

REGULATORY/POLICY COMMITTEE MEETING

• • TUESDAY, May 6, 2025



BROWNSVILLE PUBLIC UTILITIES BOARD

Call Open Meeting To Order



BROWNSVILLE PUBLIC UTILITIES BOARD

Public Comments

Items For Presentation and Discussion

- 1. Presentation and Discussion of the Proposed Flexible Work Arrangements Policy -Sergio Delgadillo
- 2. Consideration of Possible Amendment to the Rules Governing the Board of Directors (Board Order of Business) Paul Gonzalez
- 3. Presentation and Discussion of the Proposed Cost of Living Adjustment Policy -Sergio Delgadillo
- 4. Presentation and Discussion of the NERC Compliance Program and Policy Gustavo Leal
- 5. Discussion and/or Requests for Future Agenda Items -



Flexible Work Arrangements

PRESENTATION AND DISCUSSION OF THE PROPOSED FLEXIBLE WORK ARRANGEMENTS POLICY

• • REGULATORY/POLICY COMMITTEE |Tuesday, May 6, 2025

Sergio Delgadillo

Sr. Compensation & Benefits Manager

Compensation & Benefits Department

Types of Work Arrangements



Benefits to BPUB



Benefits to Employees



Increased engagement and job satisfaction



0

Alignment of

work hours

with

productive

time

Better work/life balance



Improved health



Decrease of stress / burnout

Flexible Work Arrangements

A flexible work schedule allows employees to adjust their schedules within set parameters.

•Options at BPUB will include:

Flextime Arrangement

o 8 hr. day, with flexibility in start/stop times

Compressed Work Arrangement

- Four ten-hour days and one day off each week
- Four nine-hour days and one half day off each week
- Eight nine-hour days, one eight-hour day and one day off each pay period (exempt EEs only)

Managing the Arrangements





BROWNSVILLE PUBLIC UTILITIES BOARD

Questions?



Cost of Living Adjustment Policy

PRESENTATION AND DISCUSSION OF THE PROPOSED COST OF LIVING ADJUSTMENT POLICY

• • REGULATORY/POLICY COMMITTEE |Tuesday, May 6, 2025

Sergio Delgadillo

Sr. Compensation & Benefits Manager

Compensation & Benefits Department

Importance of Employee Compensation



Cost-of-Living Adjustment

Pay adjustment usually computed as part of an annual compensation plan, applied uniformly to all employees before performance-based increases, which is dependent on the consumer price index and BPUB financing capacity.



Proposed Policy

Provides for consideration of an annual cost-of-living adjustment based on the CPI-U published by the U.S. Bureau of Labor Statistics.

In years when COLA is approved, the pay structures will also be adjusted by the same percentage to maintain pay relationships.



PUBLIC UTILITIES BOARD

NERC Compliance

• • REGULATORY/POLICY COMMITTEE MEETING | May 6, 2025

Gustavo C. Leal

NERC Compliance Manager & CCO

NERC Compliance

What is NERC?

The North American Electric Reliability Corporation (NERC) is responsible for protecting the power grid and electric generation of all of North America. Its job is to prevent things such as random blackouts or attacks on the power grid while regulating the system. It is also in charge of investigating the reasons for these blackouts and finding solutions to the cause. However, it's a relatively new organization, and is constantly undergoing change.

NERC was formed in response to the need for a more reliable and coordinated electric grid in North America and was driven by increasing concerns over power system blackouts and failures, including the 2003 North East Blackout that affected 45 million people in the USA and 10 million in Canada.

NERC History



- **1968:** The NERC started back in 1968 in the electric utility industry crafting rules and regulations for the operation of the bulk power system. However, in the beginning, these rules and regulations were simply voluntary and had no legal repercussions if an entity failed to follow them.
- 2003 Blackout: In 2003, a massive blackout hit the northeastern section of North America. This blackout remains the biggest in USA history and came from a variety of errors and malfunctions that cascaded into a huge outage for millions of people. Soon after that, an investigation found a need for better protections on the electrical grid.
- **2005**: Energy Policy Act was enacted and NERC becomes the Electric Reliability Organization (ERO). FERC designated NERC as the ERO giving NERC authority to create and enforce mandatory reliability standards. The ERO Enterprise is a collaborative, international network comprised of the North American Electric Reliability Corporation (NERC) and the eight Regional Entities that brings together collective leadership, experience, judgment, skills, and technologies for assuring the reliable operation of the North American Bulk Electric System (BES)
- **2007:** FERC Order 693 approved NERC's reliability standards through order 693 making them legally enforceable across the Bulk Electric System (BES).
- **2008:** FERC Order 706 approved the first set of NERC Critical Infrastructure Protection (CIP) standards making them mandatory. The CIP Standards were created in response to growing concerns about cybersecurity threats and physical vulnerabilities to the BES, including the 2001 9/11 attacks to the World Trade Center in NYC.



Energy Structure



- U.S. Department of Energy's (DOE) research and development to strengthen and modernize our nation's power grid to maintain a reliable, affordable, secure, and resilient electricity delivery infrastructure.
- The Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil.
- NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.
- NERC delegates to the Reliability Entities (RE) authority to enforce reliability standards. Texas RE is the Reliability Entity in the ERCOT interconnection.



NERC Interconnections



SLIDE 5

NERC Reliability Standards

Standard	#	Торіс
BAL	8	Frequency control, Area Control Error (ACE), Contingency Reserve
CIP	13	Sabotage Protection, cybersecurity
СОМ	2	Telecommunications
		Emergency operations planning, alerts, load shedding, distubance reporting,
EOP	7	restoration, black start
FAC	7	Generation, transmission and end-user connection requirements, vegetation management, facility ratings for system modelling
INT	2	Interchange transactions, tagging and implementation
		Responsibilities and authorities, facilities, operations planning, current day
IRO	11	operations, transmission loading relief
		TC,ATC, TRM calculation methodologies, capacitiy benefit margin, modelling
MOD	6	data, data exchange, load management
		Requires coordination between Nuclear Plant Generator Operators and
NUC	1	Transmission Entities
		Reliability Coordination & Responsibility, authority, training, credentials,
PER	3	staffing
PRC	18	Protecticion coordination, fault recording, misoperations, maintenance and testing, under-frequency/voltage load shedding, special protection systems
		Reliability responsibilities, operations planning, outage coordination,
		operations, operational data exchange, system monitoring, operating limit
ТОР	4	violations
TPL	2	System performance, normal and after loss of an element, reports, data
VAR	3	Voltage and reactive control



NERC Standards Subject To Enforcement

There is currently a total of 87 standards subject to enforcement including additional requirements and sub-requirements of each standard.

74 of the 87 standards are FERC Order 693 standards that define the reliability requirements for planning and operating the North American bulk power system. NERC 693 standards govern all stages of the energy process from generation to transmission to distribution.

The other 13 standards are FERC Order 706 standards that define as theCritical Infrastructure Protection (CIP) standards and are a set of standards aimed at regulating, enforcing, monitoring and managing specifically the physical and cyber security of the Bulk Electric System (BES).

BPUB is currently registered with NERC as a Transmission Owner, Transmission Operator and Transmission Planner (TO, TOP, TP), Distribution Provider(DP) and Generator Owner and Generator Operator (GO,GOP).

NERC Compliance Committee Org. Chart



Facilities Impact Rating

NERC CIP Standards categorize the BES Cyber Systems based on their potential impact on the reliability of the BES.

- **High Impact:** Systems whose compromise could cause widespread instability or cascade outages.
- **Medium Impact:** Systems whose compromise could cause significant but less widespread impacts.
- Low Impact: Systems with less critical impacts.
- BPUB has two Medium Impact rating facilities:
- Main Energy Control Center and the Backup Energy Control Center
- And 15 Low Impact facilities:
- The Silas Ray Power Plant and 14 Electrical Substations



Personnel Risk Assessment Program (PRA) BPUB conducts a Personnel Risk Assessment on all BPUB personnel and service vendors prior to granting authorized electronic or unescorted physical access to BES Cyber Systems.

The process involves the following:

- Interview Process
- Identity Confirmation
- 7-Year Background Check Performed at the Local, State and Federal Level

The criminal background check must include the following:

- Current residence, regardless of duration; and
- Other locations where, during the seven years immediately prior to the date of the criminal background check, the subject has resided for six consecutive months.



Cybersecurity Training Program

BPUB personnel and service vendors who require authorized electronic or unescorted physical Access to BES Cyber Systems must receive security training prior to being granted access.

Training must include the following content:

- Cyber security policies;
- Physical access controls;
- Electronic access controls;
- The visitor control program;
- Handling of BES Cyber System Information (BCSI) and its storage;
- Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;
- Recovery of BES Cyber Systems;
- Response to Cyber Security Incidents; and
- Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.

To retain authorized access to BES Cyber Systems, training must be renewed at least once every 15 calendar months.



Cybersecurity Awareness Program

The BPUB Awareness Program requires that all personnel who have authorized electronic or authorized unescorted physical access to low and medium impact BES Cyber Systems receive awareness training as on-going reinforcement in cyber security practices.

Awareness must be received on a quarterly basis using at least one of the following mechanisms:

- Direct Communications (emails, memos, computer-based training);
- Indirect communications (posters, intranet, brochures); and
- Management support and reinforcement (presentations, meetings, training seminars).



Electronic Security Perimeter (ESP)

BPUB implemented an Electronic Security Perimeter to protect our BES Cyber Assets with the following controls:

- Firewalls monitoring and controlling traffic from and to the ESP, limiting it to specific sources and destinations and specific communication ports.
- Intrusion Protection System monitoring the data passing through the firewall to identify and take action on malicious traffic.
- Anti-Malware Protection software at each host
- File Integrity Monitoring software
- Centralized Log Management software
- Change Control Management software
- Vulnerability Assessment software
- Enforcement of Password policies
- Enforcement of Access policies
- Periodic Electronic access verification



Physical Security Perimeter (PSP)

BPUB implemented several PSP controls to protect its BES Assets, Including:

- Controlled physical access by card reader to Main and Backup Control Centers, Silas Ray Power Plant and all substations
- Quarterly review of personnel having PSP access
- Physical Access and alarms are remotely monitored by Energy Control System Operators via SCADA system.



Incident Response Plan

BPUB created an Incident Response Plan that was designed to provide guidance when responding to incidents involving intrusion, cyber threats, security breaches or cyber attacks. This plan was prepared to detect, protect and respond from cyber and physical incidents that could impact the reliability of the BES. The Plan includes but not limited to:

- Incident identification and classification.
- Incident Response Procedures
- Incident Reporting & Documentation
- Identify and Report to authorities and management.
- Define roles and responsibilities.
- Provide training and testing for annual review
- Prevent future incidents from happening



Disaster Recovery Plan

The purpose of a disaster recovery plan is to assist BPUB respond to disruptive events, such as natural disasters, cyber attacks, or power outages. The plan's goals are to minimize damage, disruption, and economic impact.

Calls to have a recovery plan in place in the event that a disaster/incident occurs and affects the operations of BPUB. These measures also contribute to the safe, efficient, and timely restoration of BPUB BES Cyber Systems to normal operations. The goal of these processes is to minimize any negative impacts to its BES Cyber Systems and operations.

The Plan includes:

- Systems Restoration
- Data Integrity & Backup
- Defining Roles and Responsibilities
- Establishing a Recovery Process
- Performing Exercise Plans
- Implementing Change Control
- Testing Information Systems





PUBLIC UTILITIES BOARD

Information Protection

The Information Protection Program prevents unauthorized access to BPUB BES Cyber System Information (BCSI). BPUB considers BCSI as any electronic and/or physical information that could be used to gain unauthorized access or pose a security threat to applicable BES Cyber Systems. This information could include but is not limited to:

- Security procedures or security information regarding:
 - BES Cyber Systems
 - Physical Access Control Systems
 - Electronic Access Control Systems
- Collections of network addresses
- Network topologies of BES Cyber Systems
- Backup configurations/files from BES Cyber Systems





Information Protection

All documents labeled as BCSI, electronic and printed hard copy, are accessed and used **only by authorized personnel.** Each authorized individual has a responsibility to:

- Protect BCSI information while in use, stored and in transit;
- Refrain from using this information for anything but official BPUB business;
- Refrain from disclosing this information to individuals that are not authorized to view them;
- Proper disposal of BCSI in accordance with NERC CIP-011-3.

BPUB has designated physical and electronic storage locations for BCSI. Electronic BCSI must be transferred utilizing encrypted methods. Physical BCSI must be labeled as "Confidential/BCSI" on the footer of each page and must have a cover sheet with the following label:

CONFIDENTIAL, BCSI INFORMATION

THE INFORMATION CONTAINED IN THIS DOCUMENT HAS BEEN CLASSIFIED AS CONFIDENTIAL, BCSI AND IF FOUND, IT MUST BE RETURNED TO THE NERC COMPLIANCE DEPARTMENT IMMEDIATELY!

The use of removable media to transfer BCSI is strictly prohibited.



Information Protection

Disposal of Physical BCSI

 To prevent the unauthorized use of printed hard copy documents that contain BCSI, all documents must be properly disposed using a cross-cut document shredder or document destruction service to ensure that the information cannot be recovered.

Redeployment or Disposal of Electronic BCSI

 To prevent the unauthorized use of BCSI, BPUB will ensure that all BCSI residing within a cyber asset is protected or destroyed prior to redeployment or disposal.



Supply Chain Risk Management

- BPUB has implemented procedural controls to assess and manage risks originating from the supply chain.
- Vendors are evaluated during the planning process
- Risks are identified and assessed before procurement
- Any needed mitigations are put in place and tested, before, during, and after implementation.



NERC Compliance Department

- The NERC Compliance Department also assists:
- Public Utility Commission of Texas (PUCT) Rules
- ERCOT Nodal Protocols
- ERCOT Operation Guides
- Other regulatory special projects
- Corporate Emergency Operations Plan



BROWNSVILLE PUBLIC UTILITIES BOARD

Questions?

GUSTAVO C. LEAL

NERC COMPLIANCE MANAGER & CCO

SLIDE 22



BROWNSVILLE PUBLIC UTILITIES BOARD

Adjournment