

The Central District is pleased to bring you the latest information concerning utility rates, project developments, Public Service

Commission actions and other news you can use. I hope you will find this information to be a useful resource to learn about the Public Service Commission, consumer issues and the continuous work we are doing for the citizens in the Central District and across the state of Mississippi. Thank you again for allowing me to serve you in this capacity.



Make Cybersecurity A Priority at Your Business (and Home)

In addition to October being Energy Awareness Month, October is also recognized as Cybersecurity Awareness Month. While protecting the physical, operational and software systems of the utility sectors should be a 24/7/365 focus, I wish to take this opportunity to remind businesses and utility operators that implementing and maintaining cybersecurity protection measures should be at the forefront of any risk management framework.

Over the last few decades, rapid advancements in technology have transformed the energy sector, especially electricity, and the pace of the change is not slowing down. Cybercriminals don't just target personal data anymore. They now pursue the ability to disrupt critical national infrastructure and essential services and create physical and economic consequences for utilities and customers. Just as critical infrastructure operations are becoming more integrated, cyberattacks are increasingly advanced and more widespread than they have ever been.

I am proud to be a member the National Association of Regulatory Utility Commissioner's Critical Infrastructure Committee. This Committee makes cybersecurity within the energy and utility sectors one of its top priorities. Businesses, operators and regulators of all types and sizes, must understand cyber-based risks and how to defend against them. Furthermore, consumers must also understand and have confidence that their utility service providers are proactive in the protection of critical infrastructure and implement cybersecurity functions that maintain a safe, secure and reliable energy network.

While we do not have a cybersecurity division within the Mississippi Public Service Commission (MPSC), this office has conducted in-person sessions with managers of regulatory, technology, security and more of the major rate regulated utilities that provide electric and natural gas service in Mississippi. Through these interactions, I am confident that these utilities have strong cybersecurity programs that meet or exceed industry standards, have established internal processes that can identify and mitigate vulnerabilities, and collaborate with others in the industry to understand the latest tactics, techniques, and procedures used by cyberattackers. You can be confident that utility companies will continue to put resources into understanding cyber risks and how to defend against them.

While the general mission of the MPSC is to ensure safe, reliable, and adequate utility service at a fair and equitable cost to ratepayers, the evolving threat of cyber-based incidents exposes the potential need for information on cybersecurity risk management, preparedness, and mitigation programs within the MPSC. One of my past newsletters — <u>Cybersecurity and State Regulatory Commissions</u> — explores how state regulatory commissioners can implement cybersecurity in their work programs to complement existing regulatory functions.



Continued...

This week I completed in-house cybersecurity training and MPSC staff may receive random "phishing simulation emails" to see if employees can spot the typical malicious content used by groups that wish to hack into and take control of systems. I just hope the simulation emails don't include anything about SEC football. I am not sure how we would fare! But that is exactly what these "phishing" emails are designed to do: Distract you and hope you act impulsively.

As we work internally to beef up our protection systems and reduce our cyber vulnerabilities, you should also evaluate your own business's cyber risks. This should include conducting a cyber-risk analysis, evaluate your cyber readiness, and create and implement a response plan. Simply ask yourself if you can run your business in "manual" mode? If you think that you don't have any risks to be concerned about, just remember Murphy's Law!

Below, the DHS's Cybersecurity and Infrastructure Security Agency (CISA) and the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) have put together an infographic describing key areas of risk and best practices for protection systems within the electricity sector. However, these basic principles can be adopted and applied across most business and industry sectors. Protecting one's information, operation or infrastructure in today's digitally connected world requires understanding and diligence. Don't wait until after an unfortunate event to take action.

The Nation's electricity grid could be vulnerable to increasing cyber threats that have physical consequences. New vectors for a disruptive attack on the Nation's grid and operations are emerging as monitoring and control technologies and connected devices become further integrated at the industrial and consumer levels.



AREAS OF RISK

CYBER:

Cybersecurity is an evolving security challenge for the electricity sub-sector. Cyberattacks pose a persistent threat to the electricity sub-sector and can cause severe physical and economic harm. Hackers can disrupt operations through ransomware attacks or by exploiting virtual private networks and gaining access to control systems responsible for critical operational components, such as tap changers on transformers. Malicious actors may continue to use cyber activity to bypass physical security measures.

Physical security requirements for the electricity sub-sector are a complex challenge. For example, the diverse and disparate network of outdoor sub-stations are vulnerable to a number of physical attacks. Trespassers can damage transformers and compromise on-site control systems using firearms, explosives, and motor vehicles. Unauthorized persons are also increasingly using small Unmanned Aircraft Systems to bypass traditional security measures to conduct surveillance, damage transmission lines, and execute other nefarious actions.

SUPPLY CHAIN

Managing the security and quality control of component acquisition is vital for the electricity sub-sector. A single compromised manufacturer or poorly secured component for Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), or software management systems, when broadly distributed across the electricity sub-sector, could compromise utility systems. Additionally, attacks on the sub-sector's supply chain for critical component manufacturers could delay the acquisition of key operational components.

PERIPHERAL DEVICES:

Electricity sub-sector operators are increasingly integrating Industrial Internet of Things (IIIT) devices with ICS to help monitor, regulate, and manage operating environments. These connected devices pose many of the same risks to enterprise security as traditional ICS. Inherent risks of IIIT devices include vulnerabilities in design, manufacturing, implementation, configuration, and disposal. For example, an IIoT device using outdated or unpatched software or firmware could be at greater risk of compromise and used to infiltrate enterprise networks, systems, and data stored in the cloud.

BEST PRACTICES FOR SECURING THE ELECTRICITY SUB-SECTOR

Protect Networks:

 Identify, minimize, and secure all network connections to ICS assets.

- Secure ICS and supporting systems by disabling unnecessary services, ports, and protocols. Enable security features and implement robust configuration management practices.
- Continuously monitor facility networks, applications, and other ICS and SCADA software systems.
- Develop facility-wide cybersecurity standards and implement cybersecurity best practices such as multifactor authentication for system access. Regularly check, test, and implement ICS security patches.

Secure Vulnerable Infrastructure:
Develop a risk management framework to better
understand how to secure vulnerable infrastructure.
This framework can identify, analyze, and communicate
risk. It can further instruct users on accepting, avoiding,
transferring, or controlling risk to an acceptable level at an
acceptable cost. The framework should do the following.¹

- Assess the threats that are most likely to cause significant damage to components and operations.
- Prioritize vulnerability reduction efforts.
- Address physical features or operational attributes that make infrastructure elements open to exploitation.
- Mitigate the potential consequences of incidents proactively or prepare to mitigate them effectively if they do occur.

Formalize Collaboration across Organizational Security Functions:

Implement an integrated approach to security that aligns cybersecurity and physical security teams with grid operators. Cross train security personnel to enable a holistic understanding of cyber-physical threats and their impacts to grid operations and consider implementing an Insider Threat Mitigation Program. This collaboration can ensure personnel have the knowledge and tools to rapidly identify and respond to an incident with cross-sector impacts. See CISA's Cybersecurity and Physical Security Convergence Guide, which provides a framework for establishing formal collaboration between cybersecurity and physical security teams.

Update Outdated Infrastructure and Technology:

Invest in improvements to infrastructure and operational technology (OT) that are critical to daily operations. When installing new OT systems that are connected to information technology (IT) networks, ensure both systems can be readily secured and updated. Understand how OT is interacting with and connected to enterprise networks. Identify, logically isolate, and consider how obsolete or orphaned equipment is utilized in your environment and ensure risk management principles are applied.

Assess the Supply Chain:

Coordinate with individuals within the organization who engage in supply acquisition and management of security and compliance to ensure effective supply chain management practices. Establish protocols to assess already procured hardware and software components to understand which are used for critical functions and what systems have remote access capabilities to these systems. Consider how information and communications technology Supply Chain Risk Management (SCRM) and SCRM essentials integrate into each component to identify risks and vulnerabilities associated with the availability, integrity, and confidentiality of your ICS.

Secure Connected Devices:

Conduct an inventory of IIoT devices, understand how they communicate and link to the network, and disable any unnecessary internet connections, ports, and devices. Ensure connected devices connect only to intended systems. Separate the network supporting IIoT devices from the main IT and OT networks. Consider whether the IIoT device for acquisition supports software updates or security patches. Educate system administrators on the importance of cybersecurity and integrator/vendor collaboration in a connected IIoT environment.

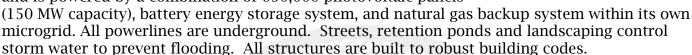
1. CISA, A Guide to Critical Infrastructure Security and Resilience (November 2019), https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience



Community Built for Resiliency Survived Ultimate Test

Hurricane Ian exerted a huge toll on Southwest Florida. Thousands are still without power and/or water and the human losses break our hearts. But like so many areas of the country hit by major storm events, Southwest Florida will eventually rebuild. And when they do, perhaps they will look to Babcock Ranch for storm resilient technologies and construction standards.

<u>Babcock Ranch</u> is located about 12 miles northeast of Fort Myers, FL. The neighborhood currently consists of about 2,000 homes and is powered by a combination of 650,000 photovoltaic panels



Other than some knocked over street signs and palm trees, little else in the neighborhood was damaged and they never lost power. Unfortunately, many in the surrounding communities did not have the same experience.

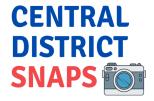
Last Week at the MPSC

- © On October 11, 2022, at 6 pm, the Central District Commissioner and representatives from the **Commission** attended and presented at a meeting that took place at the Gibson Memorial Church in Vicksburg, regarding Great River Utility Operating Company, LLC's proposed rate for three wastewater systems in the area. The meeting was hosted by Representative Kevin Ford in collaboration with three local homeowner's associations (Openwood, Brentwood, and Fairways) at the request of the HOAs. The **Commission** and **Great River Utility** were invited to present, provide information, discuss concerns, and answer questions. The Commission provided <u>handouts</u> and a <u>presentation</u> about the MPSC's overall role, the MPSC's process and proceedings, conditions of each of the wastewater systems, current rates, proposed rates, and how new rates will ultimately be established. As the night progressed, the meeting evolved into a more casual back-and-forth between those in attendance and the presenters as numerous points were made and addressed. The MPSC concluded with a reminder that Great River has filed a request for the **Commission** to approve these <u>proposed</u> new rates, and the request is undergoing a full review by the **Commission** and the Staff. **The Commission** has 120 days to render a decision on the matter, but it is highly likely these proceedings will take longer than 120 days and could stretch into 2023.
- Entergy Mississippi, LLC (EML) filed its required annual adjustment to their Middle South Energy ("MSE") Riders. Pursuant to FERC Docket Nos. ER82-616-000 and ER82-483-000, EML was allocated a 33% interest of System Energy Resource Inc.'s ("SERI") 90% interest in Grand Gulf Nuclear Station. MSE-3 provides for EML's recovery of its allocated share of Grand Gulf costs as a fixed percentage of EML's base rates. The MSE rate factor provides cost recovery of the projected level of SERI demand charges for the succeeding fiscal year, plus any over or under recovery associated with collection of the prior year's MSE Riders. Both riders are formula rates, previously approved by the Federal Energy Regulatory Commission and the Commission, and do not require Commission action to become effective. The impact of the EML's proposed factor on an average residential customer's bill, using 1,000 kWh, is an increase of \$3.00. The increase is attributable to one-time tax credits rolling off and an increase in demand charges.



Continued...

- The Commission issued an Order certifying DE Fastlink, LLC as an Eligible Telecommunications Carrier (ETC) for purposes of the continued receipt and utilization of high-cost RDOF support for the 2023 universal support funding year for broadband deployment.
- The Commission issued a Notice of Hearing in regard to the Petition of Harvest Gold Solar Power, LLC, for a Facilities Certificate to Construct and Operate a Solar Electric Generating facility in Sunflower County. The hearing will be held on October 25, 2022, at the Sunflower County Circuit Court Room, 200 Main St, Indianola, MS beginning at 5:30 p.m.
- Entergy Mississippi, LLC filed its Interim Adjustments Compliance Filing in regard to its Notice of Intent to Implement a Routine Change in Rates. This filing was made in compliance with the Commission's Order issued October 4, 2022. The net impact of both the Energy Cost Factor and Power Management Cost Factor Interim Adjustments for the typical residential customer using 1,000 kWh per month will see an increase of \$2.01 per month incrementally over six months until the total of \$12.02 is reached in April 2023. The Commission also issued an Order Approving Entergy Mississippi, LLC's Compliance filing and Tariffs.
- Intrado Corporation, together with Intrado Corporation's wholly owned indirect subsidiary Intrado Safety Communications, Inc., and Guardian US Holdco LLC filed a <u>Joint Application</u> requesting Commission approval to transfer indirect control in which they will consummate via a stock purchase transaction resulting in Guardian US Holdco LLC acquiring ultimate control of Intrado Safety Communications, Inc.
- BCM One, Inc. and Wholesale Carrier Services, Inc. filed a <u>Joint Application</u> for Approval of a Pro Forma Intermediate Transfer of Control. The Pro Forma Restructuring involves an internal corporate reorganization of the indirect upstream ownership, in which ultimate control of BCM One, Inc. and Wholesale Carrier Services, Inc. does not change as a result. The Restructuring will not discontinue, reduce, or impair service to customers or change rates, terms, or conditions of service.



Last week, I had the opportunity make a double trip up to Supertalk MS to join Gerard on MidDays with

Gerard Gibert to discuss the updated Distributed Generation Rules. The following morning, I joined Mary on the Mary Wieden & You Show regarding the anticipation of rising costs of natural gas and how to be more energy efficient to help save money on utility bills this coming winter.







Scott Larsen, Senior Pastor at Brandon First United Methodist Church, joined us for the Commission's October Docket meeting.

ICYMI: I joined
Byron Brown
on WJTV'S
Mississippi
Insight this past
Sunday. Check
out the
segment:
https://www.wjtv.com/mississippi-insight/



We joined Atmos Energy last week at the new Jackson Fire Department Station on Medgar Evers Boulevard to present a \$29,600 rebate check to the Department through Atmos Energy's Innovations Program and the Atmos Energy SmartChoice Program for the installation of a 125KW natural gas



backup generator, energy efficient natural gas appliances, including tankless water heaters, 90% AFUE natural gas furnaces, smart thermostats, and cooking equipment. The installations will save the Department over \$2,000 a year in utility costs.



Thanks to the members of the MS
Underground Utility Damage Prevention
Committee for continuing to review and
refine the laws and rules governing
excavation activities near utilities. Everyone
has a role in protecting these critical systems.





On Tuesday night I attended a meeting that took place at Gibson Memorial Church in Vicksburg. The meeting was hosted by State Rep. Kevin Ford in cooperation with

three local homeowner's associations (Openwood, Brentwood, and Fairways) at the request of the HOAs. The MPSC and Great River Utility Operating Company, LLC. were invited to present, provide information, discuss concerns, and answer questions. We appreciate Rep. Ford for the opportunity to participate in the meeting and share information on the role of the MPSC in ensuring just and reasonable rates for essential utility services.

It was my pleasure to speak at the International Right of Way Association's Mississippi Chapter Symposium and Region 6 Fall Forum in Pearl this morning. I appreciate Greg Thompson for inviting me to participate and I was followed by my good friend, MDOT Commissioner Willie Simmons. We

must support those who work in this industry as they remain committed to improving quality of life through infrastructure development.







Last week, our Consumer Complaint Specialists handled a total of 26 complaints in the Central District.

Electric Companies 15
Telecommunications 7
Natural Gas 3
Water/Sewer 1

Last week, the Central District received a total of 162 complaints from consumers against potential telemarketers through our no call app, website and mail-ins.

We encourage consumers to file

telemarketing complaints with the Federal
Trade Commission at http://www.donotcall.gov/ in addition to filing
complaints with the
Mississippi Public Service Commission.