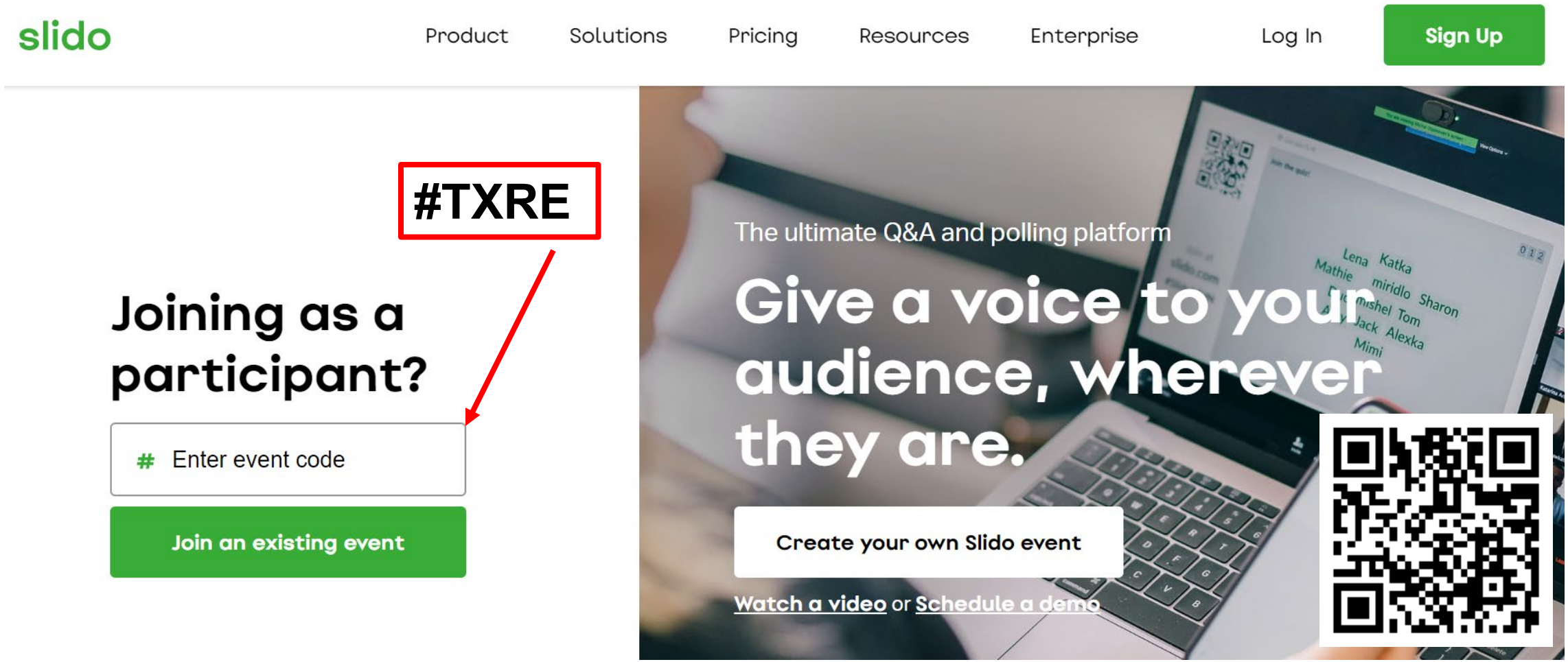
October 15-17, 2024

System Operator Conference

October 22-25, 2024

GridSecCon

Slido.com


slido
Product
Solutions
Pricing
Resources
Enterprise
Log In
Sign Up
#TXRE
Joining as a participant?
Enter event code
Join an existing event
The ultimate Q&A and polling platform
Give a voice to your audience, wherever they are.
Create your own Slido event
Watch a video or Schedule a demo

RADIAN GENERATION

Talk with Texas RE: Supply Chain & Renewables

Ensuring Reliability through Supply Chain Awareness

Kellie Macpherson | Executive Vice President, Compliance + Security

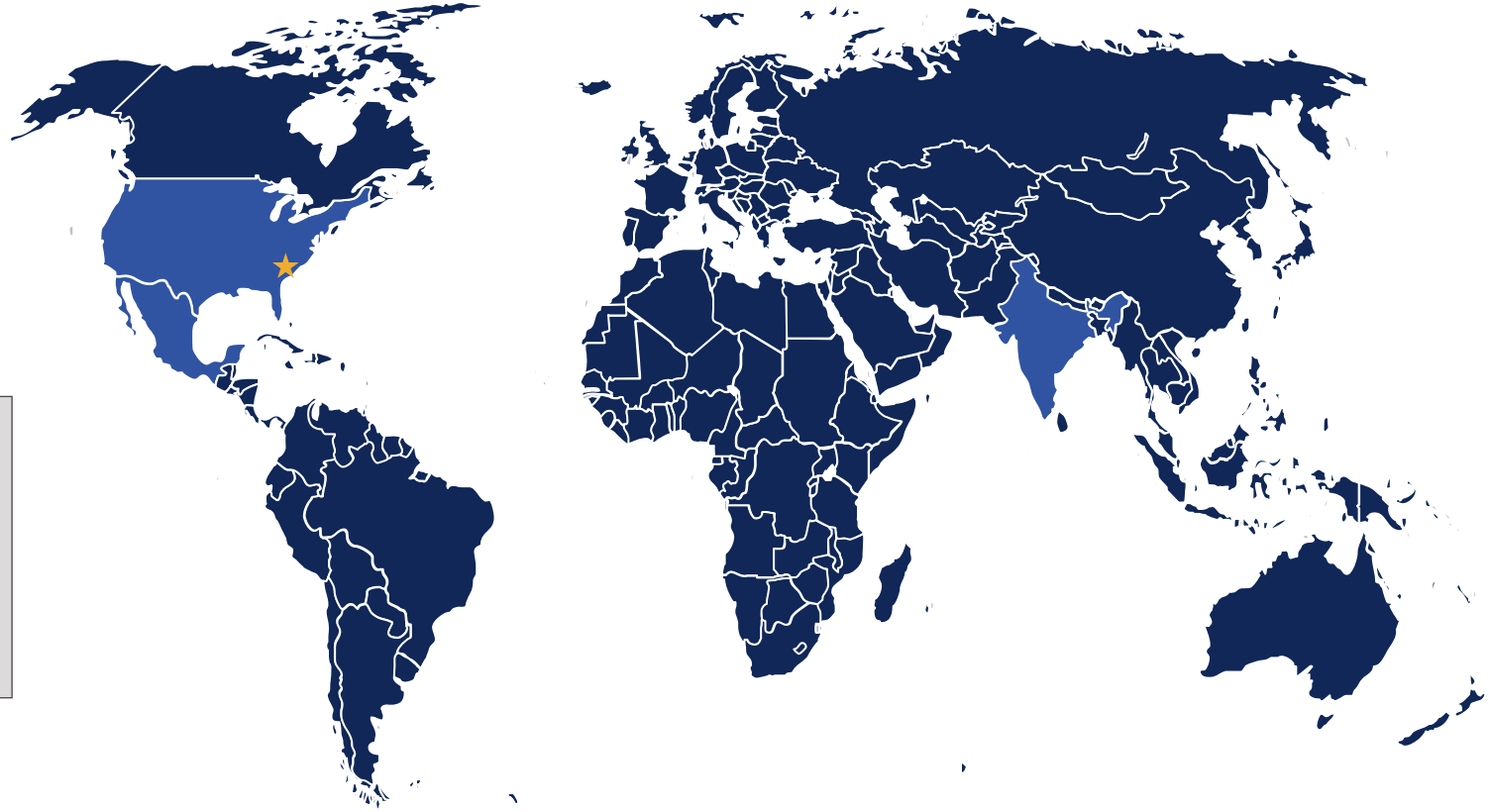
Radian Generation By The Numbers

16+ GW	28 +GW	21+ GW	21+ GW	89+ GW
ASSET MANAGEMENT SERVICES	CYBERSECURITY & OT SERVICES	NERC COMPLIANCE SERVICES	OPERATIONAL SOFTWARE CUSTOMERS	DEVELOPMENT SOFTWARE CUSTOMERS

1 GW Solar Generation:
Provides 1.5B kWh Annual Electricity
Powers 126,000 Homes Yearly

Displacing CO_2 Emissions From:
1.5M Barrels of Oil
726M Pounds of Coal

We are supporting 10X+



Founded in 2013

Headquartered in Charlotte, NC

US, Mexico & India Offices

1,200+ Project Managed (Utility & Commercial)

100+ Clients in 7 Countries (Solar, Wind, Storage)

RADIAN GENERATION

Introduction to Radian Generation

- What We Do
  - Radian Generation is a global provider of critical technology-forward services designed specifically to support the comprehensive lifecycle of renewable facilities—including solar, wind, and energy storage
- Who We Serve
  - Radian Generation's wide range of commercial, technical and compliance services provide developers, owners, and operators with critical insights into each aspect of their assets to make better-informed decisions
- Compliance + Security
  - **6 of 6 Electric Reliability Regions**
  - WECC, TRE, SERC, RF, MRO, NPCC
  - **Canadian Regions** - Alberta, British Columbia, Ontario, Quebec
  - **300+ PROJECTS** - Day to Day Compliance Obligations (POC)
  - **CLIENTS**
    - SOLAR, WIND, & STORAGE (178)
    - UTILITY & CONVENTIAL (20)
    - CONTROL CENTERS (13) (6 CIP Medium)
  - **Functional Registrations**
  - GO, GOP
  - TO, TOP, TP
  - BA, RP
  - DP, UFLS

History of Supply Chain Efforts

- Initial Focus on Reliability
- Rise of Renewable Generation (2000s)
- Cybersecurity and Supply Chain Standards (2014)
- FERC Order 829 (2016)
- Project 2016-03 (2016)
- Project 2019-03 (2019)
- Continued Evolution and Grid Transformation (2020s)
- Project 2020-03

- Industry Adjacent Work
  - CFIUS
  - Texas – Lone Star Infrastructure Protection Act

Vendor Remote Access

- Remote access by vendors is a particular security risk for the renewable industry
- This risk is the basis for several NERC requirements:
  - CIP-005 R2.4 and 2.5 is applicable to systems deemed CIP medium or high impact
  - CIP-003-9 for systems deemed CIP low impact, will go into effect on 4/1/2026
    - Note: Will require significant changes to business practices by many renewable operators
- Best Practices for Renewable Assets:
  - Ensure procurement is done with trusted and known vendors
  - During construction, ensure that vendors and OEMs are required to follow best cyber security practices
  - Prior to COD, ensure that all extraneous access is disable; only those with a true business need should keep access
  - Ensure that ongoing maintenance by OEMs is done with best cyber security practices in mind
  - Common to see OEMs creating backdoor connections, making changes to security settings, general disregard for cyber security

Vulnerabilities and Malicious Code

- Hardware, software and operating systems need to be maintained regularly to prevent the use of unmitigated vulnerabilities or malicious code for a cyber-attack
- Entities need to have established methods in place with its vendors to receive security patches and updates in a timely manner.
- While much of the NERC requirements regarding this risk only apply to systems deemed CIP medium or high impact, it is a commonsense security best practice to also apply these to your low impact systems
- Here are some of the requirements that apply to medium and high impact – and should be considered for low impact systems:
  - Ports & Services: (CIP-007 R1)
  - Security Patch Management (CIP-007 R2)
  - TCA and Removable Media (CIP-010 R4)
  - Vulnerability Assessment (CIP-010 R3)
- Best Practices for Renewable Assets
  - Train Field Staff to be your first line of defense
  - Train control center staff to trust but verify
  - Implement clear change management program with inverter and SCADA OEMs post COD

Supply Chain Risk Management

- Currently, applies to systems deemed medium or high impact
- Cyber Security Risk Assessment
  - Entities must conduct a cyber security risk assessment prior to procuring hardware, software or services
- Entities must address specific cyber security risks during the procurement process
  - Notification from the vendor of incidents related to the product or service that post a cyber security risk to the entity
  - Coordination of response to the vendor's notification of incidents
  - Notification when remote or onsite access is no longer needed
  - Disclosure by vendor of vulnerabilities related to the product or service
  - Verification of integrity and authenticity of all software and associated patches provided by the vendor
  - Coordination of controls for vendor-initiated remote access.
- Best Practices for Renewable Assets:
  - Communication and Setting Expectations
    - Remote operators
    - Remote work by OEMs

Ensuring Reliability through Supply Chain Awareness

- Vigilant eye on vendors and suppliers to catch security risks early
- Check the integrity of the hardware and software
- Set up strict access controls
- Regularly audit to identify potential vulnerabilities
- By staying aware of what's happening in our supply chain, we can quickly spot and address potential issues and ensure that the grid remains reliable

Connect With Us

Navigating the Grid with Kellie Macpherson

Find our podcast and more on our YouTube Channel @radiangen

Linkedin.com/in/kelliemacpherson

Thank You!

Questions?

www.radiangen.com

your.name@radiangen.com