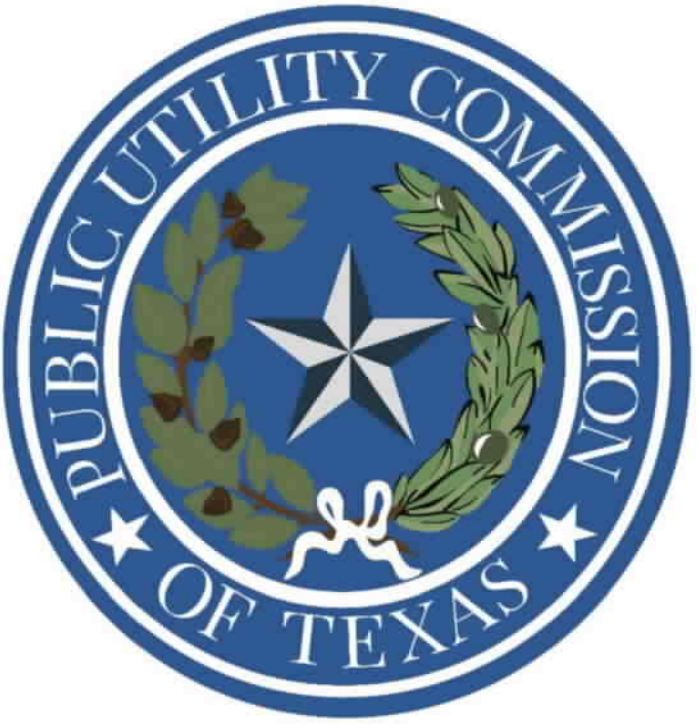


Filing Receipt

Filing Date - 2024-02-15 01:59:04 PM

Control Number - 53385

Item Number - 1708

FLOYDADA
MEMPHIS

LIGHTHOUSE ELECTRIC COOPERATIVE, INC.

A Touchstone Energy® Cooperative

P.O. BOX 600 • FLOYDADA, TEXAS 79235-0600 • PHONE 806 983-2814

February 15, 2024

Public Utility Commission of Texas
P.O. Box 13326
Austin, TX 78711

To Whom It May Concern:

Please file our EOP in Project Number 53385.

Sincerely,

Mike Green
Member Services Director

Emergency Operations Plan

of

Lighthouse Electric Cooperative, Inc.

TABLE OF CONTENTS

I. APPROVAL AND IMPLEMENTATION

A. INTRODUCTION

Lighthouse Electric Cooperative, Inc. ("Cooperative") maintains this Emergency Operations Plan ("Plan") for use during emergencies, natural disasters or situations involving curtailments or major interruptions in electrical service in compliance with 16 Texas Administrative Code § 25.53 - Electric Service Emergency Operations Plan ("Rule").

This Plan will be reviewed, and an annual drill performed at least once annually if it has not been implemented in response to an actual event within that year. Following any implementation or annual review, Cooperative shall assess the effectiveness of the Plan and modify it as needed. The official copy will be maintained at Cooperative's headquarters located at 703A Highway 70 East, and a list of modifications is included in Part I.C. below.

B. INDIVIDUALS RESPONSIBLE FOR PLAN

The individuals listed in Table 1 are responsible for maintaining and implementing the Plan and, if designated, have authority to change the Plan:

Table 1 Individual's Responsible for Plan

Name	Title	Responsibility	Authority to Change
Albert Daniel	General Manager	Principle administrator of the plan. Must review and approve all changes.	Yes

C. REVISION AND SUMMARY

This Plan, dated as of April 1, 2022, supersedes all previous versions of the Plan.

II. ORGANIZATIONAL AND PERSONNEL ASSIGNMENTS

The following is not intended as an exhaustive list of all probable or potential responsibilities required in an emergency situation. It does, however, define the essential staffing positions and responsibilities necessary for the management and resolution of unplanned system outages and events.

OPERATIONS SUPERINTENDENT OR SUPERVISOR ON-CALL

- Determines the level of the emergency and has complete responsibility and authority for completing restoration in a timely and efficient manner.
- Full responsibility for coordinating restoration efforts of Level 3 outages. If he is unavailable, the supervisor on-call will fulfill these duties. Both of these positions may be relieved by the director of operations and engineering.
- Insures adequate staffing of Operations Center to provide for the following:
  - Communication and device control
  - Data gathering and analysis
  - Limiting personnel in the Operations Center to critical staff only
  - Critical staff for Level 3 outages will include:
    - ✓ Two system operators
    - ✓ Operations superintendent or supervisor on-call
    - ✓ Director of operations and engineering (as needed)
    - ✓ Manager of communications (as needed)
    - ✓ IT personnel (as needed)
    - ✓ Division managers and other Cooperative staff (as needed)
    - ✓ Other personnel as requested by the operations superintendent
- Determines proper course of action for the restoration of affected transmission and distribution systems.
- Determines the priority for restoration, switching and patrolling.
- Secures outside contractor assistance if necessary.
- Determines and executes relief schedules during extended service restoration.
- Monitors working time of service and construction personnel so that management can determine appropriate rotation and relief schedules, insuring safety and minimizing fatigue.
- Direct strategic pre-placement of heavy equipment, dozers, etc.
- Provide periodic updates to manager of communications.

SYSTEM OPERATOR

- Notifies appropriate personnel in the event of an outage.
- Coordinates and directs activities required to restore the transmission and distribution systems during an outage.

- Maintains control of radio traffic insuring communication access for all field personnel.
- Insures strict adherence to lockout/tagout procedures.
- Insures members on life-support list receive priority status.
- Provides central communication and status information updates to the division managers and manager of communications.
- Determines extent of service interruptions by member count and by area.
- Monitors SCADA, outage management and related information systems, and logs all events during the outage.
- Requests support for various information and communication systems as needed.

LINE SUPERINTENDENTS

- Coordinate the logistics and execution of the Emergency Operations Plan by maximizing the available crews, equipment, and material.
- Establish a crew rotation plan when restoration of the system is expected to exceed 16 hours.
- Meet (as necessary) with the operations superintendent to assist in the development of restoration plans for the following day.
- Ensure outside personnel are guided by qualified Cooperative employees.
- Authorized to use direct access to system operations (806) 983-2814.

DIRECTOR OF OPERATIONS & ENGINEERING; ENGINEERING PERSONNEL

- Ensures all communication links are functional, and notifies appropriate vendors of potential troubleshooting and repair requirements to two-way radios, SCADA links, etc.
- Provides support to system operations by analyzing outage data and making recommendations for power restoration.
- Constantly monitors location and activity of all Cooperative and contract personnel working on restoration efforts and ensures this information is available to the system operator at all times.
- Inventory damaged lines/equipment and coordinate with supplier to ensure necessary material for repair is available to crews.
- Log location of all damaged or leaking devices requiring environmental cleanup.
- One field engineer shall remain in the office at all times to coordinate material needs directly to Texas Electric Cooperative ("TEC"). All requests for material, reports of oil leaks, etc., shall be reported through this one engineer.
- Keep appropriate regulatory bodies (municipal governments, Public Utility Commission of Texas ("PUCT"), environmental agencies, etc.) apprised of outage and restoration efforts as per statutory requirement.

DIVISION MANAGERS AND STAFF

- Maintain function of offices with reduced staff during normal business hours.
- Communicate with key account members.

- Coordinate and schedule member service representatives to take outage calls, and ensure designated lead is always present to serve as liaison between system operations and other member service representatives.
- Coordinate the assignment of duties to other employees to ensure any additional needs of the membership, Cooperative or the employees are addressed. Such duties may include:
  - Field inspection to assess damage.
  - Coordination and delivery of materials and meals to crews.
  - Ensure lodging is available for outside crews.
  - Guide out-of-town crews to the damaged areas.
  - Visit members that are on life-support systems if communication system is not working.
  - Transport employees to and from homes or from one crew location to another.

MEMBER SERVICE REPRESENTATIVES

- Provide trained and courteous personnel for answering member outage calls and verifying power restoration to members.
- Assist with the prioritizing of outage calls with regard to special needs or critical loads.
- Provide members with addition information with respect to anticipated outage time and the extent of the damage as supplied by press releases, et al from the manager communication.
- One member service representative will be designated by the appropriate division manager to serve as liaison between system operations and other member service representatives.
- Confirm restoration of power by follow-up phone call.

CONSTRUCTION, SERVICE AND MAINTENANCE CREWS

- Comply with all safety policies and procedures (e.g. lockout/tagout, grounding, etc.).
- Provides adequate personnel to patrol, repair, sectionalize and/or restore all damaged transmission and distribution systems.
- Coordinate material requirements with engineering to the TEC Utility Supply.
- Periodically review and determine the best utilization of equipment and personnel.
- Request mechanic personnel for emergency equipment and vehicular repair as needed.

DIRECTOR OF COMMUNICATIONS

- Serves as spokesperson for the Cooperative during emergencies.
- Prepares timely news releases, social media updates and public service announcements (see Appendix A for emergency contacts),
- Updates the general manager as advised by the operations superintendent.
- In the event of the director of communication's absence, these duties will be filled by the public relations specialist.
- Ensures member service representatives are provided with periodic updates on the status of the outage, consistent with what is reported in the general media.

MANAGER OF MEMBER SERVICES

- Complete or arrange for repairs to fleet vehicles in a timely manner to reduce downtime.
- Ensure all portable generators are operational and that any such devices used for communication purposes (backup power supply at Cooperative radio towers) are fueled and ready to run.

III. Communication Plan

EMPLOYEE COMMUNICATIONS

Communication with our employees is critical to relaying information such as where to report to work, if we need extra employees on duty, situational updates, etc. Communication tools available as needed include sending emails to Cooperative employees allowing us to reach every full-time and part-time employee; updating our employee-only website where all employees can login; updating Facebook and Twitter; texting; calling.

B. OUTAGE REPORTING/CONSUMER COMPLAINTS

Members can report outages by calling us at (806) 983-2814. If the line is busy, they can still leave a message to report their outage.

Member service representatives are called into any of our four service offices to answer calls and process outage reports recorded by the automated system. They visit our Facebook page for updates and information to share with members. Member service representatives work continuously until the outage is restored or until the operations superintendent determines that such services are no longer necessary.

Members can file complaints by calling the cooperative at (806) 983-2814.

C. PUBLIC COMMUNICATIONS

Communication tools include Facebook, along with the Cooperative's website and press releases to TV, radio and newspaper outlets. A Facebook feed is located on the Cooperative's website to connect the two information sources. The Member Services Manager is available for interviews as needed.

D. COORDINATION WITH VISITING WORK CREWS

Differences in radio frequencies combined with unfamiliarity with our transmission/distribution system make it imperative that all visiting work crews be accompanied by a qualified employee from the Cooperative during their work activities.

E. CRITICAL LOADS

The Cooperative will attempt to notify critical loads either before or at the onset of an emergency by any of the following methods: phone, social media, Cooperative's website, law enforcement officers, other important contacts and utility personnel in the field.

F. REGULATORY COMMUNICATIONS

The Director of Risk Management shall insure the timely filing of reports in the event that a system failure or load loss meets the reporting threshold of state and federal regulatory bodies.

1. Procedure for Outage Reporting to DOE

The Form OE-417 is the critical alert mechanism for informing DOE of electrical emergency incidents or disturbances that disrupt the operation of any critical infrastructure in the electric power industry.

Instructions for filing as well as a link to the on-line form are located at:

http://www.eia.gov/survey/form/oe_417/instructions.pdf

Form OE-417 must be submitted to the Operations Center if one of the following apply:

1. Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations.
2. Cyber event that causes interruptions of electrical system operations.
3. Complete operational failure or shut-down of the transmission and/or distribution electrical system.
4. Electrical system Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system.
5. Uncontrolled loss of 300 Megawatts(MW) or more of firm system loads for more than 15 minutes from a single incident
6. Load shedding of 100 MW or more implemented under emergency operational policy.
7. System-wide voltage reductions of 3 percent or more.
8. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.

Initial reports are due within 60 minutes of the time of system disruption; however the DOE will permit telephone notification (202) 287-1849 if the incident or disturbance is having a critical impact on the operations. An initial report must still be filed as soon as possible. A follow-up report is due within 48 hours of the time of the system disruption.

Instructions and forms for reporting to both the PUCT and the Department of Energy ("DOE") are located in Appendix B.

2. PUCT

Upon request by PUCT staff during an activation of the State Operations Center (SOC) by the Texas Department of Emergency Management (TDEM), the Cooperative will provide updates on the status of operations, outages, and restoration efforts. Updates shall continue until all event-related outages are restored or unless otherwise notified by PUCT staff.

3. Office of Public Utility Counsel (OPUC)

Upon request by OPUC during an activation of the SOC by the TDEM, the Cooperative will provide updates on the status of operations, outages, and restoration efforts. Updates shall continue until all event-related outages are restored or unless otherwise notified by OPUC.

G. COMMUNICATIONS WITH RELIABILITY COORDINATOR

Cooperative's Transmission Operator managers communications with Reliability Coordinator. Please refer to Appendix A for the Transmission Operator's contact information.

IV. EMERGENCY SUPPLIES & ASSISTANCE COORDINATION

Cooperative maintains an adequate number of poles, transformers, conductor, and associated hardware at our two offices. We also maintain a list of suppliers and vendors that can be contacted in case of an emergency.

Additionally, as described below Cooperative has access to mutual aid in in the event it needs access to additional supplies and work crews in an emergency.

Please refer to Appendix C: Emergency Supplies for a list of emergency supplies to be maintained at Cooperative sites and Appendix D: Restoration Crew Supplies for a list of emergency supplies for restoration personnel.

SECURING ASSISTANCE FROM REGIONAL COOPERATIVES

Cooperative has a Memorandum of Understanding ("MOU") in place between 17 adjacent distribution cooperatives plus Golden Spread Electric Cooperative ("GSEC") for emergencies that can be coordinated within the MOU participants.

During an emergency Cooperative will survey the extent of damage and determine as nearly as possible the outside personnel and equipment needed. If MOU participants are not able to respond to needs, contact Texas Electric Cooperatives to secure additional assistance. Please refer to Appendix F for a description of the MOU.

B. SECURING EMERGENCY ASSISTANCE FROM TEC

For larger widespread emergency events where multiple members of the MOU need assistance that cannot be obtained within the MOU participants, Cooperative will request mutual aid assistance according to the plan developed by Texas Electric Cooperatives through their Loss Control & Safety Program.

Cooperative will survey the extent of damage and determine as nearly as possible the outside personnel and equipment needed. Cooperative staff will contact

Martin Bevins, VP Communications & Member Services

Other contacts at TEC include:
Mike Williams
Julia Harvey
Johnny Andrews
Danny Williams

When calling for assistance, give the following information:

- Nature of emergency
- Number and type of trucks needed
- Other equipment and tools needed
- Personnel and classification needed
- Materials needed
- Weather and road conditions
- Where the crews should report, and to whom
- How to contact your cooperative
- Name of person to receive this information
- Telephone numbers other than normal usage

To facilitate giving of above information over substandard communications media, or when the message must be relayed through persons unfamiliar with the terms, use the Form For Requesting Assistance (see Appendix E).

C. COMPLIANCE WITH COOPERATIVE SAFETY RULES

All Lighthouse Electric Cooperative personnel, contractors, cooperative crews providing mutual aid, etc. shall be required to comply with all safety rules and policies of the Cooperative. Such rules and policies include, but are not limited to, all provisions of the Cooperative's current safety handbook, OSHA 29CFR 1910.269, NESC, etc.

D. UNIFORM METHOD OF REIMBURSEMENT

It is suggested that cooperatives requesting assistance will reimburse the providers of the assistance the provider's actual labor, equipment and materials costs. It is suggested that the rate of pay for labor is at least time-and-a-half for all hours worked.
Every reasonable precaution shall be used to determine whether an employee is mentally and physically qualified to follow safe work practices. The crew foreman of the cooperative providing the assistance will determine the total number of continuous work hours. It is also recommended that the current FEMA Cost Code listing be considered.

E. TEC ADDITIONAL COMMENTS

1. The Texas Electric Cooperatives Loss Control Advisory Committee hereby recognizes the need to update and amend this manual, preferably on an annual basis. This document should certainly be reviewed shortly after a disaster event has occurred in the state, and which has affected any TEC member-system cooperative. Additional recommendations and suggestions will be added as necessary, and will serve as additional attachments or amendments to this text.
2. It is further recommended that the TEC Loss Control Advisory Committee, along with the TEC Directors, review and update the TEC Mutual Aid Plan for the Electric Cooperatives of Texas on an annual basis. Such review should include: 1) an update of names, addresses and phone numbers (to include emergency contact phone numbers) of all in-house contractors used by cooperatives in the state; 2) an updated listing of the current safety practices, rules, and regulations as adopted by the TEC Safety and Loss Control Advisory Committee and the TEC Board of Directors, including any amendments thereto; 3) an annual study of wages paid to assisting co-op personnel, to include an analysis of wages paid to assisting line crews from other surrounding states; and, 4) a review of billing rates for equipment and vehicles used during emergency restoration services and in subsequent permanent repair efforts during the days and weeks following a declared disaster.
3. It is strongly recommended that an inventory of materials be commenced by the assisting cooperative for all vehicles and equipment to be used during the emergency restoration period, and that such an inventory be conducted before vehicles are sent to an affected cooperative, and after work has been completed.
4. The assisted cooperative may either return the borrowed materials OR reimburse the assisting cooperative for materials replacement.
5. TEC should appoint a designated person from its staff to serve as an official liaison to both Texas Emergency Management (TEM) and the Federal Emergency Management Agency (FEMA).
6. Such liaison should work with officials from TEM and FEMA before, during, and after all declared disasters within the state of Texas. Additionally, said TEC liaison should stress the importance of applicable Codes and Standards that all Texas electric cooperatives are required by law to abide by and to apply such Codes and Standards during the Emergency Protective Measures period and during permanent repair efforts.
7. The Committee hereby recommends that TEM officials be trained in the knowledge of applicable electric Codes and Standards, (specifically the current version of the National Electrical Safety Code (NESC).
8. The Committee further recommends that FEMA auditors be consistent in both personnel and their findings among audited cooperatives.
9. The Committee suggests that TEC contract with, or arrange for, TEM officials to conduct an annual training seminar for cooperative personnel on disaster-related topics, including but not limited to: Public Assistance, Response and Recovery, Disaster-related Mitigation, and Hazard Mitigation.
10. Finally, the Committee recommends that, within 60 to 90 days following a disaster-related event, an in-depth analysis of the response and recovery effort by affected cooperatives

be conducted in order to make necessary improvements, changes or corrections to the TEC Mutual Aid Plan and to this disaster response and recovery guidebook. Mutual Aid Agreement Participants (Texas Only).

F. MANAGEMENT ISSUES

1. Mutual Aid Agreements between cooperatives and/or other organizations should be reviewed annually. Such agreements should specify the type of assistance each participant shall provide, and at what cost. The Mutual Aid Agreement should stipulate that the "helping partner," the participant responding to a request for help from the affected system, shall bill all costs at their normal rates; any "adders" should be specified and detailed in the agreement.
2. "Projects of Work," or "PWs," should specify verifiable quantities of work to be done whenever possible. Cooperative personnel must be prepared to explain cost over-runs or reasons for higher costs than were estimated in the original PW. Each state's Emergency Management Agency should be contacted immediately if an over-run is anticipated. Such constant tracking of a PW's progress may necessitate the use of a full-time accounting manager or project accountant for FEMA-related work. Such assignment would be added to the cooperative's "Administrative Costs" for the project.
3. Consider the assignment or designation of someone to be the cooperative Project Officer throughout the course of the disaster response and recovery. Such person could be from within the cooperative, or on loan from another system outside the disaster area. The Project Officer's duties could include the following:
    a. Assistance in evaluating and estimating the extent of damage to the cooperative's system;
    b. Assistance in securing available contractors and bid lists once the 70-hour Emergency Protective Measures period has passed;
    c. Coordinating with all other cooperative departments, including but not limited to management, accounting, engineering, operations, purchasing, and warehouse operations, to ensure an orderly assessment of needs by each department, and assistance in helping individual departments meet necessary requirements during the disaster response and recovery process. Such requirements would include ensuring environmental compliance via contacts with each state's Department of Environmental Quality (DEQ), One-call digging notification, State Historic Preservation offices and each state's Archeological Survey notification, as well as each state's Floodplain Administrator office notification.
    d. The Cooperative Project Officer could also coordinate the establishment of temporary storage areas for debris, and assist in dispensing state emergency management Environmental Release Forms and Historic Site Preservation Forms

to individuals or groups who contact the cooperative regarding the re-use of damaged or destroyed wood poles)

e. Other duties possibly assigned to the Cooperative Project Officer would be the evaluation of material acquisition, material dispensation, compilation of staking sheets during both the Emergency Protective Measures period and the Utilities (permanent repairs) period, and ensuring that all required maps, invoices, time sheets, and other paperwork documentation relevant to the specified disaster be collected and retained in an orderly fashion for future review by FEMA and OIG.

4. Send personnel from the accounting, operations, and engineering departments to the Reapplicant Briefing meetings and sign up for assistance as soon as possible. To the best of your ability, make sure original estimates of damage are thorough and comprehensive. Underestimating disaster damages could create additional PWs or delay reimbursements.
5. Management may wish to implement a policy that designates key employees and supervisors be available 24-hours per day, 7 days per week during the disaster, with work schedules to be determined by department heads in conjunction with the manager/CEO.
6. Communications, marketing, and/or public relations personnel may be utilized or designated to deliver material, equipment, and/or food (meals) to crews in the field, depending upon the personnel's knowledge of the distribution system and their certification on equipment or in materials handling.
7. As soon as possible, preferably during the first 70 hours of the disaster (FEMA's usual definition of Category B, Emergency Protective Measures), contact in-house contractors and those whose bids have been accepted and determine the length of time the contractors' emergency rates are to be in effect. Do not accept a contractor's argument that FEMA will automatically pay for extended work periods utilizing emergency rates. Also, unless other arrangements are made, advise contractors that after the initial 70-hour Emergency Protective Measures period, meals and lodging will no longer be paid for by the cooperative, but should be arranged and paid for by the contractor, with copies of meal and hotel receipts to be attached to weekly invoices supplied to the cooperative. Said meal and hotel tickets should list the names of crew members and corresponding room numbers at hotels to account for appropriate meal and lodging expenses. (Reference current IRS per diem guidelines.)
8. It is strongly recommended that additional engineering resources be arranged to assist in the daily development of staking sheets, material sheets, and work order information. This will allow the staking department to stay ahead of construction crews and provide for a more orderly flow of necessary and vital information to other key departments.
9. The engineering department should begin solicitation of at least three (3) bids from contractors as soon as possible, even before the full extent of damage to the system has been determined. Both FEMA and the OIG require that bids be procured for all permanent restoration work to be done be contractors. Make sure that any 'verbal contracts' are converted to written agreements to be shown to auditors.
10. Whenever it appears that consumers may be without electric power for several days or weeks, consider hiring security guards to be in place at office headquarters and

warehouse facilities. This generally eliminates the possibility of hostile issues with consumers and sends a message that personnel, material, and equipment are being safeguarded. Once the cooperative nears completion of its service restoration efforts to residential members, the security arrangement may then be terminated.

11. It is not uncommon for employees to retire, quit, or ask for re-assignment during or following a disaster. Carefully evaluate the need for cooperative linemen to work at night; their most effective work and/or leadership will most likely be during daylight hours, when damage to the system is clearly visible and when they have been adequately rested.
12. Document the first day of the outage and the day the last consumer's service was restored. This may impact various FEMA Categories A through F on your co-op's Force Account Labor statistics.
13. Have an Organization Chart of all cooperative employees, indicating what area or department they worked in before and during the disaster. This will help resolve questions about force account labor when it is classified into Categories A, Debris Removal; B, Emergency Protective Measures; and F, Utilities (Permanent Repairs).
14. No employee should work more than a total of 16 hours time on duty, immediately preceded by 8 or more consecutive hours off duty time, except under emergency conditions, as determined by the Cooperative. Duty begins when the employee reports to work and ends when the worker is released from work, and includes breaks, interim periods, or time spent engaged in any service for the Cooperative.
15. Insurance claims filed with FEMA should have a disclaimer from the cooperative's insurance carrier. Have copies of all insurance policies available for inspection by state emergency management, FEMA, and OIG personnel.
16. Insist that daily time sheet entries be made by all personnel, listing hours worked, names of crew members, and location work was performed; document, with narrative descriptions, any work performed by office personnel if it is related to field work, i.e., delivery of meals or materials and equipment, warehouse work, etc.
17. Management should be prepared to explain the process that the cooperative used to select work crews, whether such crews were from other co-ops or were contract crews. Explanation of the cooperative's action plan and methodology used in selecting various contractors may be necessary, including lists of equipment needed and rationale used to determine which contractors and crews would be utilized.
18. Send groups of employees to state emergency management agency and FEMA training; this denotes the co-op's dedication to being properly prepared.

V. IDENTIFICATION OF WEATHER-RELATED HAZARDS

Cooperative operations personnel will monitor weather conditions, county emergency management alerts and applicable state agency advisories regarding severe weather events and conditions. Operations personnel will also participate in applicable State Operations Center (SOC) and Texas Energy Reliability Council (TERC) calls prior to and during weather and wildfire events. Cooperative's wildfire plan is addressed in greater detail in Section VI.D.

The following stages describe the various levels of preparedness in advance of, or during an outage situation.

PRE-STORM WATCH

- This is a precautionary level preceding the arrival of an anticipated severe weather event. This level would be activated following a severe weather forecast. The system operator will monitor the situation and advise the superintendent on-call. The system operator and/or superintendent may request assistance in answering phones (e.g. member service representatives, etc.).
    - o Expected outage time: None
    - o Scope of outage: No members out of service
    - o Initiated by: System operations or superintendent on-call

- **LEVEL 1**
    - Service likely to be restored in less than four hours. Typically handled by on-call service personnel, however supervisor or superintendent on-call may direct other personnel to assist as needed.
        - o Expected outage time: Less than 4 hours
        - o Scope of outage: Less than 100 members
        - o Initiated by: System operations or superintendent on-call

- **LEVEL 2**
    - Service likely to be restored in less than 12 hours without the assistance of outside crews. All construction, operations and service personnel to report.
        - o Expected outage time: 4 to 12 hours
        - o Scope of outage: Entire substation or major feeder
        - o Initiated by: Director of operations & engineering or general manager

- **LEVEL 3**
    - Requires outside help to restore service. All Cooperative employees must report.
        - o Expected outage time: More than 12 hours

o Scope of outage: Widespread damage to system
o Initiated by: Director of operations & engineering or general manager
o Operations superintendent to have full responsibility for coordinating restoration activities

VI. ANNEXES

Lighthouse maintains the annexes designated below, which are attached and incorporated into the Plan:

Annex	Title	Included	Explanation, if not included
A	Weather Emergencies	Yes	
B	Load Shed	Yes	
C	Pandemic and Epidemic	Yes	
D	Wildfires	Yes	
E	Hurricanes	No	Not applicable. Cooperative service territory is not located near or within a hurricane evacuation zone, as defined by the Texas Division of Emergency Management.
F	Cybersecurity	Yes	
G	Physical Security	Yes	
H	TDU Requirements	No	Not Applicable. Cooperative is not a Transmission and Distribution Utility as defined in 16 TAC §25.5
I	Additional annexes	No	No additional annexes necessary

ANNEX A – WEATHER EMERGENCIES

Please refer to Section II: Organizational and Personnel Assignments for a description of personnel duties during an emergency, and Section V: Identification of Weather-Related Hazards for Cooperative's process for identifying weather related hazards.

Please also refer to the following procedures:

- Appendix C: Emergency Office Supplies provides a list of emergency supplies maintained at Cooperative sites.
- Appendix: D: Restoration Crew Supplies provides a list of emergency supplies maintained on-site for restoration crews.
- Appendix G: Engineering and Operations provides engineering and operations emergency.

B. ANNEX B: LOAD SHED

1. Electric Reliability Council Of Texas ("ERCOT")

I. PROCEDURES FOR CONTROLLED SHEDDING OF LOAD

GSEC Operations Center receives Load Shed Instructions from ERCOT. GSEC's Operations Center performs a calculation to allocate the load shed requirement for Lighthouse Electric Cooperative, Inc. and communicates that instruction via voice communication.

Upon notification of curtailment and the target kW to be shed, Lighthouse Electric Cooperative, Inc. personnel will begin opening feeder circuit breakers via field personnel in the substation as outlined in the cooperative's Manual Load Shed and Under Frequency Load Shed Plan until the target kW is shed.

Once the target kW is shed, Lighthouse Electric Cooperative, Inc. will notify GSEC's Operations Center via voice communication that the allocated load has been shed.

Depending on the duration of the curtailment, it is planned to rotate load that has been shed among the substations and circuits on a time frame determined by the Lighthouse's Operations Center. This is to spread the outages as evenly among the Members as possible and minimize the inconvenience associated with the outage.

All load shed Instructions will be executed as soon as possible and without delay.

The cooperative uses discretion in prioritization of selecting load shed feeders by giving highest priority to critical natural gas facilities to remain in service, with other critical loads given lower priority to remain in service. Even though the cooperative plan attempts to prioritize critical natural gas facilities and other critical loads from manual load shed, designation as a critical natural gas facility or other critical load does not guarantee the uninterrupted supply of electricity.

Cooperative uses the following guide to curtail power to the categories listed below in sequential order:

I. Irrigation
II. Residential
III. Critical Loads

II. PRIORITIES FOR RESTORING SHED LOAD TO SERVICE

GSEC's Operations Center receives Instructions from ERCOT that load can be restored. GSEC's Operations Center performs a calculation to allocate how much load can be restored for Lighthouse Electric Cooperative, Inc. and communicates that Instruction via voice communication.

Upon notification of load restoration and the target kW to be restored, Lighthouse Electric Cooperative, Inc. personnel will begin closing feeder circuit breakers via field personnel in the substation until the target kW is restored.

Once the target kW is restored, Lighthouse Electric Cooperative, Inc. will notify GSEC's Operations Center via voice communication the amount of load that has been restored.

If any critical natural gas facilities or other critical loads were curtailed in step (i), they will be given higher priority for service restoration in the reverse order listed in Section 1.I above.

In addition to the priorities concerning community health and safety, Cooperative will assign crews to specific areas. Generally, the crews will concentrate on a given line section in order to restore power to as many members as possible. Restoration will be done systematically, with the best interest of all affected members in mind. However, one or more crews may be assigned to locations where special hazards exist or where especially critical loads require immediate attention. When not specifically assigned, these crews will be used to repair individual services

III. CONFIDENTIAL REGISTRY OF CRITICAL LOAD AND CRITICAL CARE CUSTOMERS

Cooperative maintains a registry of both critical care and critical load members; however, it is the responsibility of the member to inform the Cooperative of special medical needs. The Cooperative attempts to identify such members by asking at the time of establishing a new account whether any person residing at this new account location requires an electric-powered medical device to sustain life. Further, the Cooperative publishes reminders in the Texas Co-op Power magazine, newsletters and notices included with bills that the Cooperative needs to be informed of any special needs.

No less than twice a year, the Cooperative also provides load shed information with customer bills that addresses the procedures for implementing voluntary load shedding; the types of Member consumers who may be considered critical load or critical care and the application

process to be designated as such; and information about reducing electricity use at times when involuntary load shedding events may be implemented.

The registry is confidential and is accessible through the Accounting System at all times for use by operations personnel. The list identifies each member by location number and is cross-referenced on outage reports. These members are contacted before any planned service interruption by Cooperative personnel.
Methods to communicate with these members during emergencies when telephone service is not available include working through local law enforcement officers and emergency medical personnel in the field. Where possible, field visits by Cooperative personnel may also be used.

The registry is updated continuously, as necessary.

IV. ROTATING OUTAGES

Cooperative will attempt to inform members in advance of planned outages, however, during emergencies, outages may need to be rotated to maintain system integrity.

NOTE: Because the curtailment and shedding load is dependent on several factors (most significantly, the amount of load that needs to be curtailed), the System Operator may have discretion in determining where load shedding will best serve the interest of the cooperative.

.

2. Southwest Power Pool ("SPP")

I. PROCEDURES FOR CONTROLLED SHEDDING OF LOAD

Southwestern Public Service's ("SPS") Transmission Operations Center receives Load Shed Instructions from SPP. SPS's Transmission Operations Center performs a calculation to allocate the load shed requirement for Lighthouse Electric Cooperative, Inc. and communicates that instruction via voice communication.

Upon notification of curtailment and the target kW to be shed, Lighthouse Electric Cooperative, Inc. personnel will begin opening feeder circuit breakers via field personnel in the substation as outlined in the cooperative's Emergency Load Curtailment Plan until the target kW is shed.

Once the target kW is shed, Lighthouse Electric Cooperative, Inc. will notify SPS's Transmission Operations Center via voice communication that the allocated load has been shed.

Depending on the duration of the curtailment, it is planned to rotate load that has been shed among the substations and circuits on a time frame determined by the Lighthouse's Operations Center. This is to spread the outages as evenly among the Members as possible and minimize the inconvenience associated with the outage.

All load shed Instructions will be executed as soon as possible and without delay.

The cooperative uses discretion in prioritization of selecting load shed feeders by giving highest priority to critical natural gas facilities to remain in service, with other critical loads given lower priority to remain in service. Even though the cooperative plan attempts to prioritize critical natural gas facilities and other critical loads from manual load shed, designation as a critical natural gas facility or other critical load does not guarantee the uninterrupted supply of electricity.

Cooperative uses the following guide to curtail power to the categories listed below in sequential order:

I. Irrigation
II. Residential
III. Critical Loads

II. PRIORITIES FOR RESTORING SHED LOAD TO SERVICE

Southwestern Public Service's Transmission Operations Center receives Instructions from SPP that load can be restored. SPS's Transmission Operations Center performs a calculation to allocate how much load can be restored for Lighthouse Electric Cooperative, Inc. and communicates that Instruction via voice communication.

Upon notification of load restoration and the target kW to be restored, Lighthouse Electric Cooperative, Inc. personnel will begin closing feeder circuit breakers via field personnel in the substation until the target kW is restored.

Once the target kW is restored, Lighthouse Electric Cooperative, Inc. will notify SPS's Transmission Operations Center via voice communication the amount of load that has been restored.
If any critical natural gas facilities or other critical loads were curtailed in step (i), they will be given higher priority for service restoration in the reverse order listed in Section 2.I above.

In addition to the priorities concerning community health and safety, Cooperative will assign crews to specific areas. Generally, the crews will concentrate on a given line section in order to restore power to as many members as possible. Restoration will be done systematically, with the best interest of all affected members in mind. However, one or more crews may be assigned to locations where special hazards exist or where especially critical loads require immediate attention. When not specifically assigned, these crews will be used to repair individual services

III. PROCEDURE FOR MAINTAINING ACCURATE REGISTRY OF CRITICAL LOAD CUSTOMERS

Cooperative maintains a registry of both critical care and critical load Members, however, it is the responsibility of the member to inform the Cooperative of special medical needs. The Cooperative attempts to identify such members by asking at the time of establishing a new account whether any person residing at this new account location requires an electric-powered medical device to sustain life. Further, the Cooperative publishes reminders in the Texas Co-op Power magazine, newsletters and notices included with bills that the Cooperative needs to be informed of any special needs.

No less than twice a year, the Cooperative also provides load shed information with customer bills that addresses the procedures for implementing voluntary load shedding; the types of Member consumers who may be considered critical load or critical care and the application process to be designated as such; and information about reducing electricity use at times when involuntary load shedding events may be implemented.

The registry is confidential and is accessible through the Accounting System at all times for use by operations personnel. The list identifies each member by location number and is cross-referenced on outage reports. These members are contacted before any planned service interruption by Cooperative personnel.
Methods to communicate with these members during emergencies when telephone service is not available include working through local law enforcement officers and emergency medical personnel in the field. Where possible, field visits by Cooperative personnel may also be used.

The registry is updated continuously as necessary.

IV. ROTATING OUTAGES

Cooperative will attempt to inform members in advance of planned outages, however, during emergencies, outages may need to be rotated to maintain system integrity.

NOTE: Because the curtailment and shedding load is dependent on several factors (most significantly, the amount of load that needs to be curtailed), the System Operator may have discretion in determining where load shedding will best serve the interest of the cooperative.

C. ANNEX C: PANDEMIC PREPARDNESS PLAN

1. Objectives of the Plan

To prepare the Cooperative for the possibility of a pandemic by:

1. Educating employees about a possible pandemic event and the potential impacts

on the Cooperatives' business operations;

2. Implementing reasonable measures to mitigate the impact of a pandemic on the Cooperative and its employees;
3. Developing plans and policies for responding to a pandemic; and
4. Promoting employee wellness and minimizing opportunities for employees to be exposed to the disease while at the Cooperative.

2. Background

A pandemic is a global disease outbreak occurring when a virus emerges for which people have little or no immunity and for which there is no vaccine. The disease spreads person-to-person, causes serious illness, and can sweep across the country and ***around the world in very short time.***

It is difficult to predict when the next pandemic will occur or how severe it will be. Wherever and whenever a pandemic starts, everyone around the world is at risk. Countries might, through measures such as border closures and travel restrictions, delay arrival of the virus, but cannot stop it.

As of this writing, health professionals are concerned about the potential spread of a highly pathogenic virus.

3. Levels of Response

Because the nature of a pandemic cannot be determined in advance, this plan addresses the threat with three general levels of response: **Awareness, Epidemic** and **Pandemic**. These levels are defined as follows:

- **Level 1 – Awareness (seasonal)**
  - The virus is reported affecting 5-10% of the population within the State of Texas.
- **Level 2 – Epidemic (preparation)**
  - A widespread outbreak affecting 10-20% of the population. An epidemic may be declared by the Centers for Disease Control (CDC) or the Texas Health and Human Services Commission (HHSC).
- **Level 3 – Pandemic (implementation)**
  - A widespread outbreak affecting 20+% of the population. A pandemic may be declared by the CDC and/or the World Health Organization (WHO).

1. Preparation & Response Efforts

I. EMPLOYEE EDUCATION

Employees will be educated about the virus, how it spreads and how the Cooperative is responding.

Numerous educational resources are available from the WHO and the CDC. Employee luncheons, company intranet, posters and broadcast e-mail may be used to convey this information to employees.

Existing communication tools and communications plans would be used to educate and communicate pandemic-related messages to employees.

Level 1	▪ How to avoid the virus ▪ Preventing the spread of the virus ▪ Symptoms of virus ▪ Do not report to work if sick ▪ Do not return to work until all symptoms have cleared. Full duty release is required to return to work with no restrictions/limitations (provide specific guidance from public health organizations)
Level 2	▪ Limit face-to-face meetings ▪ Limit travel to affected areas ▪ Communicate changes in policy and/or practices
Level 3	▪ Suspend face-to-face meetings ▪ Suspend non-critical business travel

II. FLU SHOTS

Employees will be encouraged – and given an opportunity – to receive the flu vaccine.

III. SANITARY PRACTICES

Supplies to maintain a sanitary environment will be kept on hand and deployed, as necessary, including:

1 Hand Sanitizer
2 Disinfectant Spray
3 Rubber Gloves
4 Masks

Level 1	▪ Alcohol-based hand sanitizer in all areas (restrooms, break rooms, conference rooms, and at all meetings where food and drink are served) ▪ Disinfectant spray (e.g. Lysol) in all restrooms ▪ Facial tissues (e.g. Kleenex) in all meeting rooms and break rooms ▪ Brief cleaning crews on disinfecting techniques

Level 2	▪ No additional measures unless directed by the CDC or Texas HHSC
Level 3	▪ No additional measures unless directed by the CDC or Texas HHSC

IV. POLICY MODIFICATION/DEVELOPMENT

Policies related to sick leave will be reviewed with possible impacts from a pandemic in mind. The following issues will be among those considered:

1. A possible relaxing of sick leave policy during a Level 2 or 3.
2. The possibility of mandatory leave for employees with symptoms of illness
3. A set of return-to-work guidelines to prevent employees from returning while still contagious
4. Some guidance on the handling of missed time for employees that do not wish to come to work for fear of exposure
5. Guidelines to identify positions that would qualify for work-from-home (WFH)
6. Identification, by department, of potential WFH employees

Level 1	▪ Normal leave policies
Level 2	▪ WFH permitted (with supervisor approval)
Level 3	▪ WFH encouraged (with supervisor approval) ▪ Relaxation of sick leave and other relevant policies

V. BUSINESS CONTINUITY

Managers will be asked to re-examine their critical functions at a Level 1 situation. Specifically:

1. Are employees within the department cross-trained in job functions related to critical processes?
2. Could the department continue to perform its critical processes with a 40-50% employee absentee rate?
3. Which of those employees are equipped to work from home (home computer, Internet access, VPN, etc.)?

The IT Department will develop plans for a wide deployment of software and services during a Level 1 situation to support a large number of WFH employees. IT will also provide instruction on the use of the Cooperative e-mail system and other necessary programs and services from a remote location.

VI. COORDINATION/MONITORING

The Cooperative's Director of Risk Management will monitor information from the CDC and Texas HHSC for notification of activity. This should provide adequate lead time to prepare for arrival of the pandemic.

A significant increase in the level of contagious disease activity would be reported to

the General Manager and executive staff, who would then be responsible for determining if specific action related to the activation of a Level 2 or Level 3 response is required.

2. Protocols

Sick Leave	
Level 1	▪ Employees should not report for work if they show symptoms ▪ Employees should not report for work if a family member within the same household shows symptoms ▪ Employees should not return to work from an illness-related absence until they are symptom-free; a doctor's release is required
Level 2	▪ Supervisors encouraged to send sick individuals home
Level 3	▪ Consider modifications to sick leave and other relevant policies
Business Travel	
Level 1	▪ No changes
Level 2	▪ Employees should be cautioned concerning travel
Level 3	▪ Non-critical business travel suspended
Meetings	
Level 1	▪ No changes
Level 2	▪ Face-to-face meetings should be minimized
Level 3	▪ Face-to-face meetings suspended
Work from Home	
Level 1	▪ No changes
Level 2	▪ Employees approved for WFH would be allowed to do so
Level 3	▪ Employees approved for WFH would be encouraged to do so ▪ WFH employees would be expected to put in a normal work week and be available during normal business hours
Preparation	
☐ Identify potential WFH employees • Job function can be performed remotely • Employee has Internet access at home • Employee has a home PC or company-issued laptop	
☐ Train WFH employees on remote access to e-mail	
☐ Install VPN software and train employees in its use	
☐ Cross-train employees on critical business processes	
☐ Update restoration plans to address potential for 50% absenteeism	

When	Who	What
Level 1	Risk Management	▪ Initiate review of pandemic plan and recommend changes, as needed
Level 1	Executive Staff	▪ Develop and consider communications plan to educate employees about pandemic preparation efforts ▪ Identify critical business process plans ▪ Assess the need to purchase food or water
Level 1	Human Resources and Risk Management	▪ HR will prepare information to distribute to employees such as business cards with contact information for wallets and electronic email/phone notifications ▪ HR and Risk Management will educate employees on pandemic plan
Level 1	Information Technology	▪ Review configuration of remote access system and communicate any changes to employees ▪ Provide remote access training for potential WFH employees
Level 1	Risk Management	▪ Stock all restrooms and meeting rooms with hand sanitizer, and disinfectant spray ▪ Place placards and posters conveying prevention messages in all restrooms and meeting rooms

Level 2 or 3	Risk Management initiates	▪ Situational review with General Manager and staff ▪ If recommended by the CDC or Texas HHSC, medical screening of employees and/or public will be implemented to reduce potential exposure to infected individuals ▪ HR will implement the medical screening process as recommended ▪ Risk Management will provide kits for persons performing medical screening. The contents of the kits will follow the recommendation of health professionals. ▪ Information Technology will put into place door lock procedures for medical screening, virus lockdown, and initiate call center for employees to report illness. ▪ Medical Door screening for employees, contractors or any persons that will be conducting business at a local office will be conducted as follows: • NDO lobby • SDO lobby • Spur office lobby • Childress office lobby
Level 2 or 3	Director of Communications	▪ Director of Communications will provide status updates as they become necessary regarding the crisis. ▪ Changes in business operations will be communicated through Director of

		Communications to our members.
Level 2 or 3	Risk Management	▪ Prepare contact information for virus cleanup in the event it becomes necessary. This will be based on recommendations by the CDC or Texas HHSC. ▪ Prepare signs in the event of lockdown for all doors and place in company vehicles at various locations. This will be based on recommendations by the CDC or Texas HHSC.
Level 2 or 3	Information Technology	▪ Provide remote access for WFH employees
Level 2 or 3	Human Resources, Risk Management, and Engineering Manager	▪ Will communicate with employees and contractors regarding the potential pandemic preparation efforts.

I. OFFICE OPERATIONS

If a pandemic occurs all office operations will continue until it is determined that employees are at risk. Public access to the property may be denied pursuant to a determination by the General Manager.

The General Manager shall determine what alternatives will be carried out for essential business operations. Possible scenarios include:

Cashier

1. Employee will be required to wear proper PPE.
2. Limit access to drive through traffic only; no public access to facility.
3. Accept payments via electronic transmittance.

4. Employee may work from home.

Member Service Representatives

1. Employee will be required to wear proper PPE.
2. Accepting applications/payments for service via electronic transmittance.
3. Employee may work from home.

Other Office Services

1. Employee will be required to wear proper PPE.
2. Employee may work from home.

II. FIELD OPERATIONS

If a pandemic occurs all field operations will continue until it is determined that employees are at risk. The General Manager may limit or prohibit public access to Cooperative property.

The General Manager and executive staff will determine what alternatives will be carried out for essential business operations, however possible. Possible scenarios include:

1. Limited one-on-one exposure to members and public.
2. Use of PPE.
3. Employee may work from vehicle and/or home (where job duties allow).

III. CONTRACTOR OPERATIONS

If a pandemic occurs all contractor operations will continue until the General Manager and executive staff determines otherwise. The Director of Operations & Engineering will communicate as necessary with the contractor.

IV. FORMS AND FUTURE ACTION PLANS

Any forms and/or department action plans such as employees identified as critical and/or able to work from home will be attached to this plan as they become available.

D. ANNEX D – WILDFIRE MITIGATION PLAN

WILDFIRE MITIGATION PLAN

PURPOSE

- The intent of this plan is to outline the wildfire mitigation efforts of Lighthouse EC related to its overhead electrical distribution lines and associated equipment throughout its service territory.

PLAN

- Lighthouse's operations personnel will monitor weather conditions, county emergency management alerts and applicable state agency advisories regarding drought conditions and Red Flag warnings. Such sources include:

  Texas A&M Forest (www.texaswildfirerisk.com)

  Texas Forest Service (fire index ratings)

  USFS fire danger class

  NWS Red Flag warnings

  State Operations Center@tdem.texas.gov

- The following is a list of Emergency Service Agencies within or close to the Cooperative's serve area.

Briscoe County

Briscoe County Sheriff's Office
Phone: (806) 823-2135
Dispatch: (806) 995-3555

Silverton Volunteer Fire Dept.
Phone (806) 823-2125

Silverton EMS
Phone: (806) 823-2263

Quitaque VFD
Phone: (806) 455-1456

Quitaque EMS
Phone: (806) 455-1456

Childress County

Childress County Sheriff's Office
Phone: (940) 937-2535

Childress Fire Dept.
Phone: (940) 937-6562

Childress EMS
Phone: (940) 937-9169

Collingsworth County

Collingsworth County Sheriff's Office
Phone: (806) 447-5037

Wellington Fire Dept.
Phone: (806) 447-2588

Wellington EMS
Phone: (806) 447-2588

Cottle County

Cottle County Sheriff's Office
Phone: (806) 492-2145

Paducah VFD
Phone: (806) 492-3131

Paducah EMS
Phone: (806) 492-2336

Crosby County

Crosby County Sheriff's Office
Phone: (806) 675-7301

Crosbyton Fire Dept.
Phone: (806) 675-2301

Crosbyton EMS
Phone: (806) 675-2382

Lorenzo VFD
Phone: (806) 634-0153

Lorenzo EMS
Phone: (806) 634-5596

Ralls VFD
Phone: (806) 253-3503

Ralls EMS
Phone: (806) 253-1620

Dickens County

Dickens County Sheriff's Office
Phone: (806) 623-5533

Dickens Fire/EMS
Phone: (806) 271-4838

McAdoo VFD
Phone: (806) 657-7604

Spur VFD
Phone: (806) 271-3316

King County

Spur EMS
Phone: (806) 596-4111

Donley County

Donley County Sheriff's Office
Phone: (806) 874-3533

Clarendon VFD
Phone: (806) 874-3533

Clarendon EMS
Phone: (806) 874-2233

Hedley VFD
Phone: (806) 856-5241

Howardwick VFD
Phone: (806) 874-2222

Floyd County

Floyd County Sheriff's Office
Phone: (806) 983-4901

Floydada VFD
Phone: (806) 983-2834

Floydada EMS
Phone: (806) 983-3004

Lockney VFD
Phone: (806) 652-2841

Lockney EMS
Phone: (806) 652-2841

Dougherty VFD
Phone: (806) 983-4901

Hale County

Hale County Sheriff's Office
Phone: (806) 296-2724

Abernathy VFD
Phone: (806) 298-2233

Hale Center VFD
Phone: (806) 839-2419

Hale Center EMS
Phone: (806) 839-2419

Halfway VFD
Phone: (806) 889-3444

Petersburg Fire Dept.
Phone: (806) 667-3811

Petersburg EMS
Phone: (806) 667-3790

Plainview Fire Dept/EMS
Phone: (806) 296-1170

Hall County

Hall County Sheriff's Office
Phone: (806) 259-2151

Memphis Fire Dept.
Phone: (806) 259-2323

Hall County EMS
Phone: (806) 259-5059

Turkey VFD
Phone: (806) 423-1428

Lubbock County

Idalou VFD
Phone: (806) 892-2531

Idalou EMS
Phone: (806) 892-2531

New Deal VFD
Phone: (806) 746-6399

Motley County

Motley County Sheriff's Office
Phone: (806) 347-2234

Motley County VFD
Phone: (806) 347-2487

Motley County EMS
Phone: (806) 347-2340

Swisher County

Swisher County Sheriff's Office
Phone: (806) 995-3326

Happy VFD
Phone: (806) 558-2121

Kress VFD
Phone: (806) 684-2126

Kress EMS
Phone: (806) 995-2235

Tulia VFD
Phone: (806) 995-3547

Tulia EMS
Phone: (806) 995-2235

E. ANNEX E – HURRICANES

Not applicable. Lighthouse's service territory is not located near or within a hurricane evacuation zone, as defined by the Texas Division of Emergency Management.

F. ANNEX F – CYBERSECURITY

Incident Reporting and Response Plan

1 PURPOSE

The purpose of this Incident Reporting and Response Plan is to provide a process for Cooperative's formal, focused, and coordinated approach to responding to security events categorized as either cyber security or physical security incidents.

This Incident Reporting and Response Plan ensures that incidents are responded to in a systematic approach that is consistent with Cooperative's overall objectives and strategies. The plan ensures communication efforts to appropriate federal agencies, law enforcement agencies, shareholders, customers, and the media are defined, focused, and controlled. The plan will also ensure consistent incident handling and response and provides for future development and refinement of security controls.

2 SCOPE

The Incident Reporting and Response Plan (IRRP) is applicable to all personnel who have been identified to have direct or indirect assigned duties for Cooperative. Cooperative maintains physical and cyber security best practices. These best practices are based on the NIST Cybersecurity Framework.

3 GOALS

Cooperative works to promote resilience and enhance cyber security capabilities and works to convey current information on emerging cyber threats and initiatives, including critical infrastructure protection efforts, and realistic practices for improving operational resilience. The information technology team will keep cooperative members and staff informed while maintaining a working partnership amongst the various cooperative functional groups on matters of cyber security.

Short Term Goals:

- Identify gaps in cyber management practices and recommend process improvements.
- Reinforce cyber security best practices and examine resilience concepts and objectives.
- Discuss processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Share information with cooperative functional groups related to cyber security policies, initiatives, and capabilities.

Long Term Goals:

- Address gaps in cyber management practices and implement process improvements.

- Document a process to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- Enhance cyber incident response and business continuity capabilities.
- Increase the cybersecurity maturity and resilience of the cooperative.

4 ROLES AND RESPONSIBILITIES

This Incident Reporting and Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of Cooperative. All personnel are referred to as staff within this plan.

Below are details about the roles and responsibilities of each member of Cooperative to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

Attachment A lists the name of the person who currently holds each role/position.

4.1 Incident Response Lead

The Incident Response lead is responsible for:

- Making sure that the Security Incident Reporting and Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective.
- Making sure that the Security Incident Reporting and Response Plan is current, reviewed and tested at least once each year.
- Making sure that staff with Security Incident Reporting Response Plan responsibilities are properly trained at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Reporting and Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

4.2 Security Incident Response Team (SIRT)

The Security Incident Response Team (SIRT) is responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.

- Investigating and documenting each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

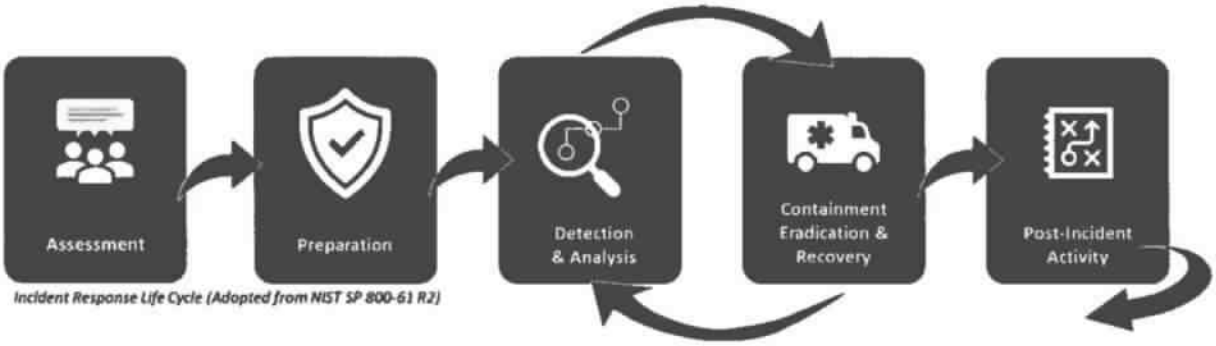
4.3 All Staff Members

All Staff Members are responsible for:

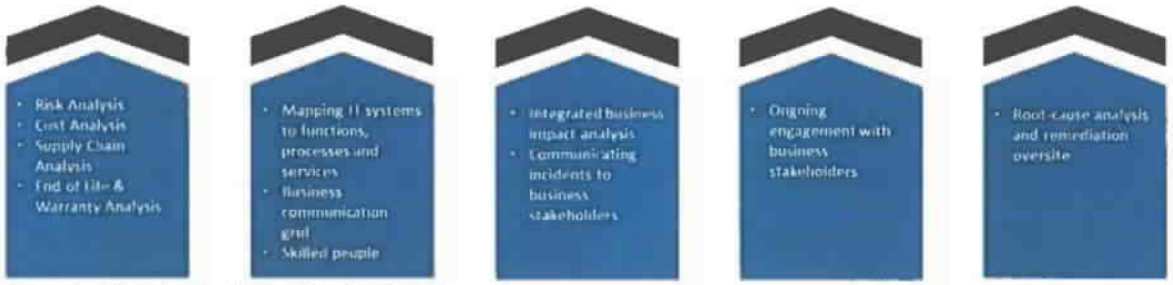
- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the IT Director.
- Reporting any security related issues or concerns to management, or to IT Director.
- Complying with the security policies and procedures of Cooperative.

5 INCIDENT RESPONSE LIFE CYCLE

This Incident Response Plan is designed to provide a Cooperative-wide, systematic business approach to the Incident Response Life Cycle. The Incident Response Life Cycle is paralleled with business operations to perform impact analysis.



Incident Response Life Cycle (Adopted from NIST SP 800-61 R2)



Integration with business operations to perform impact analysis

5.1 Life Cycle Objectives and Processes

5.1.1 Assessment

Establish an approach to analyze business impact and risk. Perform a risk analysis Cooperative wide and understand what assets and resources must be protected. Determine operational and financial risks that could impact business operations in the event of a security incident. Regularly review supply chain risk and vulnerability management assessments.

5.1.2 Preparation

Establish an approach to incident handling that includes development of policy and procedures. Review and codify an organizational security policy, perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Security Incident Response Team (SIRT).

5.1.3 Detection and Analysis

Analyze detection devices and reports from people to identify and classify the activity and begin handling the evidence. Monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents. When an incident is discovered, collect additional evidence, establish its type and severity, and document everything.

5.1.4 Containment

Ensure the impact of the incident does not increase. Perform short-term containment, for example by isolating the network segment that is under attack. Then focus on long-term

containment, which involves temporary fixes to allow systems to be used in production, while rebuilding clean systems.

5.1.5 Eradication

Determine the cause and remove it. Remove malware from all affected systems, identify the root cause of the attack, and take action to prevent similar attacks in the future.

5.1.6 Recovery

Restore the system to its original state and validate the clean system. bring affected production systems back online carefully, to prevent additional attacks. Test, verify and monitor affected systems to ensure they are back to normal activity.

5.1.7 Post-Incident Activity

Develop follow-up reports, identify lessons learned, and update procedures as necessary. No later than two weeks from the end of the incident, perform a retrospective of the incident. Prepare complete documentation of the incident, investigate the incident further, understand what was done to contain it and whether anything in the incident response process could be improved. In some instances, documentation may be needed for compliance requirements.

5.2 Integration of Business Operations

Develop a risk register which includes the systems and processes necessary to continue business operations and the impacts of each in the event systems are not available. The risk register should also include a list of contacts. The integration of business operations will assist incident handlers and stakeholders with identifying potential risks and associated services along the incident response life cycle. The risk register and contact lists should be kept as a hard copy for reference when systems are not available.

6 INCIDENT SCORING AND IMPACT RATING

Cooperative uses a weighted arithmetic mean to produce a score from zero to 10. This score drives the incident triage and escalation processes and assists in determining the prioritization of limited incident response resources and the necessary level of support for each incident.

(Current Functional Impact * 40%) + (Potential Functional Impact * 25%) + (Informational Impact * 10%) + (System Criticality *20%) + (Recoverability Timeframe * 5%) = The Incident Score

The five factors are assigned values between 0 and 10 based on value assigned the individual severity rating for each of the factors as described in this plan using the formula above.

The purpose of weighting the factors is to provide a repeatable formula that is heavily biased by the actual impact of the incident but also considers potential impacts to Cooperative if the incident were not contained guide appropriate actions with sufficient urgency to prevent a minor or moderate incident from escalating into an emergency.

7 Incident Categorization

7.1 CAT 1 UNAUTHORIZED ACCESS

Physical

1. Could the incident impact the reliability of the bulk power system?
2. Was there intentional damage to security systems that protect the physical perimeter.
3. Was sensitive information lost or removed without authorization. Was social engineering involved?

Cyber

1. Could the incident impact Cooperative? Was social engineering involved? Was sensitive information copied, transmitted, viewed, stolen or used by an unauthorized individual?
2. Was this an attempt to compromise Cooperative either electronically or physically? (report within 1 hour)

7.2 CAT 2 DENIAL OF SERVICE

1. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of the bulk power system?
2. Was social engineering involved?
3. If yes to any of these questions report to E-ISAC within the listed timeframe

7.3 CAT 3 MALICIOUS CODE

1. Was malicious software or data modification discovered on a cyber asset or assets that may impact the reliability of Cooperative?
2. Was social engineering involved?

7.4 CAT 4 IMPROPER USAGE

Was social engineering involved?

Did an unauthorized employee access confidential or restricted resources?

7.5 CAT 5 SCANS/PROBES/ATTEMPTED ACCESS/SURVEILLANCE/THREATS

Physical

1. Was this an attempt to compromise Cooperative either electronically or physically?
2. Was suspicious photo taking observed?
3. Were suspicious surveillance activities observed?
4. Was a suspicious fly over observed?
5. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
6. Were explosives discovered at or near a facility?

7. Were there suspected or actual attacks against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel?

7.6 CAT 6 INVESTIGATION

1. Could the incident impact the reliability of Cooperative?
2. Is there targeted, focused, or repetitive attempted access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability?
3. Was social engineering involved?
4. Was a threat communicated where the threatened action has the potential to damage or compromise facility or personnel?
5. Was this an attempt to compromise the bulk power system either electronically or physically?

8 INCIDENT REPORTING GUIDELINES

8.1 Reporting Forms (Internal)

Incidents are currently reported via email or by directly taking to the IT Director. Appropriate action is taken immediately upon notification.

8.2 Reporting Agency Forms (External)

8.2.1 Department of Energy (DoE)

Required Respondents (taken from the DoE website)

Electric utilities that operate as Control Area Operators and/or Reliability Authorities as well as other electric utilities, as appropriate, are required to file the form. The form is a mandatory filing whenever an electrical incident or disturbance is sufficiently large enough to cross the reporting thresholds. Reporting coverage for the Form DOE-417 includes all 50 States, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, and the U.S. Trust Territories.

Electric Disturbance Events (DOE-417)

Online Form: https://www.oe.netl.doe.gov/OE417/

Downloadable PDF Form: https://www.oe.netl.doe.gov/docs/OE417_Form_05312024.pdf

Offline Reporting: If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.

8.2.2 Electricity Information Sharing and Analysis Center (E-ISAC)

The Electricity Information Sharing and Analysis Center (E-ISAC) provides Cooperative an option to add a physical or cyber bulletin posting for information sharing purposes. An account must be created and approved for sharing information. Information shared may include details about a security incident attack and the Indicators of Compromise (IoC) to assist other cooperatives with mitigation of similar attacks.

E-ISAC website login: https://www.eisac.com

8.3 What to Include in your Incident Report

The following format is a guide. While internal reporting must be complete, some external reports may need to omit certain pieces of information to retain confidentiality. External reporting should be reviewed by managers, senior leadership, and sometimes legal counsel.

The following must be determined for each incident:

- Incident Type
- Names of system(s) involved (spell out each acronym used at its first use
- If the system has failed over to an available backup system
- Categorization of system(s) involved
- Type of data involved (Confidential or Restricted Information)
- Functional use of systems involved
- Identified or suspected cause of incident
- Identified or suspected impact of incident
- What dangers or effects on the facility or facility personnel safety may be caused by the event?
- If the incident has the potential to spread across other networks or even outside to partners or customers
- Investigation, containment, and remediation steps taken
- Incident detection/identification method
- Parties involved (include descriptive titles and names if required for remediation)
- Date and timeframe of occurrence(s)
- If the reported incident is real or a false positive
- What stage the incident is in—beginning, in process, or has already occurred
- What organizations will be affected and who should be part of the response.

If applicable, provide:

- Host-based indicators, Network indicators, and Email characteristics
- Security controls that blocked and/or detected the activity
- Date/time the activity was blocked and/or detected
- Host operating systems
- Name of malicious logic
- How did the exploit occur, and can it happen again? In what timeframe?
- What type of attacker tools if any were placed onto the system?
- Actions taken by affected system
- Network activity observed (including IPs and URLs connections made or attempted, associated ports)
- Type of unauthorized access attempted or obtained (including capabilities associated with that type of access)
- Attack vector

For incidents involving privacy or PII, also include:

- The number of individuals
- The number of records
- The number of data points or source of compromise

9 COMMUNICATIONS

9.1 Internal Reporting Chain

Cooperative's Internal Reporting Chain during an incident is based on the severity rating. If a member of the reporting chain is unavailable, their designated delegate will be contacted. If the both the primary and their delegate cannot be contacted, the next person in the chain will be notified. All members of the chain must select a delegate.

Severity	Reporting Guidance
Insignificant	Reporting is not necessary
Low	The IT Director who then decides whether or not to notify the General Manager.
Medium	The IT Director who then decides whether or not to notify the General Manager.
High	The IT Director who then notifies the General Manager. The IDT also informs other departments that have a need to know. At this severity level, the IDT will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.
Extreme	The Incident Response Lead will notify the IT Director who then notifies the President and Chief Executive Officer. The IDT also informs other departments that have a need to know. At this severity level, the ISM will establish a Virtual channel for incident handling activities understanding that Confidential or Restricted Information is not stored or shared via the channel.

9.2 External Reporting Chain

Name	Email	Phone
Department of Energy (DOE)	https://www.oe.netl.doe.gov/OE417/ FAX Form DOE-417 to (202) 586-8485 Email Form DOE-417 to doehqeoc@hq.doe.gov	(202) 586-8100

E-ISAC	operations@eisac.com	404-446-9780 #2
Federal Bureau of Investigation (FBI)	dallas.fbi.gov	972-559-5000
NCCIC (includes ICS-CERT and US-CERT)	central@cisa.gov Online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
ICS-CERT	soc@us-cert.gov online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
US-CERT	soc@us-cert.gov online form: https://us-cert.cisa.gov/forms/report	1-888-282-0870
Department of Homeland Security, Cyber Security Regional Contact	Chad Adams CISARegion6@hq.dhs.gov	1-888-282-0870

9.3 Key Vendor Contacts

Blue Layer IT in Lubbock, Texas

Golden Spread EC, Amarillo, Texas

9.4 Media Communications

Only employees authorized by the General Manager and his or her designee are permitted to speak to, give statements to, or participate in interviews with members of the news media as an official representative of the Cooperative.

By default, employees are not authorized by the General Manager to communicate with the news media as an official representative of the Cooperative and should refer any news media enquiries to an authorized employee.

9.5 Impaired Communications

Cooperative will identify another means to establish communications in the event that communications are disrupted. Cooperative will utilize cell phones, networks, the internet, etc.

10 FORENSICS

Cooperative, when deemed necessary to investigate possible criminal activity, will provide forensic services and it is not intended for law enforcement or to be court admissible. If it is determined that forensics be conducted, the cooperative shall require a dedicated evidence storage and analysis facilities with physical access limited to authorized forensics personnel, mobile evidence gathering tools required to establish chain of custody; to collect and label evidence at incident sites; and to securely package and transport the collected evidence. Cooperative shall: Develop, maintain, and follow a Standard Operating Procedure (SOP) for computer forensics collection and analysis follow Cooperative disclosure and privacy guidance and maintain a chain of custody of evidence. In the event that law enforcement services are required, the Incident Response Lead makes initial contact with senior leadership, legal and law enforcement organizations to establish evidentiary chain of custody. The Incident Response Lead will coordinate with appropriate law enforcement organizations. If necessary, Cooperative or the Incident Response Lead may package and ship equipment to a designated computer forensic processing facility. If it is determined that the source of the suspected criminal activity is external to Cooperative, the appropriate law enforcement organization will be notified immediately by the Incident Response Lead, or if necessary, by other organizations who will inform Cooperative at the earliest time possible.

11 TESTING AND PLAN CHANGES

The Incident Reporting and Response Plan will be reviewed and tested at least once every 24 calendar months for updates and improvements. Cooperative reserves the right to modify or amend this policy at any time, with or without prior notice. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response, lessons learned, or the absence of any lessons learned will be documented. The Incident Reporting and Response Plan will be updated and distributed to those individuals with a documented role and responsibility in the IRRP via email based on any documented lessons learned associated with the plan. If roles and responsibilities change or if there is a technology change that impacts Cooperative's ability to execute the plan, the Incident Reporting and Response Plan will be updated and each person with a defined role and responsibility in the IRP will be notified via email.

12 TRAINING REQUIREMENTS FOR INCIDENT RESPONSE TEAMS

Training requirements for the incident handlers includes:

- Intrusion Detection System training
- Security Information and Event Management training (if applicable)
- Ticketing/Reporting system
- Additional security monitoring and reporting tools as necessary
- Regular review of the Incident Response and Reporting Plan
- Cybersecurity Framework for all areas of Cooperative
- Communications applications (Teams, etc.)
- Practice with locating and filling our External Agency reports (DoE, E-ISAC, etc.)

13 ROADMAP FOR MATURING THE INCIDENT RESPONSE CAPABILITY

Cooperative will follow the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), to define their roadmap for maturity in Incident Reporting and Response Planning.

ATTACHMENT A – ASSIGNED ROLES

Role	Name(s)
Incident Response Lead	Tim Kendall, IT Director

ATTACHMENT B – Incident Response Plan Checklist

Response

Responding to security incidents can take several forms. Incident response actions may include triaging alerts from your endpoint security tools to determine which threats are real and/or the priority in which to address security incidents. Incident response activities can also include containing and neutralizing the threat(s)—isolating, shutting down, or otherwise "disconnecting" infected systems from your network to prevent the spread of the cyber attack. Additionally, incident response operations include eliminating the threat (malicious files, hidden backdoors, and artifacts) which led to the security incident.

- Immediately contain systems, networks, data stores and devices to minimize the breadth of the incident and isolate it from causing wide-spread damage.
- Determine if any sensitive data has been stolen or corrupted and, if so, what the potential risk might be to your business.
- Eradicate infected files and, if necessary, replace hardware.
- Keep a comprehensive log of the incident and response, including the time, data, location and extent of damage from the attack. Was it internal, external, a system alert, or one of the methods described previously? Who discovered it, and how was the incident reported? List all the sources and times that the incident has passed through. At which stage did the security team get involved?
- Preserve all the artifacts and details of the breach for further analysis of origin, impact, and intentions.
- Prepare and release public statements as soon as possible, describe as accurately as possible the nature of the breach, root causes, the extent of the attack, steps toward remediation, and an outline of future updates.
- Update any firewalls and network security to capture evidence that can be used later for forensics.
- Engage the legal team and examine compliance and risks to see if the incident impacts any regulations.
- Contact law enforcement if applicable since the incident may also impact other organizations. Additional intelligence on the incident may help eradicate, identify the scope, or assist with attribution.

Post-incident activities (Recovery and Follow-up actions) include eradication of the security risk, reviewing and reporting on what happened, updating your threat intelligence with new information about what's good and what's bad, updating your IR plan with lessons learned from the security incident, and certifying then re-certifying your environment is in fact clear of the threat(s) via a post-incident cybersecurity compromise assessment or security and IT risk assessment.

Recovery

- Eradicate the security risk to ensure the attacker cannot regain access. This includes patching systems, closing network access, and resetting passwords of compromised accounts.
- During the eradication step, create a root cause identification to help determine the attack path used so that security controls can be improved to prevent similar attacks in the future.
- Perform an enterprise-wide vulnerability analysis to determine whether any other vulnerabilities may exist.
- Restore the systems to pre-incident state. Check for data loss and verify that systems integrity, availability, and confidentiality has been regained and that the business is back to normal operations.
- Continue to gather logs, memory dumps, audits, network traffic statistics and disk images. Without proper evidence gathering, digital forensics is limited so a follow-up investigation will not occur.

Follow-Up

- Complete an incident response report and include all areas of the business that were affected by the incident.
- Determine whether management was satisfied with the response and whether the organization needs to invest further in people, training or technology to help improve its security posture.
- Share lessons learned. What went well, what didn't and how can procedures be improved in the future?
- Review, test and update the cybersecurity incident response plan on a regular basis, perhaps annually if possible.
- Conduct a compromise assessment or other security scans on a regular basis to ensure the health of systems, networks and devices.
- Update incident response plans after a department restructure or other major transition.
- Keep all stakeholders informed about the latest trends and new types of data breaches that are happening. Promote the message that "security is everyone's job."

ATTACHMENT C – Ransomware Attack Response and Prevention

Ransomware Attack Response Checklist

Step 1: Disconnect Everything

- ☐ Unplug computer from network
- ☐ Turn off any wireless functionality; Wi-Fi, Bluetooth, NFC

Step 2: Determine the Scope of the Infection, Check the Following for Signs of Encryption

- ☐ Mapped or shared drives
- ☐ Mapped or shared folders from other computers
- ☐ Network storage devices of any kind
- ☐ External Hard Drives
- ☐ USB storage devices of any kind (USB sticks, memory sticks, attached phones/cameras)
- ☐ Cloud-based storage: DropBox, Google Drive, OneDrive etc.

Step 3: Determine Ransomware Strain

- ☐ What strain/type of ransomware? For example: CyrptoWall, Teslacrypt etc.

Step 4: Determine Response

Ransomware response should be determined by a response team, senior leadership, and legal counsel at a minimum. In many cases, law enforcement may provide addition insight or suggestions. You may also want to call in a ransomware response team to assist with restoration.

Response 1: Restore your Files from Backup

1. Locate your backups
    - Ensure all files you need are there
    - Verify integrity of backups (i.e., media not reading or corrupted files)
    - Check for Shadow Copies if possible (may not be an option on newer ransomware)
    - Check for any previous versions of files that may be restored on cloud storage e.g., DropBox, GoogleDrive, OneDrive

2. Remove the ransomware from your infected system
3. Restore your files from backups
4. Determine infection vector and handle

Response 2: Try to Decrypt

1. Determine strain and version of the ransomware if possible
2. Locate a decryptor, there may not be one for newer strains; If successful, continue to next steps...
3. Attach any storage media that contains encrypted files (hard drives, USB sticks etc.)
4. Decrypt files
5. Determine the infection vector and handle

Response 3: Do Nothing (Lose Files)

1. Remove the ransomware
2. Backup your encrypted files for possible future decryption (optional)

Response 4: Negotiate and/or Pay the Ransom

- **If possible, you may attempt to negotiate a lower ransom and/or longer payment period**
- **Determine acceptable payment methods for the strain of ransomware: Bitcoin, Cash Card etc.**
- **Obtain payment, likely Bitcoin:**

  - Locate an exchange you wish to purchase a Bitcoin through (time is of the essence)
  - Set up account/wallet and purchase the Bitcoin

- **Re-connect your encrypted computer to the internet**
- **Install the TOR browser (optional)**
- **Determine the Bitcoin payment address. This is either located in the ransomware screen or on a TOR site that has been setup for this specific ransom case**
- **Pay the ransom: Transfer the Bitcoin to the ransom wallet**

- **Ensure all devices that have encrypted files are connected to your computer**
- **File decryption should begin within 24 hours, but often within just a few hours**
- **Determine infection vector and handle**

Step 5: Protecting yourself in the Future

- Implement Ransomware Prevention Checklist to prevent future attacks

Ransomware Prevention Checklist

First Line of Defense: End Users

- Implement effective security awareness training to educate users on what to look for to prevent criminal applications from being downloaded/executed.
- Conduct simulated phishing attacks to inoculate users against current threats.
- Require multi-factor authentication for all end user accounts, regular and administrative

Second line of Defense: Software

- Ensure you have and are using a firewall.
- Implement antispam and/or ant phishing. This can be done with software or through dedicated hardware.
- Ensure everyone in your organization is using top notch up-to-date antivirus software, or more advanced endpoint protection products like whitelisting and/or real-time executable blocking.
- Implement software restriction policies on your network to prevent unauthorized applications from running. (optional)
- Implement a highly disciplined patch procedure that updates any and all applications that have vulnerabilities.

Third Line of Defense: Backups

- Implement a backup solution: Software based, hardware based, or both.

- [ ] Ensure all possible data you need to access or save is backed up, including mobile/USB storage.
- [ ] Ensure your data is safe, redundant and easily accessible once backed up.
- [ ] Regularly test the recovery function of your backup/restore procedure. Test the data integrity of physical backups and ease-of-recovery for online/software based backups.

G. ANNEX G – PHYSICAL SECURITY INCIDENT

1. PURPOSE

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

In order to recognize a physical security event, one must understand what a physical security event is. For this procedure, the following definitions will be utilized:

Sabotage is defined as a deliberate action designed to disrupt or destroy any facilities, including, but not limited to, elements of the Bulk Electric System (BES). It can also be a deliberate action at weakening or destroying infrastructure through subversion.

Vandalism is defined as the malicious and deliberate defacement or destruction of property.

Criminal Mischief is defined as any damage, defacing, alteration, or destruction of tangible property with criminal intent.

Vandalism and Criminal Mischief can, and often do, go hand in hand with each other.

- **DEFINITION**

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

- **RECOGNITION**

All Cooperative personnel are responsible for following the reporting procedures in this section for any event that involves:

- Damage or destruction of facilities that results from actual or suspected intentional human action.
- Physical threats to Cooperative's personnel.
- Physical threats to a facility that have the potential to degrade the normal operation.

- Suspicious device or activity at a facility.
- Theft that has the potential to degrade operation

Determining what is truly Sabotage from Vandalism or Criminal Mischief can be a daunting task. The key to determining physical security is intent. If the intent is to disrupt or disable the BES, then the event would be considered Sabotage. Most events experienced by Cooperative are simply mischievous people or those with criminal intent. Below is a list of events that may possibly occur on Cooperative's system and the determination of the event status:

Sabotage Event	Criminal Mischief/Vandalism Event
Unbolting transmission tower legs (deliberate act to cause harm to the electric system and electric operations)	*A farmer who cuts a pole down due to blocking access to his fields (intent is access property not disrupt electric operations)*
Coordinated destruction of wooden structures (deliberate and coordinated attack to cause harm to the electric system and electric operations)	*Entry into a substation to steal copper conductor (intent is theft by taking, not disruption of electric operations)*
Shooting transmission facilities intending to cause destruction and electrical disturbances (typically multiple insulator strings along a stretch of line)	*Isolated shooting of a transmission line insulator (intent is criminal (destruction of property), not disruption of electric operations)*
Breaking and entering into a substation to destroy equipment (intent is to disrupt electric operations and cause harm to the BES and electric operations)	*Motor vehicle accident (consequence of action may be harm to the BES or electric operations; however, the intent was not to cause disruption)*
Driving a motor vehicle through a substation fence (substations are typically away from road rights of ways indicating an intentional action)	*Graffiti on equipment (while this indicates entry into station, the intent was not disruption and no physical damage was done to facilities)*
Deliberate cyber attack or cyber intrusion with intent to disrupt or take down SCADA network that could have a material impact on the BES	*Deliberate cyber intrusion with the intent of stealing personally identifiable information for the purposes of stealing Cooperative's personnel' identities for monetary gain*

Suspicious Activity, Objects, or Persons	
Threats to disrupt or damage Cooperative's electric system or other infrastructure	*Threats to injure Cooperative's personnel*
Intentional injury to Cooperative's personnel	*Unauthorized attempts to access Cooperative's facilities, such as a substation*
Unauthorized individuals present on Cooperative's property who exhibit suspicious behavior	*Unauthorized photography of Cooperative's facilities*

Unauthorized access or attempted access to the Cooperative's computer systems through physical or cyber intrusion	*Unknown persons loitering in the vicinity of Cooperative's facilities for extended periods of time*
Individuals, without proper identification or escort, and /or having unusual dress, appearance, or accents	*Unknown person calling Cooperative's facilities to ascertain security, personnel or procedural information*
Unknown persons who attempt to gain information about Cooperative's facilities by walking up to personnel or their families and engaging them in a conversation	*Theft of facility vehicles, personnel identification, uniforms or operating procedures*

- **REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY INCIDENT (COOPERATIVE FIRST RESPONDER)**

The Cooperative employee who discovers a possible or actual physical security event (First Responder) should take the following actions upon discovery if the Cooperative employee's safety is not at risk:

Actions Upon Discovery of a Possible or Actual Physical security Event (First Responder)
1. **Make sure the scene is safe for you and the public. Make the scene safe if possible.**
2. **Stay calm and quickly report to your Manager.**
3. **Make a clear and accurate report to your Manager. Provide your name and contact information.**
4. **Describe the possible or actual physical security act. Be as specific as possible.**
5. **Remain in contact with your Manager until released. Additional information may be requested.**
6. **Record any information about your surroundings including vehicles, people, or abnormal odors.**
7. **Remain available for further questions from law enforcement.**

If your personal safety is at risk, retreat to a safe area and contact your Manager as soon as possible. Notify law enforcement and emergency services for response to the scene. Keep the public away from the danger and evacuate area as necessary.

- **REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY (MANAGER)**

Once a possible or actual physical security event has been reported, the Manager shall inform all operating personnel of the possible or actual event. The Cooperative shall as soon as possible notify their Transmission Operator of the event and details. The Cooperative should provide the following information:

Information to Provide to Transmission Operator (see Appendix B for Physical Security Incident Information Form)
1. Geographic area and county affected/impacted.
2. Date and time incident began.
3. Date and time incident ended.
4. Did the incident originate at your Cooperative?
5. Amount of demand involved (estimated).
6. Number of member-consumers affected.
7. Physical or cyber attack.
8. Equipment involved in the event.
9. Description of events.
10. Station or line identifiers.

- **Roles**

Cooperative serve as First Responders for this procedure and must never ignore a suspected or actual act of physical security or suspicious person, object or activity that could threaten the Cooperative's facilities, personnel or operations. In addition, the Cooperative provides key information to their Transmission Operator to allow for timely and accurate reporting of possible or confirmed physical security events or subversive activities.

- **Training**

Cooperative shall review and perform training on this procedure at least annually.

ATTACHMENT A

Physical Security Incident Information Form

Cooperative: _____ **Facility:** _____

1. Date and time of incident: _____

2. Location of incident (e.g. county, city, line and station identifiers): _____

3. Type of incident (e.g. physical, cyber): _____

4. System parameters before the incident (Voltage, Frequency, Flows, Lines, Substations, etc.)

_____

5. System parameters after the incident: _____

6. Network configuration before the incident _____

7. Relay indications observed and performance of protection: _____

8. Damage to equipment: _____

9. Supplies interrupted and duration, if applicable: _____

10. Amount of electric service lost (demand/member-consumers), if applicable: _____

11. Estimate of time to return to service: _____

12. Cause of incident (if known): _____

13. Any other relevant information including notifications [and remedial action taken]: _

_____

_____

14. Recommendations for future improvement/repeat incident: _____

_____

Time:	
Date:	Signature and Designation of the Distribution Cooperative Person(s) Reporting the Incident

2. PURPOSE

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

In order to recognize a physical security event, one must understand what a physical security event is. For this procedure, the following definitions will be utilized:

Sabotage is defined as a deliberate action designed to disrupt or destroy any facilities, including, but not limited to, elements of the Bulk Electric System (BES). It can also be a deliberate action at weakening or destroying infrastructure through subversion.

Vandalism is defined as the malicious and deliberate defacement or destruction of property.

Criminal Mischief is defined as any damage, defacing, alteration, or destruction of tangible property with criminal intent.

Vandalism and Criminal Mischief can, and often do, go hand in hand with each other.

• DEFINITION

This document provides Cooperative personnel with the tools necessary to understand and identify a possible or actual local physical security event at Cooperative's facilities and immediately report suspicious activity or actual malicious destruction of any of their facilities. It addresses how personnel interact with each other and other entities to provide timely information and situational awareness.

• RECOGNITION

All Cooperative personnel are responsible for following the reporting procedures in this section for any event that involves:

- Damage or destruction of facilities that results from actual or suspected intentional human action.
- Physical threats to Cooperative's personnel.
- Physical threats to a facility that have the potential to degrade the normal operation.
- Suspicious device or activity at a facility.
- Theft that has the potential to degrade operation

Determining what is truly Sabotage from Vandalism or Criminal Mischief can be a daunting task. The key to determining physical security is intent. If the intent is to disrupt or disable the BES, then the event would be considered Sabotage. Most events experienced by Cooperative are simply mischievous people or those with criminal intent. Below is a list of events that may possibly occur on Cooperative's system and the determination of the event status:

Sabotage Event	Criminal Mischief/Vandalism Event
Unbolting transmission tower legs (deliberate act to cause harm to the electric system and electric operations)	*A farmer who cuts a pole down due to blocking access to his fields (intent is access property not disrupt electric operations)*
Coordinated destruction of wooden structures (deliberate and coordinated attack to cause harm to the electric system and electric operations)	*Entry into a substation to steal copper conductor (intent is theft by taking, not disruption of electric operations)*
Shooting transmission facilities intending to cause destruction and electrical disturbances (typically multiple insulator strings along a stretch of line)	*Isolated shooting of a transmission line insulator (intent is criminal (destruction of property), not disruption of electric operations)*
Breaking and entering into a substation to destroy equipment (intent is to disrupt electric operations and cause harm to the BES and electric operations)	*Motor vehicle accident (consequence of action may be harm to the BES or electric operations; however, the intent was not to cause disruption)*
Driving a motor vehicle through a substation fence (substations are typically away from road rights of ways indicating an intentional action)	*Graffiti on equipment (while this indicates entry into station, the intent was not disruption and no physical damage was done to facilities)*
Deliberate cyber attack or cyber intrusion with intent to disrupt or take down SCADA network that could have a material impact on the BES	*Deliberate cyber intrusion with the intent of stealing personally identifiable information for the purposes of stealing Cooperative's personnel' identities for monetary gain*

Suspicious Activity, Objects, or Persons	
Threats to disrupt or damage Cooperative's electric system or other infrastructure	*Threats to injure Cooperative's personnel*
Intentional injury to Cooperative's personnel	*Unauthorized attempts to access Cooperative's facilities, such as a substation*
Unauthorized individuals present on Cooperative's property who exhibit suspicious behavior	*Unauthorized photography of Cooperative's facilities*

Unauthorized access or attempted access to the Cooperative's computer systems through physical or cyber intrusion	*Unknown persons loitering in the vicinity of Cooperative's facilities for extended periods of time*
Individuals, without proper identification or escort, and /or having unusual dress, appearance, or accents	*Unknown person calling Cooperative's facilities to ascertain security, personnel or procedural information*
Unknown persons who attempt to gain information about Cooperative's facilities by walking up to personnel or their families and engaging them in a conversation	*Theft of facility vehicles, personnel identification, uniforms or operating procedures*

- **REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY INCIDENT**

(COOPERATIVE FIRST RESPONDER)

The Cooperative employee who discovers a possible or actual physical security event (First Responder) should take the following actions upon discovery if the Cooperative employee's safety is not at risk:

Actions Upon Discovery of a Possible or Actual Physical security Event (First Responder)
8. **Make sure the scene is safe for you and the public. Make the scene safe if possible.**
9. **Stay calm and quickly report to your Manager.**
10. **Make a clear and accurate report to your Manager. Provide your name and contact information.**
11. **Describe the possible or actual physical security act. Be as specific as possible.**
12. **Remain in contact with your Manager until released. Additional information may be requested.**
13. **Record any information about your surroundings including vehicles, people, or abnormal odors.**
14. **Remain available for further questions from law enforcement.**

If your personal safety is at risk, retreat to a safe area and contact your Manager as soon as possible. Notify law enforcement and emergency services for response to the scene. Keep the public away from the danger and evacuate area as necessary.

- **REPORTING POSSIBLE OR ACTUAL PHYSICAL SECURITY (MANAGER)**

Once a possible or actual physical security event has been reported, the Manager shall inform all operating personnel of the possible or actual event. The Cooperative shall as soon as possible notify their Transmission Operator of the event and details. The Cooperative should provide the following information:

Information to Provide to Transmission Operator (see Appendix B for Physical Security Incident Information Form)
11. Geographic area and county affected/impacted.
12. Date and time incident began.
13. Date and time incident ended.
14. Did the incident originate at your Cooperative?
15. Amount of demand involved (estimated).
16. Number of member-consumers affected.
17. Physical or cyber attack.
18. Equipment involved in the event.
19. Description of events.
20. Station or line identifiers.

- **Roles**

Cooperative serve as First Responders for this procedure and must never ignore a suspected or actual act of physical security or suspicious person, object or activity that could threaten the Cooperative's facilities, personnel or operations. In addition, the Cooperative provides key information to their Transmission Operator to allow for timely and accurate reporting of possible or confirmed physical security events or subversive activities.

- **Training**

Cooperative shall review and perform training on this procedure at least annually.

ATTACHMENT A
Physical Security Incident Information Form

Cooperative: _____ **Facility:** _____

1. Date and time of incident: _____

2. Location of incident (e.g. county, city, line and station identifiers): _____

3. Type of incident (e.g. physical, cyber): _____

4. System parameters before the incident (Voltage, Frequency, Flows, Lines, Substations, etc.)

_____

5. System parameters after the incident: _____

6. Network configuration before the incident _____

7. Relay indications observed and performance of protection: _____

8. Damage to equipment: _____

9. Supplies interrupted and duration, if applicable: _____

10. Amount of electric service lost (demand/member-consumers), if applicable: _____

11. Estimate of time to return to service: _____

12. Cause of incident (if known): _____

13. Any other relevant information including notifications [and remedial action taken]: _

_____

_____

14. Recommendations for future improvement/repeat incident: _____

_____

Time:	
Date:	Signature and Designation of the Distribution Cooperative Person(s) Reporting the Incident

H. ANNEX H: REQUIREMENTS FOR TRANSMISSION AND DISTRIBUTION UTILITIES

Not Applicable. Cooperative is not a Transmission and Distribution Utility as defined under 16 TAC §25.5.

VII. REQUIREMENTS FOR GENERATORS.

Not applicable. Cooperative does not operate generation assets as defined in 16 Texas Administrative Code § 25.5 (33).

VIII. REQUIREMENTS FOR RETAIL ELECTRIC PROVIDERS

Not applicable. Cooperative is not a Retail Electric Provider as defined under 16 TAC §25.5.

IX. ANNEX H REQUIREMENTS FOR ERCOT

Not applicable. Requirements apply exclusively to ERCOT.

APPENDIX A. EMERGENCY CONTACTS

EMERGENCY CONTACTS, MEDIA AND SCHOOL

EMERGENCY CONTACTS

Albert Daniel, General Manager

Danny Nixon, Operations Manager

Johnny Gourdon, Line Superintendent

DESIGNATED SPOKESPERSON

Mike Green, Member Services Manager

Albert Daniel, General Manager

Brad Jackson, Safety & Training Coordinator

RADIO

KFLP Floydada (806) 983-5704

KLSR Memphis (806) 259-3511

KKYN Plainview (806) 291-0123

KLLL Lubbock (806) 762-3000

TV

KCBD Channel 11, Lubbock (806) 744-1414

Fox 34 News, Lubbock (806) 745-3434

KAMC Channel 28, Lubbock (806) 745-2345

KFDA Channel 10, Amarillo (806) 383-1010

KVII ABC 7, Amarillo (806) 373-1787

KAMR TV 4, Amarillo (806) 383-3321

NEWSPAPERS

Floyd County Hesperian Beacon – Floyd County

Plainview Herald – Hale County

Caprock Courier – Silverton, Quitaque, Turkey. Flomot, Matador, Roaring Springs, Paducah and Guthrie, Texas

The Valley Tribune – Briscoe County, Hall County, and Motley County

The Red River Sun – Memphis, Wellington, and Childress, Texas

Crosby County News – Crosby County

Facebook Page – https://www.facebook.com/ligthouseelectriccooperative

Webpage – www.lighthouse.coop

SCHOOLS

Turkey-Quitaque ISD (806) 455-1411

APPENDIX B. REPORTING TO THE DOE AND PUCT

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.

RESPONSE DUE:
Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met.
Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met.
By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. *Note: 4:00pm local time will be considered the end of the business day*

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident. For NERC reporting entities registered in the United States: NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE
(Retain a completed copy of this form for your files.)

Online: Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/
FAX: FAX Form OE-417 to the following facsimile number: (202) 586-8485.
Alternate: If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply)
See Instructions For More Information

EMERGENCY ALERT **File within 1-Hour** If any box 1-8 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on Line A below.	1. [ ] Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. [ ] Cyber event that causes interruptions of electrical system operations 3. [ ] Complete operational failure or shut-down of the transmission and/or distribution electrical system 4. [ ] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system 5. [ ] Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident 6. [ ] Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 7. [ ] System-wide voltage reductions of 5 percent or more 8. [ ] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System
NORMAL REPORT **File within 6-Hours** If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on Line A below.	9. [ ] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems 10. [ ] Cyber event that could potentially impact electric power system adequacy or reliability 11. [ ] Loss of electric service to more than 50,000 customers for 1 hour or more 12. [ ] Fuel supply emergencies that could impact electric power system adequacy or reliability

SCHEDULE 1 -- ALERT CRITERIA -- CONTINUED

(Page 2 of 4)

SYSTEM REPORT
File within 1-Business Day

If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident OR by the end of the next business day. *Note:* 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert Status) on Line A below.

13. [ ] Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a Bulk Electric System Emergency.

14. [ ] Damage or destruction of its Facility that results from actual or suspected intentional human action.

15. [ ] Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility, Or suspicious device or activity at its Facility.

16. [ ] Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.

17. [ ] Bulk Electric System Emergency resulting in voltage deviation on a Facility: A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes

18. [ ] Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts

19. [ ] Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.

20 [ ] Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements

21 [ ] Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing)

22 [ ] Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more

23 [ ] Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more.

24 [ ] Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.

If significant changes have occurred after filing the initial report, re-file the form with the changes and check Update (for the Alert Status) on Line A below.

The form must be re-filed within 72 hours of the incident with the latest information and Final (Alert Status) checked on Line A below, unless updated

LINE NO.						
A.	Alert Status (check one)	Emergency Alert [ ] 1 Hour	Normal Report [ ] 6 Hours	System Report [ ] 1 Business Day	Update [ ] As required	Final [ ] 72 Hours
B.	Organization Name					
C.	Address of Principal Business Office					

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2022 Burden Per Response: 1.8 hours

SCHEDULE 1 – ALERT NOTICE
(Page 3 of 4)

INCIDENT AND DISTURBANCE DATA

D.	Geographic Area(s) Affected (County, State)			
E.	Date/Time Incident Began (mm-dd-yy/hh:mm) using 24-hour clock	___ - ___ - ___ / ___ : ___ mo dd yy hh mm	[ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] Alaska [ ] Hawaii	
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	___ - ___ - ___ / ___ : ___ mo dd yy hh mm	[ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] Alaska [ ] Hawaii	
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes [ ]	No [ ]	Unknown [ ]
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero [ ]	Unknown [ ]
I.	Estimate of Number of Customers Affected		Zero [ ]	Unknown [ ]

SCHEDULE 1 – TYPE OF EMERGENCY
Check all that apply

J. Cause	K. Impact	L. Action Taken
❑ Unknown ❑ Physical attack ❑ Threat of physical attack ❑ Vandalism ❑ Theft ❑ Suspicious activity ❑ Cyber event (information technology) ❑ Cyber event (operational technology) ❑ Fuel supply emergencies, interruption, or deficiency ❑ Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure ❑ Transmission equipment failure (not including substation or switchyard) ❑ Failure at high voltage substation or switchyard ❑ Weather or natural disaster ❑ Operator action(s) ❑ Other ❑ Additional Information/Comments:	❑ None ❑ Control center loss, failure, or evacuation ❑ Loss or degradation of control center monitoring or communication systems ❑ Damage or destruction of a facility ❑ Electrical system separation (islanding) ❑ Complete operational failure or shutdown of the transmission and/or distribution system ❑ Major transmission system interruption (three or more BES elements) ❑ Major distribution system interruption ❑ Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more ❑ Loss of electric service to more than 50,000 customers for 1 hour or more ❑ System-wide voltage reductions of 3 percent or more ❑ Voltage deviation on an individual facility of ±10% for 15 minutes or more ❑ Inadequate electric resources to serve load ❑ Generating capacity loss of 1,400 MW or more ❑ Generating capacity loss of 2,000 MW or more ❑ Complete loss of off-site power to a nuclear generating station ❑ Other ❑ Additional Information/Comments:	❑ None ❑ Shed Firm Load. Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) ❑ Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system ❑ Implemented a warning, alert, or contingency plan ❑ Voltage reduction ❑ Shed Interruptible Load ❑ Repaired or restored ❑ Mitigation implemented ❑ Other ❑ Additional Information/Comments

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2011 Burden Per Response: 1.5 hours

SCHEDULE 2 – NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION		
M.	Name	
N.	Title	
O.	Telephone Number	( )
P.	FAX Number	( )
Q.	E-mail Address	

Provide a description of the incident and actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Be sure to identify: the estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can be supplied to meet the requirement; this includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 needs to be filed. Check the Final box on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours after detection that a criterion was met.

R. Narrative:

S. Estimated Restoration Date for all Affected Customers Who Can Receive Power	- - mo dd yy

T. Name of Assets Impacted	

U. Notify NERC/E-ISAC	Select if you approve of all of the information provided on the Form being submitted to the North American Electric Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-ISAC) NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards. If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemsreliability@nerc.net and/or operations@esisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC. ☐ Notify NERC ☐ Notify E-ISAC

Public Utility Commission

EVENT REPORTING FORM

1. Event Name:_____

2. Utility Reporting:_____

3. Date of Report: _____ 4. Time of Report:_____

5. Reporting Contact:_____ 6. Title:_____

7. Contact Number:_____

8. Counties Involved:_____

9. Cities Involved:_____

10. Customers Out of Service/Affected:_____

11. Total Customers on System by County:_____

_____

12. Estimated Restoration Date and Time:_____

_____

13. Requests for Help:_____

_____

_____

14. Major Feeders, Substations, and Facilities Out of Service:_____

_____

_____

15. Area Affected – Explanation of Outages:_____

_____

_____

_____

_____

_____

_____

_____

APPENDIX C. EMERGENCY SUPPLIES

Emergency Supplies List

At each Cooperative facility, it will be the responsibility of the facility/site manager to maintain a cache of emergency supplies for use in periods of severe weather likely to result in power outages or facility damage.

The responsible Cooperative manager will ensure that those items with a shelf life, such as batteries, are replaced on an appropriate schedule.

The following are the minimum emergency supplies that will be kept at each Cooperative site. Additional items may be listed in operations and engineering procedures.

- Duct tape
- 10 Flashlights
- Flashlight batteries (4 sets for each flashlight)
- Rain ponchos
- Plastic tarps or sheeting
- Staple gun
- Bungee cords
- Rope
- Backup generator fuel (as appropriate)
- 2-way radios
- Large trash bags with ties
- Leather gloves

APPENDIX D. RESTORATION PERSONNEL SUPPLIES

- Ice chest(s) 48 Quart or Larger
- Drinking Water Cooler
- Gator Aid or Squelcher
- Bottled water
- Insect Repellent & Sun Screen
- Fully supplied First Aid Kit & BBP kit
- Work Zone Protection Signs, Vest, & Traffic Cones
- Trucks fully stocked with tools
- Live Line tools, rubber goods
- Lights & extra batteries or chargers
- Generator or Inverter for Small Microwave and Charging Lights, Batteries
- Outrigger Pads
- Personal Grounds
- All Personal Protective Equipment
- Climbing Tools & Hand tools
- Overshoes & Rainwear
- Drinks, Snacks, Canned Foods
- Personal Hygiene Products
- FR Uniforms & Clothing for 7 Days
- Extra Boots
- Cash, Phone card
- Prescribed Medicine, Enough for 7 Days

APPENDIX E. FORM FOR REQUESTING ASSISTANCE

Cooperative requesting emergency assistance: _____
Telephone
number(s):_____
(Use headquarters town name)
Nature of disaster: _____
Number and type of trucks needed: _____
Other equipment and tools needed:

_____
_____
_____
_____
Personnel and classifications needed: _____
Materials needed: _____
Weather and road conditions: _____
Where crews should report and to whom: _____
Estimate of how long the help may be needed: _____
How to contact your cooperative during the emergency: _____
Name of person to receive this information: _____
Date: _____Time:_____

APPENDIX F. MEMORANDUM OF UNDERSTANDING

Responsibilities of Cooperative(s) receiving assistance:

1. Plan the organization of all help and integrate all assistance with its own personnel and facilities.
2. Provide each crew with a map or information, showing the area to which they have been assigned, source of supply, direction of feed and location of sectionalizing equipment.
3. Provide a representative from the cooperative to perform necessary liaison for each crew or group of units operating together.
4. Provide procedures to properly account for materials used and retired, hours worked by employees.
5. Maintain contact with all units. All dispatching should be directed by person or persons who are thoroughly acquainted with the system in the affected area.
6. Prescribe the number of hours to be worked, however, it is recommended no more than 16 hours in a 24-hour period.
    a. Time begins when Crews enter vehicles to begin the day, including all meals, and ends when they arrive back at place of lodging.
    b. Travel time to and returning from Cooperative receiving assistance.
7. Provide sleep accommodations for assisting personnel and pay for all lodging. (Personnel may be required to share a motel room with two double beds.)
8. Damages and breakdown repair costs of vehicles remain the responsibility of the assisting Cooperative that owns vehicles.
9. Provide or reimburse for all meals (Breakfast, Lunch, and Supper) If crews need to purchase meals while assisting with repairs, they will keep receipts to be turned in to their cooperative for reimbursement.
10. Provide or reimburse for all fuel used by crew vehicles while assisting in restoration and repairs. (If Cooperative receiving assistance does not have fueling facilities, assisting crew may have to fuel vehicles at commercial facilities, they will keep receipts to be turned in to their cooperative for reimbursement.
11. Provide assisting Cooperative personnel laundry service when needed.

Responsibilities of Assisting Cooperative:

1. Dispatch properly-trained and equipped personnel and equipment in good working condition
2. Inform its own personnel of all aspects of its agreement.
3. Provide workers' compensation insurance coverage for injuries sustained by assisting personnel, wherever such injuries might occur.

4. Ensure that each employee leaving home to assist another has sufficient cash or cooperative credit card or incidental expenses. Instruct crew to keep all receipts and turn them in to their cooperative when they have returned home, for reimbursement.
5. Bill the cooperative requesting aid for the total actual payroll costs of the assisting personnel at the time and a half rate for all hours worked. Will not bill for transportation costs or overhead cost.

Resources possibly provided by assisting Cooperatives

1. Line personnel with all necessary equipment (preferably Line/Crew Forman, Journeymen, Apprentice, Groundmen and/or Digger-Operator.
2. Staking technicians with vehicle, laptop, tablet, iPad etc., and staking software if compatible.
3. Warehouse personnel
4. Vehicle Mechanics
5. Member Services Personnel

Golden Spread Electric Cooperative, Inc: will serve as primary point of contact for Cooperative requesting assistance. They will get information out to all Cooperative Systems participating in this Memorandum of Understanding.

Compensation for Assisting Personnel working Out of State

For out-of-state work, all personnel will also receive wages at one and one-half times their regular hourly rate for all labor hours worked.

The following Electric Cooperatives agree to and support implementation of the Memorandum of Understanding as a guide and agreement for providing personnel and equipment during Mutual Aid for storm or natural disaster restoration.

1. Bailey County Electric Cooperative Association
2. Big Country Electric Cooperative, Inc.
3. Coleman County Electric Cooperative, Inc.
4. Concho Valley Electric Cooperative, Inc.
5. Deaf Smith Electric Cooperative, Inc.
6. Greenbelt Electric Cooperative, Inc.
7. Lamb County Electric Cooperative, Inc.
8. Lea County Electric Cooperative, Inc.
9. Lighthouse Electric Cooperative, Inc.

10. Lyntegar Electric Cooperative, Inc.
11. North Plains Electric Cooperative, Inc.
12. Rita Blanca Electric Cooperative, Inc.
13. South Plains Electric Cooperative, Inc.
14. Southwest Texas Electric Cooperative, Inc.
15. Swisher Electric Cooperative, Inc.
16. Taylor Electric Cooperative, Inc.
17. TCEC (Tri-County Electric Cooperative, Inc.)
18. Golden Spread Electric Cooperative, Inc.

APPENDIX G. MUTUAL AID AGREEMENT

In consideration of the mutual commitments given herein, each of the Signatories to this Mutual Aid Agreement agrees to render aid to any of the Signatories as follows:

1. Request for aid. The Requesting Signatory agrees to make its request in writing to the Aiding Signatory within a reasonable time after aid is needed and with reasonable specificity. The Requesting Signatory agrees to compensate the Aiding Signatory as specified in this Agreement and in other agreements that may be in effect between the Requesting and Aiding Signatories.
2. Discretionary rendering of aid. Rendering of aid is entirely at the discretion of the Aiding signatory. The agreement to render aid is expressly not contingent upon a declaration of a major disaster or emergency by the federal government or upon receiving federal funds.
3. Invoice to the Requesting Signatory. Within 90 days of the return to the home work station of all labor and equipment of the Aiding Signatory, the Aiding Signatory shall submit to the Requesting Signatory an invoice of all charges related to the aid provided pursuant to this Agreement. The invoice shall contain only charges related to the aid provided pursuant to this Agreement.
4. Charges to the Requesting Signatory. Charges to the Requesting Signatory from the Aiding Signatory shall be as follows:
   a) Labor force. Charges for labor force shall be in accordance with the Aiding Signatory's standard practices.
   b) Equipment. Charges for equipment, such as bucket trucks, digger derricks, and other special equipment used by the aiding Signatory, shall be at the reasonable and customary rates for such equipment in the Aiding Signatory's locations.
   c) Transportation. The Aiding Signatory shall transport needed personnel and equipment by reasonable and customary means and shall charge reasonable and customary rates for such transportation.
   d) Meals, lodging and other related expenses. Charges for meals, lodging and other expenses related to the provision of aid pursuant to this Agreement shall be the reasonable and actual costs incurred by the Aiding Signatory.
5. Counterparts. The Signatories may execute this Mutual Aid Agreement in one or more counterparts, with each counterpart being deemed an original Agreement, but with all counterparts being considered one Agreement.
6. Execution. Each party hereto has read, agreed to and executed this Mutual Aid Agreement on the date indicated.

Date _____ Entity _____

By _____

Title _____

APPENDIX H. ENGINEERING AND OPERATIONS PROCEDURES

1. Engineering departments should develop and submit to management and boards of directors a policy concerning specific pole and conductor sizes and other items to be used in a "Standard Construction Policy." Co-op staking sheets and work plans may be used as examples to show proof of a "replacement standard" being in place prior to the occurrence of a natural disaster.
2. Engineering and operations personnel should note the date and time the first outage occurred due to the disaster, and the date and time the last consumer's electricity is restored.
3. The engineering/operations department should solicit at least three (3) bids for permanent repair work to be done, preferably before the conclusion of the 70-hour Emergency Protective Measures period. Bids from contractors must be received, along with price sheets for storm labor and equipment. It is recommended that bids be made on a per-unit basis, rather than hourly. However, if billing is hourly, proof must be shown that the contractor was supervised by the cooperative, complete with daily notes and documentation.
4. It is strongly recommended that additional engineering resources be arranged to assist in the daily development of staking sheets, material sheets, and work order information. This will allow the staking department to stay ahead of construction crews, and provides for an orderly flow of necessary and vital information to other key departments.
5. Member donated items, such as food, services and labor, must be well documented. It may be necessary for the member or group providing these items to sign an affidavit listing the cost of donated items, or for an invoice to be provided. This could then be included in Administrative Expense by the cooperative.
6. Prepare staking sheets as soon as possible for work to be done. Make sure that all permanent work has a staking sheet documenting the completed work. The labor for making the staking sheets should be included in the work order and is FEMA reimbursable (Category F). <u>The labor involved in looking for and estimating damage to the system **is not** reimbursable **except** as Administrative Expense</u>.
7. Damage surveys: It is strongly recommended that, if possible, co-op personnel resist the urge to send all available human resources into the field to assist in the repair of damage. Instead, the following is advised:
    a. Send several experienced field personnel on a 'Fast Survey' of the areas in which damage is suspected. Use enough personnel to drive through the damaged area(s) in one day or less.
    b. Initially, some lineman may need to be utilized to patrol line rather than to repair it. The Fast Survey is designed to rapidly determine the extent of damage throughout the co-ops' system. It will allow for better decision-making concerning crews, materials and equipment.
    c. Damage reports from survey personnel should list the location, approximate length (1 mile, etc.) of damage in area, the type of damaged pole line, i.e., "south side of

section 23, T15N, R1W – One mile of 3 phase line, 1/0 conductor on 45-foot, Class 4 poles is down."

d. Collect all reports during the survey at the dispatch center or Emergency Operations Center and draw the damaged locations on a Key Map. Start a database using Excel or Access software to log each of the damage reports by line section or map location number. This will help the engineering and operations departments document the scope and location of the damage for later accounting purposes.
e. If possible, allow survey teams to use cell phones to report damage; designate someone to log these reports onto the Key Map and also log the reports into the database. This is also the time to note the locations of any lines that may be blocking major roadways, since main roads will need to be cleared quickly.
f. Do not allow survey teams to stop and draw staking sheets or to make detailed material sheets during the initial Fast Survey. The goal is to rapidly drive through the damage area(s) to determine the extent and locations of damage. The information gathered will then be used to determine crew and material requirements. The earlier the co-op gets a handle on the extent of the damage, the earlier proper staking sheets can be developed for known damage locations.

8. Beginning repairs: Concentrate on the areas that will allow the cooperative to get power restored to the most consumers with the least amount of work, and to critical loads, if any. Begin work at substations and work main feeder lines outward from that point. If damage is extensive in an area, staking technicians may need to be sent ahead of repair crews in order to draw staking sheets and set stakes. Identify in advance all feeder lines and critical loads.
9. Some lines can be repaired with little or no staking; others will have to be staked as if they are new construction. In the case of strong tornadoes or hurricanes, the pole line may be completely obliterated, with no poles left for reference points. In these cases, the line may have to be completely re-staked prior to reconstruction.
10. Ice storms, on the other hand, may break poles down, but type of framing and original hole locations will still be known. Repair crews can reset new poles in these instances without staking sheets or stakes, unless the damage involves Codes and Standards changes, which may necessitate re-staking due to changes in ruling spans being made for proper clearance purposes.
11. Quick staking sheet drawings listing pole framing requirements are very helpful for repair crews, but in ice storms, with a visible pole line in place, it may not be necessary for staking technicians to 'wheel off' spans or set stakes. Whether damage is caused by an ice storm, hurricane or tornado, staking teams will have to coordinate with repair crews, and vice-versa.
12. Inspect and document the repairs: Once repairs are underway, use engineering personnel to inspect completed repair locations. Consider using consultants or additional engineering help from neighboring co-ops. Engineering teams will have to look for all poles and construction units that were set or replaced during the disaster. Some repairs may have been made without benefit of written records; the purpose of the engineering follow-up inspection is to further document repair locations and materials used.
13. The second purpose of the inspection is similar to work order inspections. List the material units used at each damaged pole location, noting any cleanup or corrections that may be

required in order to bring the line into compliance with current co-op, RUS and NESC Codes and Standards.

14. For Category F, Utility (permanent repairs), it is extremely important to have in place board-approved co-op design standards and staking tables. This customized "Standard Construction Policy" should spell out standard pole heights, conductor sizes and ruling spans to be used at the cooperative, and should be utilized every day by co-op staking personnel.
15. The third purpose of the inspection is to have engineers check surrounding areas for damaged lines possibly overlooked during the initial Fast Survey. Some lines may serve idle or seasonal services and should be closely evaluated for rebuild or retirement.
16. Inspection notes must be detailed and listed by map location number. The notes should be entered into a database for easy retrieval and subsequent evaluation. Documentation of all work performed during the disaster is a major task, but is absolutely critical if a cooperative expects to qualify and receive FEMA reimbursement. These records will be used to ensure the system is returned to current Codes and Standards, and to help document material and labor costs associated with all reconstruction efforts.
17. Contracts from contractors: The co-op must have in place, or be prepared to receive from at least three (3) different sources, bids for permanent repairs. This is preferable during the 70-hour Emergency Protective Measures period immediately following the disaster. During the initial emergency period, if a contract has not been signed by the contractor, any record of contact, arrival times, and/or anything discussed by phone or in person with the contractor should be documented. OIG auditors may allow these costs from contractors, but only if the co-op proves such verbal agreement existed via documentation.
18. Contractors unfamiliar with local co-op service areas will require supervision and instruction by local co-op employees. It is suggested that trained and experienced employees be used to supervise these contractor crews, such as those employees from the co-op's staking department, marketing department, or key accounts department.
19. If predicted storms appear to be extremely destructive in nature (forecasted ice storms, hurricanes, or tornado outbreaks), consider creating work orders in advance to charge all time and materials to.
20. If possible and if needed, use in-house contractors and any of their extra crews before calling in or bidding other contract crews. In-house crews are contractors the cooperative presently employs for contract construction work. Make sure the in-house contractor has their emergency storm repair rates on file with the cooperative, as well as rates for permanent repairs.
21. Keep **all** receipts during the event, in case the storm or event is later declared a federal disaster.
22. Work Orders: Some co-ops prefer to make one work order per disaster. Counties (or parishes, etc.) are designated with map location numbers noted on all time sheets, staking sheets and material sheets.
23. On-file contracts: Some co-ops retain contracts and keep them on file from contractors. Included in those contracts is a sheet pertaining to emergency storm work. However, it is usually a good practice to call in contractors within the first 24 to 36 hours of the disaster if

damage warrants their assistance. Again, bids for repairs should be let during the 70-hour Emergency Protective Measures period, and before permanent repairs begin.

24. In-house contractors: These are contractors already under contract with the cooperative and are usually already familiar with the co-op's crews and service area. These contractors may or may not need the direct supervision of a cooperative employee, depending upon their knowledge of the co-op's system, its substations, main feeder circuits, critical loads, etc.
25. Rights-Of-Way (R-O-W) contractors: Some co-ops maintain rights-of-way contractors on an annual basis. These R-O-W contractors can be very beneficial during a disaster, especially if needed for debris removal. These contractors may still need to be supervised by co-op personnel, and will need to provide complete details of their daily work to the affected cooperative, preferably submitting detailed invoices on a weekly basis.
26. Co-op R-O-W supervisors can be very helpful in preparing damage report maps, locations of work to be performed, and in preparing transformer or pole replacement reports. Because of their experience, some co-ops may choose to make these R-O-W supervisors their disaster Project Officers. This will obviously vary from co-op to co-op.
27. Notify all other departments of work orders assigned to the disaster. Other departments should also be informed of activity codes that may be assigned. Coordinate specifically with the accounting department to ensure that copies of all time sheets, invoices, checks and cash receipts are obtained. Keep a working file that is designated by work order number, FEMA Category A through F, and location (map number, county, etc.).
28. Utilize marketing, public relations, or key accounts employees, based on their experience and level of training, to deliver food and/or materials to crews in the field. Ask them to keep all receipts and detailed logs of material and/or equipment delivered.
29. Arrange for fuel (diesel, gas, etc.) from suppliers throughout the co-op's service area. Have a contingency plan to deliver properly-sized backup generators to these fuel suppliers in case their pumps have no electricity due to the disaster.
30. Have all contactors sign a simple contract stating that they are indeed contractors and that they agree to "hold harmless" the cooperative from liability, worker's compensation claims, damage to hotel/motel rooms, and damage to public/private property due to their crews' negligence. Include in this agreement that weekly invoicing for work performed by the contractor is expected by the cooperative.
31. Engineering firms may need to be used to prepare bid specifications. Utilize their services during a disaster situation. This will also help in allowing the cooperative's in-house engineering and staking department personnel to stay ahead of contractors and construction crews with staking and material sheets, **which is absolutely necessary**.
32. As soon as possible during the disaster, utilize public relations personnel, part-time employees, or possibly retirees to take both still pictures and videos of the damage. This serves two purposes: **1.)** It makes a permanent record of the amount of ice that was on the line or the level of devastation caused by a hurricane or tornado, thus making damage repair estimates more realistic; and, **2.)** Photos and videos can be used to show FEMA and/or state emergency management personnel conditions that caused the damage to the cooperative's system. Remember that FEMA and/or state emergency management personnel often do not show up at the cooperative until several days (or weeks) have passed, so these photos and

videos can play a very important role in verifying and validating damage assessments and the necessary levels of permanent repairs to be stipulated in PWs.

33. **Any verbal contract or agreement** between contractors and cooperative personnel should be written down and recorded. A checklist should be made by the engineering/operations departments of documentation to be required from all contract crews. This documentation will serve as backup for review of billing invoices submitted by contractors. If documentation is not present and does not backup an invoice submitted by the contractor, the contractor should be required to find and submit the proper documents before payment is made to the contractor by the cooperative.
34. Contractors should be required to submit weekly invoices, including time sheets, detailing individual crew member names, where they worked, hours worked, equipment used, etc., and listing costs for pieces of equipment used in both the emergency restoration and permanent repair efforts.
35. Engineering/operations personnel should be prepared to document and explain the process used by the local cooperative to select work crews, whether from other co-ops (through the Mutual Aid Plan) or from contract construction crews. An 'Action Plan' detailing how the co-op selected contractors and why specific equipment was requested for the emergency restoration and permanent repairs process should also be developed.

NOTE: Department of Public Safety officials should be notified anytime a cooperative declares an Emergency Outage Situation due to a disaster, thus extending "Hours of Service" driving regulations for certain personnel.