Filing Receipt

Filing Date - 2024-03-08 10:32:27 AM

Control Number - 53385

Item Number - 1832

Affected Entity: South Plains Electric Cooperative, Inc. **PROJECT NO.** 53385

EXECUTIVE SUMMARY

This Executive Summary provides an overview of South Plains Electric Cooperative, Inc. ("Cooperative's") process for maintaining all aspects of Cooperative's business following various disasters in compliance with 16 Tex. Admin. Code § 25.53, Public Utility Commission of Texas' ("PUCT") substantive rule regarding Electric Service Emergency Operations Plan ("Rule").

Table 1 provides an overview of the contents and policies included in Cooperatives Emergency Operations Plan ("Plan").

Policy	Section	Page
APPROVAL AND IMPLEMENTATION	I.	4
ORGANIZATIONAL AND PERSONNEL ASSIGNMENTS	II.	6
COMMUNICATION PLAN	III.	9
EMERGENCY SUPPLIES & ASSISTANCE COORDINATION	IV.	12
IDENTIFICATION OF WEATHER-RELATED HAZARDS	V.	18
WEATHER EMERGENCY PROCEDURES	VI.A	20
LOAD SHED PROCEDURES	VI.B	20
PANDEMIC PREPARDNESS PLAN	VI.C	22
WILDFIRE MITIGATION PLAN	VI.D	31
CYBERSECURITY ANNEX	VI.F	32
PHYSICAL SECURITY INCIDENT ANNEX	VI.G	53

[*Remainder of Page Intentionally Left Blank*]

Affected Entity: South Plains Electric Cooperative, Inc. **PROJECT NO.** 53385

Table 2 provides an overview of the Plan's compliance with the Rule.

CITATION	DESCRIPTION OF REQUIREMENT	APPLICABILITY	EOP SECTION	EOP PAGE #
25.53(d)(1)(A-E)	APPROVAL AND IMPLEMENTATION SECTION	YES	I	4-5
25.53(d)(2)(A)	COMMUNICATION PLAN FOR ENTITIES WITH TRANSMISSION OR DISTRIBUTION SERVICE	YES	III	9-12
25.53(d)(2)(B-D)	COMMUNICATION PLAN FOR GENERATORS, REP AND ERCOT	NO		
25.53(d)(3)	PLAN TO MAINTAIN PRE-IDENTIFIED SUPPLIES FOR EMERGENCY RESPONSE	YES	IV, Appendix C, Appendix D	12-18, 93,94
25.53(d)(4)	PLAN THAT ADDRESSES STAFFING DURING EMERGENCY RESPONSE	YES	II	6-9
25.53(d)(5)	A PLAN THAT ADDRESSES HOW AN ENTITY IDENTIFIES WEATHER-RELATED HAZARDS. INCLUDING TORNADOES, HURRICANES, EXTREME COLD WEATHER, EXTREME HOT WEATHER, DROUGHT, AND FLOODING, AND THE PROCESS THE ENTITY FOLLOWS TO ACTIVATE THE EOP	YES	V	18-19
25.53(e)(1)(A)(i-ii)	WEATHER EMERGENCY ANNEX	YES	VI.A, Appendix C, Appendix	20-21, 93,94,98

			D, Appendix G	
25.53(e)(1)(B)(i-iii)	LOAD SHED ANNEX	YES	VI.B	20-21
25.53(e)(1)(C)	A PANDEMIC AND EPIDEMIC ANNEX	YES	VI.C	22-30
25.53(e)(1)(D)	A WILDFIRE ANNEX	YES	VI.D	31-32
25.53(e)(1)(E)	A HURRICANE ANNEX THAT INCLUDES EVACUATION AND RE-ENTRY PROCEDURES FACILITIES ARE LOCATED WITHIN A HURRICANE EVACUATION ZONE, AS DEFINED BY THE TEXAS DIVISION OF EMERGENCY MANAGEMENT (IDEM);	YES	VI.E	32
25.53(e)(1)(F)	CYBERSECURITY ANNEX	YES	VI.F	32-52
25.53(e)(1)(G)	PHYSICAL SECURITY INCIDENT ANNEX	YES	VI.G	53-57
25.53(e)(1)(H)	A TRANSMISSION AND DISTRIBUTION UTILITY THAT LEASES OR OPERATES FACILITIES UNDER PURA §39.918(B)(1) OR PROCURES, OWNS, AND OPERATES FACILITIES UNDER PURA §39.918(B)(2) MUST INCLUDE AN ANNEX THAT DETAILS ITS PLAN FOR THE USE OF THOSE FACILITIES; AND	NO		
25.53(e)(1)(I)	ANY ADDITIONAL ANNEXES AS NEEDED OR APPROPRIATE TO THE ENTITY'S PARTICULAR CIRCUMSTANCES	NO		

Affected Entity: South Plains Electric Cooperative, Inc. **PROJECT NO.** 53385

25.53(e)(2)(A-H)	REQUIREMENTS FOR GENERATORS	NO		
25.53(e)(3)(A-E)	REQUIREMENTS FOR REPS	NO		
25.53(e)(4)(A-F)	REQUIREMENTS FOR ERCOT	NO		

[*Remainder of Page Intentionally Left Blank*]

Table 3. lists the titles and names of employees receiving access to and training on this Plan, including the date of access to or training.

NAME	TITLE	DATE OF ACCESS OR TRAINING
Dale Ancell	Executive V.P. and G.M.	10-31-2023
Randal Bailey	Assistant G.M.	10-31-2023
Jamey Phillips	Attorney	10-31-2023
Lynn Simmons	Director of Communications	10-31-2023
Tahnee Truitt	Director of Human Resources	10-31-2023
Shane Adams	Chief Financial Officer	10-31-2023
Dianne Hewett	Manager of Executive Services	10-31-2023
Jon Henson	Division Manager	10-31-2023
Steven Latham	Manager of I.T.	10-31-2023
Brandon Loth	Manager of Engineering	10-31-2023
Ben Greene	Division Manager/Manager of Risk Management	10-31-2023
Jeremy Herring	Manager of Operation Systems	10-31-2023
Jeff Watson	Manager of Key Accounts	10-31-2023
Matt Quinn	Manager of Accounting	10-31-2023

Table 4. lists the primary and backup emergency contacts for individuals who can address urgent requests and questions from the PUCT during an emergency.

NAME	TITLE	RESPONSIBILITY	CONTACT INFORMATION
Randal Bailey (Primary)	Assistant G.M.	Principal administrator of the Plan. Must review and approve all changes.	T: 806-775-7732 M: 806-787-9099
Dale Ancell (Backup)	Executive V.P. and G.M.	Backup administrator of the Plan. Must review and approve all changes	T: 806 775-7732 M: 806-535-7740
Jamey Phillips (Backup)	Attorney	Contact for PUCT	T: 806-775-7854 M: 806-438-2993
Ben Greene (Backup)	Manager of Risk Mgmt	Contact for PUCT	T: 806-775-7731 M: 806-252-8087

Affected Entity: South Plains Electric Cooperative, Inc. **PROJECT NO.** 53385

AFFIDAVIT

STATE OF TEXAS §

COUNTY OF LUBBOCK §

BEFORE ME, the undersigned authority, on this day personally appeared, and who, after being duly sworn, stated on his or her oath that he or she is entitled to make this Affidavit, and that the statements contained below are based on personal knowledge and are true and correct.

I, Dale Ancell, swear or affirm the following on behalf of South Plains Electric Cooperative, Inc. ("Cooperative"), an electric cooperative operating in the State of Texas:

a. Relevant operating personnel are familiar with and have received training on the applicable contents and execution of the Emergency Operations Plan ("EOP"), and such personnel are instructed to follow the applicable portions of the EOP except to the extent deviations are appropriate as a result of specific circumstances during an emergency.

b. The EOP has been reviewed and approved by the appropriate executives.

c. Drills have been conducted to the extent required.

d. The EOP or an appropriate summary has been distributed to local jurisdictions as needed.

e. Cooperative maintains a business continuity plan that addresses returning to normal operations after disruptions caused by an incident; and

f. Cooperative's emergency management personnel who are designated to interact with local, state, and federal emergency management officials during emergency events have received the latest IS-100, IS-200, IS-700, and IS-800 National Incident Management System Training.

g. The EOP was revised on March 5, 2024 to include updated procedures regarding Mutual Aid in Appendixes F and G, pages 96-102.

_____ (Signature of Officer of the Cooperative)

Sworn to and subscribed before me on this 6th day of March, 2024

_____

Notary Public in and for the State of Texas

JAMEY L. PHILLIPS
Notary Public, State of Texas
Comm. Expires 04-27-2025
Notary ID 10021157

Notary Seal

South Plains Electric Cooperative, Inc.

Your Touchstone Energy® Cooperative

The power of human connections

EMERGENCY OPERATIONS PLAN

November 1, 2022

Revised March 5, 2024

TABLE OF CONTENTS

I. APPROVAL AND IMPLEMENTATION

A. INTRODUCTION

South Plains 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").

A significant portion of the plan concerns the coordination of emergency assistance with Lubbock's Office of Emergency Management and other local emergency agencies, neighboring cooperatives, construction contractors, and other utilities. It outlines procedures for securing assistance according to the plan developed by Texas Electric Cooperatives through their Loss Control & Safety Program. SPEC personnel designated to interact with local, state, and federal emergency management officials during emergency events have completed FEMA NIMS training (IS-700.a, IS-800.b, IS-100.b and IS-200.b.).

This plan is based on the model developed by Texas Electric Cooperatives to facilitate uniform application and implementation among the electric cooperatives of Texas.

Since South Plains Electric Cooperative operates no generation facilities, nothing has been included in this plan on the topics of power plant weatherization or alternative fuel and storage.

This plan will be reviewed at least once annually if it has not been implemented in response to an actual event within the preceding 12 months. Following any implementation or annual review, SPEC shall assess the effectiveness of the plan and modify it as needed. The official copy will be maintained in the Operations Center at 110 N. Interstate 27, Lubbock, Texas, 79424.

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
Dale Ancell	Executive Vice President and General Manager	Backup administrator of Plan. Must review and approve all changes	Yes
Randal Bailey	Assistant General Manager	Principal administrator of the Plan. Must review and approve all changes	Yes

Jamey Phillips	Attorney	Assist administration of plan	No
Ben Greene	Manager of Risk Mgmt/ Division Mgr	Assist administration of plan	No

C. REVISION AND SUMMARY

This Plan, dated as of November 1, 2022, supersedes all previous versions of the Plan. Please refer to Table 2 for records of revision.

Table 2 Records of Revision

Revision Date	Section	Summary of Change	Inserted by (name and signature)
December 20, 1992	unknown	revised original Plan dated May 1991	unknown
December 10, 1994	unknown	unknown	unknown
December 13, 1996	unknown	unknown	unknown
June 12, 1997	unknown	unknown	unknown
January 12, 2001	unknown	unknown	unknown
April 20, 2005	unknown	unknown	unknown
July 17, 2006	unknown	unknown	unknown
January 11, 2008	unknown	unknown	unknown
April 25, 2008	unknown	unknown	unknown
March 31, 2015	unknown	unknown	unknown
October 29, 2015	unknown	revised after annual review	Allan Brown
February 1, 2017	Media, school, and emergency contacts	updated information	Allan Brown
October 29, 2019	Media, school, and emergency contacts	updated information	Ben Greene
November 12, 2019	Responsible persons	updated titles after annual review	Ben Greene
October 28, 2021	Media, school, and emergency contacts	revised after annual review	Ben Greene
April 6, 2022	all	revised Plan in accordance with 16 Texas Administrative Code § 25.53 - Electric Service Emergency Operations Plan	Ben Greene
November 1, 2022	Emergency contacts	revised after annual review	Ben Greene
March 5, 2024	Appendixes F, G	revised mutual aid	Ben Greene

II. ORGANIZATIONAL AND PERSONNEL ASSIGNMENTS

The following is not intended as an exhaustive list of all probable or potential jobs encountered in an emergency situation. It does, however, define the essential 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 SPEC 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 SPEC employees.
- Authorized to use direct access to system operations (775-7752).

Manager 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 SPEC 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 TEC. All requests for material, reports of oil leaks, etc., shall be reported through this one engineer.
- Keep appropriate regulatory bodies (municipal governments, 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 a 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 of 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 media, school and 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 SPEC radio towers) are fueled and ready to run.

III. COMMUNICATIONS

A. 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 "SPEC 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/COMPLAINTS

Members can report outages by calling our automated system at 806.741.0111 or 888.741.0111. The system works on caller ID technology. If the member is not calling from a phone number recognized by the system, they can still leave a message to report their outage.

Members can use the outage texting service by texting "OUT" to 85700. Members must first sign-up for the service by texting "SPEC" to 85700. The system works on caller ID technology, so the member's phone number must be in our database. In addition, members opted-in to our outage texting system may receive texts pushed out by the Cooperative with pertinent updates.

Members can use the SPEC App to report outages. Once a member is logged in, they can select the "Report an Outage" icon to submit outage details. They can also request a call back or select the option to receive power out notifications.

Members can also dial the office directly at 806.775.7732. Depending on the call volume, all calls may be routed to the automated system.

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.

The Cooperative's website, at www.SPEC.coop, publishes mobile phone numbers for key staff and many members contact key staff directly.

Police, fire and other emergency service organizations are provided with unpublished phone numbers for reaching the Operations Center directly.

Members can file complaints through the Cooperative's website contact form located at www.SPEC.coop. Email addresses and mobile phone numbers for key staff are also available on the website. Members can contact us privately or publicly through Facebook at www.facebook.com/southplainselectric, Twitter at www.twitter.com/southplainsec, or dial the office directly at 806.775.7732.

C. PUBLIC COMMUNICATIONS

Communication tools include Facebook and Twitter, 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 Communications Department is available for interviews as needed. We also have the ability to pull member lists for email and text communications.

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, texting, email, radio, television, social media, Cooperative's website, law enforcement officers, other important contacts, and utility personnel in the field.

F. REGULATORY COMMUNICATIONS

The Attorney for South Plains Electric Cooperative shall insure the timely filing of reports in the event a system failure or load loss meets the reporting threshold of state and federal regulatory bodies.

1. Procedure for outage reporting to the U. S. Department of Energy

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 (202-586-8100) 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 AND ASSISTANCE COORDINATION

SPEC maintains poles, conductors, associated hardware, and other supplies readily available on site to restore power after an emergency before permanent work commences.

Additionally, as described below SPEC 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 SPEC sites and Appendix D: Restoration Crew Supplies for a list of emergency supplies for restoration personnel.

A. SECURING ASSISTANCE FROM REGIONAL COOPERATIVES

SPEC 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 SPEC 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, SPEC will request mutual aid assistance according to the plan developed by Texas Electric Cooperatives through their Loss Control & Safety Program.

SPEC 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 (512-486-6249 Office---(512) 584-7758 Cell) and advise of your needs.

Other contacts at TEC include:
Mike Williams, 512-486-6203 Office---(512) 789-6210 Cell
Julia Harvey, 512-486-6220 Office---(512) 789-3349 Cell
Johnny Andrews, 512-763-3330 Office---(512) 426-1567 Cell
Danny Williams, 512-413-0509 (Office)---

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 Requesting Assistance (see Appendix E).

C. COMPLIANCE WITH COOPERATIVE SAFETY RULES AND POLICIES

All SPEC 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. Consider the development of a Rest and Recuperation Policy (R & R) for employees. Such policy should be designed for the safety and well-being of the cooperative's employees, and for the general public. The policy should be developed by management, and approved/adopted by the co-op's board of trustees. If such a policy is enacted during the disaster, the date and time should be noted in the form of a written memorandum.

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 coops 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 Cooperative'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 storm. 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.).

- ***Expected outage time: None***
- ***Scope of outage: No members out of service***
- ***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.

- ***Expected outage time: Less than 4 hours***
- ***Scope of outage: Less than 100 members***
- ***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.

- ***Expected outage time: 4 to 12 hours***
- ***Scope of outage: Entire substation or major feeder***
- ***Initiated by: Director of operations & engineering or general manager***

Level 3

Requires outside help to restore service. All Cooperative employees must report.

- ***Expected outage time: More than 12 hours***
- ***Scope of outage: Widespread damage to system***
- ***Initiated by: Director of operations & engineering or general manager***
- ***Operations superintendent to have full responsibility for coordinating restoration activities***

VI. ANNEXES

Cooperative 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

A. 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 Personnel Supplies provides a list of emergency supplies maintained at Cooperative sites.
- Appendix G: Engineering and Operations provides a list of emergency supplies maintained at Cooperative sites.

B. ANNEX B - LOAD SHED

I. CURTAILMENT REGISTRY OF CRITICAL LOAD AND CRITICAL CARE CUSTOMERS

South Plains Electric Cooperative uses the following procedure for shedding load during emergencies that require the curtailment of electrical power. These procedures include curtailing power to the categories listed below in sequential order:

1. Oilfield
2. Irrigation
3. Industrial
4. Commercial
5. Residential
6. Radio and television stations
7. Critical load - public safety (e.g. police, fire, hospitals, assisted living/nursing/hospice facilities, etc.)
8. Chronic condition and critical care residential members

II. ROTATING OUTAGES

South Plains Electric 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 will have discretion in determining where load shedding will best serve the interest of the cooperative.

III. PRIORITIES FOR RESTORATION OF SERVICE

South Plains Electric Cooperative will endeavor to use the following order of load classification when restoring service after a loss of power due either to outage conditions or curtailment procedures:

1. Chronic condition and critical care residential members
2. Critical load - public safety (e.g. police, fire, hospitals, assisted living/nursing/hospice facilities, etc.)
3. Radio and television stations
4. Residential
5. Commercial
6. Industrial
7. Irrigation
8. Oilfield

In addition to the priorities concerning community health and safety, South Plains Electric will assign crews to specific areas. Generally, the crews will concentrate on a given line section 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.

IV. CONFIDENTIAL REGISTRY OF CRITICAL LOAD AND CRITICAL CARE CUSTOMERS

South Plains Electric 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.

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.

C. ANNEX C- PANDEMIC PREPAREDNESS 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).

4. 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 Manager 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.

VII. 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: • North lobby • West 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

PURPOSE

The intent of this plan is to outline the wildfire mitigation efforts of South Plains Electric Cooperative related to its overhead electrical distribution lines and associated equipment throughout its service territory.

PLAN

South Plains Electric Cooperative 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 warning

When conditions warrant (or when relevant advisories are issued), South Plains Electric Cooperative will require a visual inspection of any line in its Rolling Plains division that has been de-energized by protective relaying prior to re-energizing.

The following is a list of Cooperative stations with circuits located in areas susceptible to wildfires; responding local fire departments are also listed.

Substation	Wildfire Potential	Responding Fire Department
Abernathy	N	
Acuff	N	
Aspermont	Y	Aspermont FD
Becton	N	
Bissett	Y	Aspermont FD
Caprock	Y	Ralls FD
Clairemont	Y	Jayton FD
Cooper	N	
Copper Breaks	Y	Hardeman County FD
Cotton Center	N	
County Line	N	
Erskine	N	
Espuela	Y	Spur FD
Frankford	N	
Frenship	N	

Glenn	Y	Dickens FD
Guthrie Switch St.	Y	King County FD
Halfway	N	
Henry	Y	Childress, Cottle, Hardeman FD
Hettler	N	
Hurlwood	N	
Idalou	N	
Jayton	Y	Jayton FD
Kalgary	Y	Crosbyton, Spur, Post FD
King	Y	King County FD
McAdams	Y	Foard County FD
Midway Sw.	N	
New Deal	N	
Paducah	Y	Cottle County FD
Pleasant Hill	N	
Posey	N	
Quaker	N	
Ralls	N	
Ransom Canyon	N	
Reese	N	
Robertson	Y	Lorenzo FD
Salt Creek	N	
Shallowater	N	
Slaton	N	
SMS	Y	Spur FD
Smyer	N	
Union	N	
Upland	N	
Wolfforth	N	
Woodrow	N	

E. ANNEX E- HURRICANES

Not applicable. SPEC 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

South Plains Electric Cooperative, Inc.

Your Touchstone Energy® Cooperative

Incident Response Plan

South Plains Electric Cooperative, Inc.
P.O. Box 1830
Lubbock, TX 79408

Revision History

REVISION HISTORY			
DATE	VERSION	DESCRIPTION	MODIFIED BY
06/17/2020	0.1	Early Draft	Logan DeWitt
06/23/2020	0.2	Revised Draft	Logan DeWitt
7/21/2020	0.3	Addition of non-malware type incidents	Logan DeWitt
1/13/2021	0.4	Addition of workflow model, minor adjustments	Logan DeWitt
2/1/2021	0.5	Adjusted job titles, minor wording adjustments	Tim Warren

Table of Contents

Contents

1.0 Introduction

1.1 Purpose

This document describes the plan for responding to **cyber security incidents** at South Plains Electric Cooperative, Inc. (SPEC). For the purposes of this plan, "incident response" in all cases refers to *cyber security incidents*. It defines the roles and responsibilities of Information Security Personnel at SPEC, how incidents are characterized, relationships to other policies and procedures, and reporting requirements. The goal of the Cyber Security Incident Response Plan (CSIRP) is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to the necessary parties, and reduce the likelihood of the incident from reoccurring.

1.2 Scope

This plan applies to all Information Systems, Company Data, Member/Client Data under company control, Company Networks, Client Networks, and any person or device that gains access to these systems, data, and/or networks.

1.3 Maintenance

The SPEC Manager of Information Technology is responsible to oversee the maintenance and revision of this document as appropriate.

2.0 Definitions

2.1 Event

An *event* is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

2.2 Cyber Security Incident

A *cyber security incident* (short: *incident*) is a violation or imminent threat of violation of computer security policies, acceptable use policies, standard security practices, or a suspected compromise of the confidentiality, integrity, or availability of SPEC controlled information. If IT, Security, or Risk Management employees must take actions to contain, clean, or recover from an event or series of events, it is an incident. An incident can also be declared and later found to be a non-incident. The types and fidelity of information often evolves over the course of an investigation, but the response team should not wait to declare an incident until "we are sure" or "it is confirmed." When we suspect that we have the elements for an incident, we declare an incident, respond in accordance with the plan, and let the investigation make a final determination of the incident closed status and severity. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

- Users are tricked into opening a "quarterly report" sent via email that is actually malware;
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.
- Malware establishes a foothold on any connected device and is not remediated by anti-virus or prevented from executing by other security controls. Malware on an end point, cleaned by anti-virus is an *event*, not an incident.

An incident must be formally declared by the employee(s) deemed responsible for the asset or the employee(s) taking responsibility of the asset in the absence of the responsible employee(s).

2.3 Reportable Incident

A *reportable incident* is one that must be acted upon in order to respond to or mitigate a potential cyber security threat.

This includes instances involving threats the True Digital Security SOC has received on behalf of SPEC through existing security infrastructure, for which the SOC was not able to issue a definitive determination that the threat was mitigated, false positive, or otherwise required no action.

2.4 Personally Identifiable Information (PII)

PII is defined as any part of a person's legal name in combination with one or more of the following data elements:

- Social Security Number (SSN)
- State-issued driver's license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

2.5 Protected Health Information (PHI)

PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any form or medium by a Covered Component. PHI is considered individually identifiable if it contains one or more of the following identifiers:

2. Name
3. Address (all geographic subdivisions smaller than a state including street address, city, county, precinct, or zip code)

4. All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death, and exact age)
5. Telephone numbers
6. Fax numbers
7. Electronic mail addresses
8. Social Security Numbers
9. Medical Record Numbers
10. Health plan beneficiary numbers
11. Account numbers
12. Certificate/license numbers
13. Vehicle identifiers and serial numbers, including license plate number
14. Device identifiers and serial numbers
15. Universal Resource Locators (URLs)
16. Internet Protocol (IP) Addresses
17. Biometric identifiers, including finger and voice prints.
18. Full face photographic images and any comparable images
19. Any other unique identifying number, characteristic or code that could identify an individual

2.6 Severity Level Matrix and Notification

Incidents need to be categorized by their severity level. Some incidents represent a low level of risk to the organization however these are still incidents which will be recorded in the incident log and provide a basis for metrics to track trends and keep the executive leadership team informed.

Severity	Definition	Notification
Low	When a single device that has no sensitive information is affected	N/A
Medium	When a single device with sensitive information (PII, PHI, or research and development sensitive information per ref j.) is affected or more than 10 workstations are affected in a single incident	Manager of IT
High	When a single device with sensitive information or where compliance is affected, or when 20 or more workstations are impacted	Manager of IT and Executive Staff
Critical	When a device or multiple devices within the scope of compliance requirements is affected.	Manager of IT and Executive Staff

3.0 Roles and Responsibilities

3.1 Executive Vice President (EVP)

The EVP is overall responsible for the effective exercise of SPEC legal and compliance requirements relative to incident response and incident reporting. He will work through the Manager of Information Technology to guide specific incident response actions.

3.2 Manager of Information Technology

The Manager of Information Technology is responsible for all Information Technology related aspects of the Incident Response, including maintenance of cyber detection and response systems and all recovery aspects of incident response.

The Manager of Information Technology also is responsible to the EVP for SPEC physical security activities and compliance requirements relative to federal contracting physical security requirements. The Manger of Information Technology will be included in Cyber Incident Response when appropriate and needed as determined by the CIRT Leader.

3.3 Cyber Incident Response Team (CIRT) Leader

The CIRT Leader is the principal leader of SPEC's response to a cyber incident. Additionally, the CIRT Leader coordinates any outside parties assisting with incident response, such as a forensics or recovery team.

In the case that a single employee is responsible for the software and/or equipment and is responding to the incident accordingly, this employee becomes the CIRT. In a case where more SPEC employees are required or the incident covers equipment that falls under multiple employee's responsibility, the Manager of Information Technology will appoint the CIRT.

3.4 Manager of Risk Management

The Manager of Risk Management is responsible for advising the EVP on the company's legal responsibilities following a cyber incident. These especially could include notifying employees, the state, federal or other governing entities, members, or outside law enforcement.

3.5 Director of Communications

The Director of Communications is not a core member of the incident response team but will be included as needed. This role will handle all communications needed for press interaction.

3.6 Information Systems Security Provider (ISSP)

The ISSP will provide 24/7 monitoring of SPEC information systems and incident detection capabilities. The ISSP's response to potential incidents will conform to this plan.

4.0 Methodology

This plan outlines the general tasks for Incident Response (IR) and may be supplemented by specific internal guidelines and procedures that describe the use of specific security tools and/or channels of communication.

4.1 Event Identification and Notification

Determine if an incident has occurred. Determinations regarding this should be sourced from the definitions of **event** and **reportable incident** given hereabove.

If an incident has occurred, notify the appropriate members of the core incident response team.

a. The core incident response team will include: The CIRT Leader, the Manager of Information Technology, and the ISSP. The ISSP is not involved with direct handling of incident response but is notified of incidents in order to appraise SOC watchstanders of events which may be seen at the SIEM level relating to the incident, and IoC's that should be monitored until incident closure.

4.2 IRP Documentation

The Incident Response Team will endeavor to thoroughly document all relevant data regarding their response to an incident, including:

- Actions taken to appraise appropriate parties
- Actions taken to investigate, what evidence resulted in the classification of the event as an incident
- Actions taken to mitigate risk
- Resolution and Lessons Learned

4.3 Determine Scope

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. SPEC staff will periodically train on procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response and that post-incident lessons learned are incorporated into procedural enhancements.

4.4 Response according to Scope

Accurate and timely detection of an incident or potential incident is one of the most challenging areas of incident response. We will maintain risk categorization aligned with best practice guidelines, SPEC risk tolerance, and the threats posed to client data.

4.4.1 Low

EXAMPLE: [Single asset malware infection, single user account compromise, single asset needs to be reviewed for compromise, etc.]

Containment: Isolate by removing system from production, taking system offline or disabling account. This may be done physically, by changing networks, applying firewall rules, or utilizing software that is designed to isolate a system.
Remediation: Utilize tools necessary to resolve the incident. Preserve evidence as much as possible.
Monitor the asset
Return asset to normal operation
Document the incident

4.4.2 Medium

EXAMPLE: [Multi-asset malware infection, multi-user account compromise, etc.]

Containment: Isolate known assets by removing systems from production, taking systems offline, or disabling accounts. This may be done physically, by changing networks, applying firewall rules, or utilizing software that is designed to isolate the systems. Review the rest of the environment to verify other systems are not affected.
Remediation: Utilize tools necessary to resolve the incident. Preserve evidence as much as possible. Verify the events on the assets or accounts are related to the same incident.
Monitor the assets
Return assets to normal operation
Document the incident

4.4.3 High

EXAMPLE: [Single compromise instance on asset within compliance scope, single user compromise involving possible sensitive information access, etc.]

Containment: Isolate known asset by removing system from production, or taking system offline. This may be done physically, by changing networks, applying firewall rules, or utilizing software that is designed to isolate the system. Review the rest of the environment to verify other systems are not affected.
Remediation: Consult full IR team to determine next steps. Utilize tools necessary to resolve the incident. Preserve evidence as much as possible.
Monitor the assets: Consult full IR team to determine what is best to be monitored.
Return assets to normal operation
Document the incident

4.4.4 Critical

EXAMPLE: [Multi-asset or multi-user compromise within compliance scope, multi-asset/multi-user compromise involving confirmed sensitive info leak, etc.]

Containment: Isolate known assets by removing systems from production, or taking systems offline. This may be done physically, by changing networks, applying firewall rules, or utilizing software that is designed to isolate the systems. Review the rest of the environment to verify other systems are not affected.
Remediation: Consult full IR team to determine next steps. Utilize tools necessary to resolve the incident. Preserve evidence as much as possible. Verify the events on the assets or accounts are related to the same incident.
Monitor the assets: Consult full IR team to determine what is best to be monitored.
Return assets to normal operation
Document the incident

5.0 Escalation

At any point in the incident response process, the CIRT Leader may be called upon to escalate any issue regarding the process or incident. The CIRT Leader will determine when such escalation may occur and will take the appropriate action according to the severity of the incident.

5.1 Low Severity Incident

A low severity incident affects a single device that has no sensitive information. They have minimal business impact risk to the organization or its reputation. Low severity incidents do not need to be reported or trigger the incident response protocol unless their severity level is upgraded upon review.

5.2 Moderate Severity Incident

A moderate severity incident occurs when more than 5 assets are affected in a single incident. A single server incident is considered a moderate severity incident.

The True Digital Security SOC will report any medium severity alert, as defined in the current security incident and event monitoring (SIEM) ruleset to SPEC via established communications protocols within 60 minutes unless the alert is investigated and found to be a false positive before that time is reached.

5.3 High Severity Incident

A high severity incident occurs when a device with sensitive information is affected. It can also occur when more than 20 workstations are impacted, or a number of servers greater than one and less than four in total. The EVP will be notified promptly when a *potential* high severity incident is identified.

The ISSP will report any high severity alert, as defined in the current security incident and event monitoring (SIEM) rule set to SPEC via established communications protocols unless the alert is investigated and found to be a false positive or otherwise require no action.

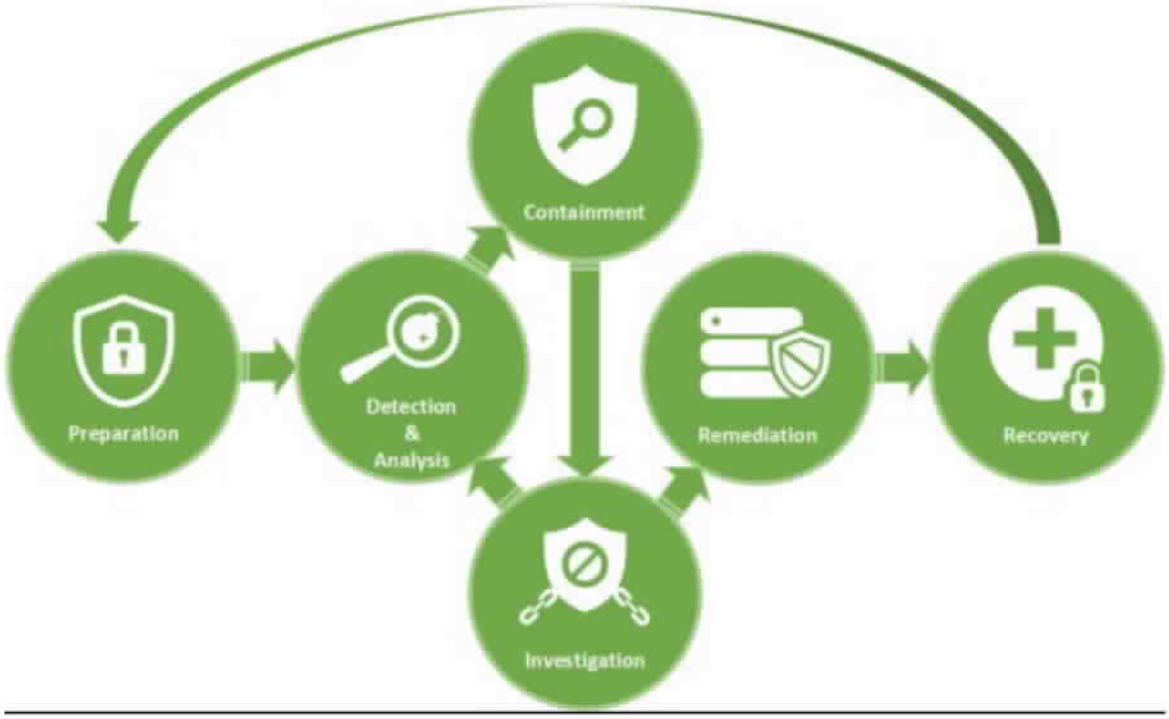
5.4 Critical Severity Incident

A critical severity incident occurs when multiple devices with sensitive information or within compliance scope are affected. Incidents involving the confirmed compromise of core networking devices, substation devices, or four or more servers are also considered critical severity. The EVP will be notified promptly when a *potential* critical severity incident is identified.

The ISSP will report any high severity alert, as defined in the current security incident and event monitoring (SIEM) rule set to SPEC via established communications protocols unless the alert is investigated and found to be a false positive or otherwise require no action.

6.0 Incident Response Cycle

The basic cyber security incident process encompasses six phases: preparation, detection, containment, investigation, remediation, and recovery. This plan is the primary guide for the preparation of local guidelines and procedures that will allow the CIRT team to be ready to respond to any incident. Recovery includes a lessons-learned process to re-evaluate the preparation of specific procedures and modifying them when it is appropriate.



6.1 Preparation

Preparation includes those activities that enable the CIRT Leader to respond to any incident: policies, tools, procedures, effective documentation, and a communication plan. Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analyses from prior incidents should form the basis for continuous improvement of this stage.

6.2 Detection & Analysis

Detection is the discovery of the event with security tools or notification by an inside or outside party about a suspected incident. This phase includes the declaration and preliminary classification of the incident.

6.3 Containment

Containment is the triage phase where the affected host or system is identified, isolated, or other mitigated, and when affected parties are notified and investigative status established. This phase may include seizure and evidence handling, escalation, and communication.

6.4 Investigation

Investigation is the phase where Cyber Incident Response Team (CIRT) personnel determine the authoritative classification and root cause of the incident. The escalation level of the event will be determined by the Investigation. This stage also determines whether external resources should be leveraged to assist with the investigation, remediation, or recovery phase.

6.5 Remediation

Remediation is the post-incident repair of affected systems, communication, and instruction to affected parties, and analysis that confirms the threat has been contained. The determination of whether there are regulatory requirements for reporting the incident (and to which outside parties) will be made at this stage. Apart from any formal reports, the post-mortem will be completed at this stage as it may impact the remediation and interpretation of the incident.

6.6 Recovery

Recovery is the analysis of the incident for its procedural and policy implications, the gathering of metrics, and the incorporation of lessons learned into future response activities and training. The CIRT Team Leader will ensure the proper documentation and reporting of the incident.

7.0 Data Backup Procedures

SPEC maintains data integrity by backing up company data to two data centers.

7.1 Backup of Data Center Virtual Environments

Our virtual servers are backed up daily or more often. The server's data is stored in various datastores on the virtual environment storage. Snapshots are taken of these datastores and replicated across between North and Admin.

7.2 Backup of Remote Servers, Personal Computers, and Network Equipment

7.2.1 Remote Servers

Servers that are not in the Admin or North data center virtual environment are backed up to a repository or a share in the North data center. This data is then replicated to the Admin data center daily.

7.2.2 Personal Computers

Some laptops and desktops are deemed to have significant or sensitive information that needs to be backed up. These devices are backed up to a repository or share in the North data center. This data is then replicated to the Admin data center daily.

7.2.3 Network Equipment

The configuration files for the Cisco network equipment are archived by Prime Infrastructure (PI) daily. PI is a server in our virtual environment and is backed up and replicated as seen in 7.1.

8.0 Disaster Response

In this context, a disaster is any unforeseen event that can significantly put your organization at risk by interfering with your IT operations - whether natural, like flooding or pandemic, or man-made, such as a cutting through a water main.

8.1 Disaster Incident Classification

Not every disruptive event is a disaster – for instance, a short power outage after which all critical systems are promptly and successfully restored would be considered an event, not an incident. Events do not require the deployment of the incident response plan.

On the other hand, a power outage which is excessively prolonged would be classified as an incident. An outage which has been resolved but from which critical systems were unable to be completely restored would also be classified as an incident.

Some of the questions you should consider when deciding whether an event should be classified as an incident are:

1. Has the event already resolved? If not, is it expected to resolve promptly without SPEC's intervention?
2. If the event has resolved, have all critical systems recovered? Examples of critical systems would be: domain controllers, substation assets, channels of communication, etc.
3. Has the event caused safety hazards to personnel? Is it possible it could?

4. If the event has resolved, has it caused damage which must be repaired?
5. Has the event caused disruptions to SPEC's IT operations that may negatively impact customers, clients, or affiliates?

8.2 Disaster Recovery

Disaster recovery is the process of resuming normal operations following a disaster by regaining access to data, hardware, software, networking equipment, power, and connectivity. However, if your facilities are damaged or destroyed, activities may also extend to logistical considerations like finding alternate work locations, restoring communications, or sourcing anything from desks and computers to transportation for employees.

The top priority of SPEC will be to enact the steps outlined in this plan to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- Maintaining the safety of personnel, customers, clients, and other affiliates.
- Preventing the loss of the organization's resources such as hardware, data, and physical IT assets
- Minimizing downtime related to IT
- Keeping the business running in the event of a disaster

8.3 Disaster Recovery Teams

1. **Management Disaster Recovery Team**
   The management team will be directly responsible for all decisions related to employee safety; correspondingly, as decisions within this scope arise among non-management disaster response teams, these concerns should be communicated directly to the management team for consideration. The management team will also be responsible for the overall coordination of other response teams.

Name	Title	Email	Phone
Steven Latham	Manager of I.T.	Slatham@spec.coop	806-775-7762
Ben Greene	Manager of Risk Management	Bgreene@spec.coop	806-775-7731

2. **Network Disaster Recovery Team**
   The Network Team focuses on restoring any impacted network devices or related infrastructure that has been impacted by a disaster. Though primarily responsible for providing baseline network functionality, they may assist other D.R. Teams as required.

Name	Title	Email	Phone

I.T. Department		Slatham@spec.coop	806-775-7762

3. **Server Disaster Recovery Team**
   The Server Team will be responsible for restoring the physical server infrastructure required for the organization to run its IT operations and applications in the event of and during a disaster. Though primarily responsible for providing baseline server functionality, they may assist other D.R. Teams as required.

Name	Title	Email	Phone
I.T. Department		Slatham@spec.coop	806-775-7762

4. **Application Disaster Recovery team**
   The Applications Team will be responsible for ensuring that all organization applications are recovered and operate as required to meet business objectives in the event of and during a disaster. While primarily responsible for ensuring and validating appropriate application performance, they may assist other Teams as required.

Name	Title	Email	Phone
I.T. Department		Slatham@spec.coop	806-775-7762

5. **IT Support Disaster Recovery Team**
   The IT Support Team will be responsible for assisting personnel with completing IT functions as the incident develops. They will interface with other teams to determine what guidance users should be provided as the overall effort to recover proceeds.

Name	Title	Email	Phone
I.T. Department		Slatham@spec.coop	806-775-7762

9.0 Disaster Response Workflow

Standard disaster response workflow should start with classification (event or incident), followed by alerting the Disaster Recovery Lead. The lead identifies the scope of the incident, then assigns the incident to the appropriate team(s).

Once briefed on the situation, the lead(s) for the team(s) assigned to the incident formulate a response strategy, notify the Disaster Recovery lead of the steps they'll be taking to mitigate the situation, and begin the recovery process.

The Disaster Recovery Lead will be responsible for coordinating actions between teams to ensure action plans do not conflict. Documentation follows the same process as a standard malware incident, utilizing the incident response worksheet.

10.0 Workflow Model

A visual representation of the workflow model implemented by this plan is included below.

Incident Response Worksheet

1.0 Detection and Analysis:

1.1 Detection Source:

What was the source of the detected event? (SIEM, FirePower, User Reported, etc.)

Click or tap here to enter text.

1.2 Preliminary Classification:
(Reference Section 4.1)

Has an incident occurred?

☐ Yes ☐ No

1.3 Preliminary Classification:
(Reference Section 4.4)

☐ Event ☐ Low ☐ Medium ☐ High ☐ Critical

1.4 Have the appropriate parties been notified?
(Reference Section 2.6)

☐ Yes ☐ No ☐ Notification not required

1.5 Description
Describe the incident.

2.0 Containment:

(If you answered "no" to section 1.2, continue to report end to sign, date, and complete your report.)

Containment Actions Taken:
(Reference section 4.4)

(EX: SentinelOne deployed, removed from network, account disabled, etc.)

3.0 Investigation:

3.1 Authoritative Classification:

(Reference section 4.1)

If the investigation results in a change in severity classification, document below:

☐ No change ☐ Event ☐ Low ☐ Medium ☐ High ☐ Critical

3.2 External Resources:

If it's decided that external resources should be leveraged for the Investigation, Remediation, or Recovery phase, please document this below:

(EX: SentinelOne deployed, removed from network, account disabled, etc.)

3.3 Investigation:

(EX: SentinelOne deployed, removed from network, account disabled, etc.)

4.0 Remediation

(Reference section 6.5)

Document the repair of affected systems, communication, instruction to affected parties, and analysis that confirms the threat has been contained.

(EXAMPLE: SentinelOne deployed, threat quarantined, evaluated, and deleted. Asset monitored post incident, no additional events after mitigation. Threat communicated internally to affected users and teams, full CIRT not deployed. Associated communication accompanies this report in a separate file.)

5.0 Recovery

(Reference section 6.6)

5.1 Procedural/Policy Implications/Lessons Learned

Document any changes to procedure, policy, or the incident response plan itself that should be made correspondent to the incident, our response to it, and especially with respect to the prevention of similar incidents hereafter.

Incident Response Participants

(By signing, you agree that all information hereabove is true and accurate to the best of your knowledge)

First: Dale Last: Ancell
Role: Executive V.P. and G.M.
Signature: _____

First: Steven Last: Latham
Role: Manager of I.T.
Signature: _____

First: Ben Last: Greene
Role: Manager of Risk Management
Signature: _____

First: Lynn Last: Simmons
Role: Director of Communications
Signature: _____

First: Kris Last: Kerr
Role: Cyber Incident Response Team Leader
Signature: _____

First: [first-name] Last: [last-name]
Role: [CIRT role]
Signature: _____

List of Internal Contacts

- Employees referenced above

List of External Contacts

- Law Enforcement
    - Lubbock Sheriff Department – 806-775-1400
    - Lubbock Police Department – 806-775-2865
    - Lubbock area FBI – 806-765-8571
- Cyber Insurance -
- Public Utility Commission of Texas
    - Main Number – 512-936-7000
- ERCOT
    - IT Support – 866-870-8124
- Southwest Power Pool
    - Main Number – 501-614-3200
- Golden Spread
    - Alicia's cell phone – 806-577-7108 (text preferred)
- Brazos
    - Main Number – 254-750-6500
- TrueDigital
    - SOC – 918-524-9455

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.

2. 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.

3. 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 does 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*

4. 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.

5. 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.

6. 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.

7. 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.

I. ANNEX I- ADDITIONAL ANNEXES

None

APPENDIX A. EMERGENCY CONTACTS

City of Lubbock
Joe Moudy,
Emergency Management Coordinator & Homeland Security Director, City of Lubbock
(806) 775-3401 - office
JMoudy@mylubbock.us

Nikolas Fort,
Deputy Director, Emergency Management, City of Lubbock
(806) 775-3402 - office
NFort@mylubbock.us

Lubbock County
Clinton S. Thetford, Coordinator
Emergency Management Coordinator
Lubbock Co. Sheriff's Department/RACES
(806) 775-7300 office
(806) 786-8717 work cell
(806) 775-7309 fax
cthetford@lubbockcounty.gov

Kathleen Finley
Asst. Emergency Management Coordinator, Lubbock County
(806) 775-7008 - office
(806) 239-6087 - cell
kfinley@lubbockcounty.gov

Lubbock County Judge
Honorable Curtis Parrish
775-1679 office
775-7950 fax
ldiaz@co.lubbock.tx.us

New Deal
Michael Hopson
Emergency Management Coordinator
Police Chief
806-746-5860 office

Idalou
Suzette Williams
Emergency Management Coordinator
806-892-2531 office

Swilliams@cityofidalou.com

Slaton
Clinton S. Thetford, Coordinator
Emergency Management Coordinator
Lubbock Co. Sheriff's Department/RACES
(806) 775-7300 office
(806) 786-8717 work cell
(806) 775-7309 fax
cthetford@lubbockcounty.gov

Wolfforth
Rick Scott
Emergency Management Coordinator
Police Chief
806-855-4160 office

Shallowater
Cory Buck
Emergency Management Coordinator
806-832-4521 office
806-632-8901 cell
cbuck@shallowatertx.us

Abernathy
Ron Johnson
Emergency Management Coordinator
Mayor
806-298-2546
citymgr@cityofabernathy.org

Ransom Canyon
James Hill
Emergency Management Coordinator
806-829-2600 office
806-786-8513 cell
police@sptc.net

Buffalo Springs
Jana Trew
Mayor
806-829-2470

Woodrow Community
Wesley Boone

Fire Chief
806-745-3658 office
806-759-1630 cell
woodrowvfd@sbcglobal.net

Roosevelt Community
Bill Sides
Fire Chief
806-842-3317 office
806-438-5423 cell
bsides@sptc.net

West Carlisle Community
Tim Smith
Fire Chief
806-797-0412 office
806-786-0166 cell
smith@door.net

Texas Tech University
Ronald Phillips
Emergency Management Coordinator
806-742-2121 office
806-438-3175 cell
Ronald.phillips@ttu.edu

State of Texas DEM (TDEM)
Region 5 District 2
Erica McDowell
District Coordinator
(806)-740-8982 office
(806) 548-4344 cell
Erica.McDowell@tdem.texas.gov

Brandi Ashby-Fisher
Assistant Chief-Region 5
806-740-8983 office
806-517-0581 cell
Brandi.Ashby-Fisher@tdem.texas.gov

State Operation Center
(512) 424-2208 main office
(512) 424-7160 fax
Media email: media@tdem.texas.gov

South Plains Association of Governments

Tommy Murillo
Homeland Security
(806) 762-8721 office
(806) 454-1284 cell
TMurillo@spag.org

State Emergency Preparedness
Natalie Vega, Unit Chief
Natalie.Vega@tdem.texas.gov

Lead, PUC Emergency Management Team
Shawn Hazard
512-936-7106 office
512-680-7586 cell
Shawn.hazard@puc.texas.gov

TDEM Main Fax
512 424 7160
Voice number @ SOC to confirm fax was received is 512/424-2208

NWS Lubbock Severe Weather Reporting
(877)-582-5697 or (877)-LUBK-NWS
Please remember, this number is reserved for use by spotters, law enforcement, emergency managers, and other government officials. **Please do not distribute this number to the general public.**

Jody James
Warning Coordination Meteorologist
National Weather Service - Lubbock, TX
Voice: 806.745.3916 x223
Email: jody.james@noaa.gov
Web: www.weather.gov/Lubbock

American Red Cross
Judy Pevytoe
Director of Disaster Services
Volunteer Coordinator
(806) 765-8534 - office
(806) 765-5963 - fax

Goodwill of Northwest Texas
Robin Raney
806-744-8419 office
806 781-1405 cell
rraney@goodwillnwtexas.org

Salvation Army
Jacob Bailey
Disaster Services & Volunteer Coordinator
(806)-765-9434

Lubbock Area Railroad Companies

BNSF Railway –
500 Main Street, Lubbock, TX 79401
220 RR Ave. Slaton, TX 79364

Emergencies
1-800-832-5452
Reporting: Railroad Crossing Collisions
RR Crossing Signal Malfunctions
Damages to a RR Xing Signal Device
Obstructions / Vehicles on or near Railroad Tracks
Crimes Against the Railroad

Lubbock Terminal Office
806-765-3941

Slaton Terminal Office
806-765-3989

Lubbock and Western Railway
109 E. Texas Ave.
Eunice, NM 88231

Emergencies
1-866-386-9321 ext 6171

Office: 866-889-2826

South Plains Lamesa Railroad (also: SPL Rwy)
10917 E. FM # 2150 at E. CR 78
Slaton, TX 79364
Office: 806-828-4841

Police, Fire, Ambulance, Sheriff

Abernathy

Emergency: 911
Ambulance: (806) 298-2241
Fire Dept.: (806) 298-2233 (VFD), 298-2546 (City)
Police: (806) 298-2545

Aspermont

Emergency: 911
Sheriff: (940) 989-3333
Fire Dept.: (940) 989-3596

Childress

Emergency: 911
Police: (940) 937-2546
Fire: (940) 937-6562
Sheriff: (940) 937-2535

Crosbyton

Emergency: 911
Ambulance: (806) 675-2382
Sheriff: (806) 675-7301

Crowell/Foard County

Ambulance & fire: (940) 684-1200
Non-emergency fire: (940) 684-1722
Sheriff: (940) 684-1501

Cottle County

Sheriff: (806) 492-2145

Cotton Center

Fire Dept.: (806) 879-2157

Dickens

Emergency: 911
Sheriff: (806) 623-5532

Floyd County

Sheriff: (806) 983-4901

Garza County

Sheriff: (806) 495-3595

Guthrie

Emergency: 911

Sheriff: (806) 596-4413
Sheriff Dispatch: (806) 596-4470

Hale Center

Volunteer Fire Department
(806) 839-2419
Police: (806) 839-4450

Hale County

Sheriff: (806) 296-2724

Hardeman County/Quanah

Non-emergency fire: (940) 663-2963
Sheriff: (940) 663-5374

Hurlwood

Emergency: 911

Idalou

Emergency: 911
Police: (806) 892-2531

Jayton

Emergency: 911
Sheriff: (806) 237-3801

Lamb County

Sheriff: (806) 385-7900

Levelland

Emergency: 911
EMS: (806) 894-8855
Fire Chief: (806) 894-3155
Police: (806) 894-6164

Littlefield

Emergency: 911
Fire Dept.: (806) 385-5161
Police: (806) 385-5161

Lorenzo

Emergency: 911
City Hall: (806) 634-5596

Lubbock

Emergency: 911

Fire Dept.: (806) 765-2632
Police: (806) 775-2816
Sheriff non-emergency: (806) 775-1600

Lynn County

Sheriff: (806) 561-4505

Matador

Emergency: 911
Sheriff: (806) 347-2234
Fire Dept.: (806) 347-2323

New Deal

Police: (806) 746-5860
City Hall: (806) 746-6399

Paducah

Emergency: 911
Police: (806) 492-3131
EMS: (806) 492-2336
Fire: (806) 492-2929

Petersburg

Emergency: 911
Fire Dept.: (806) 667-3461
Police: (806) 667-3461
Sheriff: (806) 667-3681

Plainview

Emergency: 911
Fire/EMS Emergency: (806) 296-1170
Police Emergency: (806) 296-1111
Police Non-Emergency: (806) 296-1182

Post

Emergency: 911
Fire Dept.: (806) 535-7328
Police Dept.: (806) 495-3595

Quanah

Emergency: 911
Police: (940) 663-2821
Fire: (940) 663-2963
Sheriff: (940) 663-5374

Ralls

Emergency: 911

City office: (806) 253-2558

Ransom Canyon

City Hall: (806) 829-2470
Fire Dept.: (806) 829-2123 VFD
Police: (806) 829-2600

Shallowater

Emergency: 911
Fire Dept.: (806) 832-5917
Police Dept.: (806) 832-4561

Slaton

Fire Dept. (806) 828-2025
Police: (806) 828-2020

Smyer

Emergency: 911
Fire Dept. & City Hall: (806) 234-3861

Spur

Emergency: 911
Sheriff: (806) 623-5533

Wolfforth

Emergency: 911
Ambulance Non-Emergency: (806) 866-9126
Fire Dept.: (806) 866-9126
Police: (806) 866-4160

Volunteer Fire Departments by County For updates: http://tfsfrp.tamu.edu/fdd/directory/

Childress County

Childress Fire Department (combination paid & volunteer)
Daniel Tyler
100 Commerce
Childress, Texas 79201
940-937-6562

Cottle County

Paducah VFD

Gene Whitener
P. O. Box 884 Paducah, Texas 79248
806-346-7099

Crosby County

Crosbyton Volunteer Fire Dept.
Acting Fire Chief: J. J. Justus
221 West Main
Crosbyton, TX 79322
806-675-2301

Lorenzo Volunteer Fire Dept.
Chief: Mark Majors
P O Box 430
Lorenzo, TX 79343
806-283-5233

Ralls Volunteer Fire Dept.
Fire Chief: Billy Tidwell
800 Ave I
Ralls, TX 79357
806-777-5393

Dickens County

Dickens VFD
Will Humphreys
P. O. Box 189
Dickens, TX 79229
806-269-1978

McAdoo VFD
Mack Gardner
P. O. Box 79
McAdoo, Texas 79243
806-657-7132 (Gardner's phone)
806-657-7604

Spur VFD
Wess Abbott
P. O. Box 396
Spur, Texas 79370
806-549-1731

Floyd County

Floydada Volunteer Fire Dept.*

Fire Chief: Chad Guthrie
114 West Virgina Street
Floydada, TX 79235
806-983-2834

Lockney Volunteer Fire Dept.*
Fire Chief: Donnie McLaughlin
P O Box 10
Lockney, TX 79241
806-983-1848

Foard County

Crowell VFD
Perry Shaw
P. O. Box 814 Crowell, Texas 79227
940-684-1112 City Hall
940-655-4949 (Shaw's phone)

Garza County

Post Volunteer Fire Dept.
Fire Chief: Jimmy Valdez
105 E Main
Post, TX 79356
806-241-5076

Hale County

Abernathy Volunteer Fire Dept.
Fire Chief: Kelly Vandygriff
1511 Ave M
Abernathy, TX 79311
806-298-2546

Edmonson Volunteer Fire Dept.*
Fire Chief: Robert Block
P O Box 55
Edmonson, TX 79032
806-864-3300

Hale Center Volunteer Fire Dept.
Fire Chief: Mike Watson
702 Main
Hale Center, TX 79041
806-729-1320

Halfway Volunteer Fire Dept.
Fire Chief: Dale Gibson

801 W. US 70
Plainview, TX 79072
806-774-3559

Petersburg Volunteer Fire Dept.
Fire Chief: T. J. Marquez
P O Box 326
Petersburg, TX 79250
806-667-3461

Hall County

Memphis VFD
Terry Altman
721 Robertson
Memphis, Texas 79245
806-259-2323

Hardeman County

Chillicothe VFD
Troy Perkins
P. O. Box 126
Chillicothe, Texas 79225 940-839-9228

Quanah VFD
Casey O'Neal
P. O. Box 629
Quanah, Texas 79252
940-663-2963 (fireman on duty)

Hockley County

Anton Volunteer Fire Dept.*
Fire Chief: Douglas Mitchell
P O Box 128
Anton, TX 79313
806-997-2801

Levelland Volunteer Fire Dept.
Fire Chief: Bill Durham
502 Ave F
Levelland, TX 79336
806-894-3155

Smyer Volunteer Fire Dept.
Fire Chief: Chris Bradberry
P O Box 203
Smyer, TX 79367

806-234-3861

Sundown Volunteer Fire Dept.*
Fire Chief: Cole Mulloy P O Box 975
Sundown, TX 79372
806-891-5999

Kent County

Kent Co VFD
Nathan Brooks
P. O. Box 30
Jayton, Texas 79528
806-237-3801

King County

King County Volunteer Fire Department
Ricky Criswell
P. O. Box 84 Guthrie, TX 79236
806-392-6088 (Rickey's phone)

Lamb County

Amherst Volunteer Fire Dept.*
Fire Chief: RD Gass
P O Box 58
Amherst, TX 79312
806-246-3226

Earth Volunteer Fire Dept.*
Fire Chief: Matthew Goe
P O Box 274
Earth, TX 79031
806-640-2413

Littlefield Volunteer Fire Dept.*
Fire Chief: Jamie Grey
P O Box 1267
Littlefield, TX 79339
806-785-1261

Olton Volunteer Fire Dept.*
Fire Chief: Hector Galvan
Po Box 1087
Olton, TX 79064
806-638-2099

Springlake Volunteer Fire Dept.*

Fire Chief: Shane Furr
P O Box 58
Springlake, TX 79082
806-946-9697

Sudan Volunteer Fire Dept.*
Fire Chief: Mike Hill
P O Box 491
Sudan, TX 79371
806-227-2113

Lubbock County

Buffalo Springs Lake Volunteer Fire Dept.
Fire Chief: John Keys Jr.
99 C Pony Express
Buffalo Springs, TX 79404
806-317-0726

Carlisle Volunteer Fire Dept.
Fire Chief: Tim Smith
P O Box 98055
Lubbock, TX 79499
806-786-0166

Idalou Volunteer Fire Dept.
Fire Chief: Russ Perkins
P O Box 1277
Idalou, TX 79329
806-789-0833

New Deal Volunteer Fire Dept.
Fire Chief: Randy Teeter
P O Box 75
New Deal, TX 79350
806-746-5222

Ransom Canyon Volunteer Fire Dept.
Fire Chief: Rand McPherson
1 Ridge Road
Ransom Canyon, TX 79366
806-773-8482

Roosevelt Volunteer Fire Dept.
Fire Chief: Bill Sides
9401 E FM 40
Lubbock, TX 79403

806-842-3317

Shallowater Volunteer Fire Dept.
Fire Chief: Mackie Buck
P O Box 246
Shallowater, TX 79363
806-632-8901

Slaton Volunteer Fire Dept.
Fire Chief: Ethan Johnston
200 S 8th ST
Slaton, TX 79364
806-828-2025

Wolfforth Volunteer Fire Dept.
Fire Chief: Lance Barrett
P O Box 36
Wolfforth, TX 79382
806-548-1377

Woodrow Volunteer Fire Dept.
Fire Chief: Wesley Boone
15715 Loop 493
Lubbock, TX 79423
806-745-3658; 806-759-1630

Lynn County

O'Donnell Volunteer Fire Dept.*
Fire Chief: Brandon Pyron
P O Box 84
O'Donnell, TX 79351
806-549-6709

New Home Volunteer Fire Dept.
Fire Chief: Ryan Gill
P O Box 2253
New Home, TX 79383
806-773-8269

Tahoka Volunteer Fire Dept.
Fire Chief: Bryan Reynolds
P O Box 300
Tahoka, TX 79373
806-759-1102

Wilson Volunteer Fire Dept.

Fire Chief: Craig Wilke
P O Box 22
Wilson, TX 79381
806-778-7326

Motley County

Matador VFD
Lee Jones
P. O. Box 222
Matador, Texas 79244
806-549-4936

Roaring Springs VFD
Les Woolsey, Fire Chief
P. O. Box 222
Roaring Springs, TX 79256
806-422-0196

Stonewall County

Stonewall County VFD
Jimmy Pittcock
P. O. Box 834 Aspermont, Texas 79502 940-256-3961
940-989-3596

Tell Volunteer Fire Department
Chief: Paul Bryant
14830 CR X
Tell, Texas 79259-9004
940-585-4652
940-585-6244

*not considered a VFD that serves our area and/or members

TV Stations

KAMC ABC 28
7403 S. University, Lubbock 79423
Crystal Reagan, General manger
806-745-2345

KLBK CBS 13

7403 S. University, Lubbock 79423
www.everythinglubbock.com
Cindy Gilstrap, General Manger
Phone: (806) 745-2345 (main switchboard)

KCBD News Channel 11

5600 Ave. A, Lubbock, 79404
www.KCBD.com
11listens@kcbd.com
Greg McAlister, General Manager
806-761-4200
Phone: (806) 744-1414
New Fax: (806) 749-1111

KJTV Fox 34

9800 University Ave., Lubbock 79423
www.myfoxlubbock.com
news@fox34.com
Newsroom: 745-4545
Newsroom fax: 748-9387
News director: Matt Ernst mernst@fox34.com
Greg McAlister, General Manager
806-748-9300

Ramar Communications

9800 University Ave.
Lubbock, TX 79423
806-745-3434

Channel Two News (Quanah)

319 S. Main St., Quanah
Phone: (940) 663-6311
Fax: (940) 663-6825; (940) 663-6311

Radio Stations

KJAK FM 92.7

www.kjak.com
kjak@kjak.com
Business: (806) 745-6677

Fax: (806) 745-8140

KRFE AM 580 Lubbock – Jim Stewart

www.am580lubbock.com
jim@am580lubbock.com
wade@wadewilkes.com
Business: (806) 745-1197
Jim cell: (806) 241-1331

For all three stations (Next Media Group)– 96, 100.3, 101.1
Business: (806) 762-3000
Fax: (806) 770-5363 Attn: Tony

KLLL FM 96

www.klll.com
jscott@wilkslubbock.com
jscott@klll.com

Listener: (806) 770-5555

KMMX FM 100.3

www.kmmx.com
info@kmmx.com
Listener: (806) 770-5649

KONE FM 101.1 Classic Rock

www.cr101.com
Listener: (806) 770-5000
Office Line: 806-762-3000
Program Director: Sean Dillon; sdillon@wilkslubbock.com

For all five ClearChannel (790 AM, 1340 AM, 94.5, 98.1, 99.5 and 102.5) stations
Business: (806) 798-7078
Fax: (806) 783-9067 Attn: Robert Snyder

KFYO AM 790

www.kfyo.com
jane@kfyo.com
Listener: (806) 770-5790

KZII FM 102.5

Listener: (806) 770-5102

KKCL FM 98.1
Listener: (806) 770-5665

KQBR FM 99.5
Listener: (806) 770-5995

KFMX FM 94.5
Listener: (806) 770-5369

KRFE AM 580
Business: (806) 745-1197
Listener: (806) 745-1197
Fax: (806) 745-1088
Wade Wilkes — wade@wadewilkes.com
Jim Stewart — jim@am580lubbock.com

KFLP FM 106.1 & AM 900 (Floydada)
www.kflp.net
tony@kflp.net
Tony St. James, GM
Business: (806) 983-5704
Fax: (806) 983-5705

For all Ramar Stations: 97.3, 107.7, 93.7, Double T 104.3, 100.7, 97.7, 96.9
Business 806.748.2404
Fax: 806.748.2470

KXTQ FM 97.3
Business: (806) 745-3434
Listener: (806) 770-5937
Fax: (806) 748-2470
jmartinez@ramarcom.com; vcarillo@ramarcom.com

KJTV AM/Fox News 950
Listener: (806) 770-5950
Business: (806) 745-3434
Fax: (806) 748-2470

KRBL FM 105.7
Business: 806-438-4998
Dave Walker dave@walkerbc.com

KLFB Spanish Radio
Business: (806) 765-8114
Listener: (806) 765-5016
Fax: (806)

KCTX FM 96.1 (Childress)
Business: (940) 937-6316
Fax: (940) 937-6551
Jay Boles, Owner
kctxradio@gmail.com

KVRP 97.1 Big County (Haskell)
Business: (940) 864-8505
1406 N 1st ST
Haskell, TX 79521

KKYN AM (Plainview)
Listener: (806) 296-2771

Newspapers

Abernathy Advocate
Kristina Janet, Editor & Publisher
P. O. Box 157
Abernathy, TX 79311
Phone: (806) 632-3822
Fax: (806) 892-2233
E-mail: abernathyadvocate@windstream.net

Caprock Courier (covering Motley Co.)
Kay Ellington, Publisher
Barbara Brannon, Editor
P.O. Box 430
Spur, TX 79370
Phone: (806) 271-3381
Fax: (806) 271-3966
E-mail: caprockcourier@gmail.com and spur@thetexasspur.com

Crosby County News
Valentine Publishing Company
John Valentine
817 Main St.
Ralls, TX 79357
Phone: (806) 253-0211
Fax: (806) 253-0211

E-mail: crosbycountynews@windstream.net

Idalou Beacon
Jona Janet, Editor & Publisher
P.O. Box 887
Idalou, TX 79329
Phone: (806) 892-2233
Fax: (806) 892-2233
E-mail: beacon@windstream.net

Lubbock Avalanche-Journal
710 Ave. J
Lubbock, TX 79401
Phone: (806) 766-8722 or (806) 762-8844
Fax: (806) 744-9603
Send News Releases to:
Public Safety Reporter: Erica Pauda; epauda@lubbockonline.com; Cell: (806) 549-2499; Office: (806) 766-8742
Local News Editor: Adam Young; ayoung@lubbockonline.com; Cell: (706) 766-8725; Office: (806) 766-8725
Associate News Editor: Karen Brehm; kbrehm@lubbockonline.com; Cell: (806) 766-8706; Office: (806) 766-8717
Deadlines for business news in Sunday AJ is Thurs. noon unless a holiday, then usually a day earlier.
Check newspaper for other deadlines.

Plainview Daily Herald
Ellysa Harris
820 Broadway St.
Plainview, TX 79072
Phone: (806) 296-1353
Fax: (806) 296-1363
E-mail: ellysa.harris@hearstnp.com

Post Dispatch
Julia Childs, Editor
123 E. Main St.
P. O. Box 490
Post, TX 79356
Phone: (888) 400-1083 ext. 100
Fax: (806) 495-2059
E-mail: Thepostcitydispatch@gmail.com

Quanah Tribune Chief
Shane Lance, Editor
310 Mercer

Quanah, TX 79252
Phone: (940) 663-5333
Fax: (940) 663-5073
E-mail: editor@quanahtribunechief.com

Slatonite
Melissa McCaghren, GM
P.O. Box 667
Slaton, TX 79364
Phone: (806) 828-6201
Fax: (806) 828-6202
E-mail: melissa@slatonitenews.com

The Paducah Post
Chad & Jody Piper, Editors
808 15th St.
Paducah, TX 79248
Phone: (806) 341-8077 or 806-492-2329
E-mail: paducahposted@gmail.com

The Red River Sun (for Childress)
Can't find a name right now, but know Chris sold it
226 N Main
Childress, TX 79201
P.O. Box 1260
Phone: (888) 400-1083 ext. 100
E-mail: news@redriversun.com
Mention in email that ad is for "Childress section"

The Texas Spur
Barbara Brannon, Editor and Kay Ellington, Publisher
P.O. Box 430
Spur, TX 79370
Phone: (806) 271-3381
Fax: (806) 271-3966
E-mail: news@thetexasspur.com and spur@thetexasspur.com

Others:
RE Magazine
Scot Hoffman, Managing Editor
4301 Wilson Blvd.
Arlington, VA 22203-1867
Phone: (703) 907-5701
Fax: (703) 907-5519
Email: remag@nreca.coop, scot.hoffman@nreca.coop

Electric Co-op Today
Martin W.G. King, Editor
4301 Wilson Blvd.
Arlington, VA 22203-1867
Phone: (703) 907-5881
Fax: (703) 907-5951
Email: ectoday@nreca.org

Golden Spread Electric Cooperative
D'Ann Allen
P.O. Box 9898
Amarillo, TX 79105-5898
Phone: (806) 379-7766
Cell: 806.418.1677
Fax: (806) 374-2922
E-mail: dallen@gsec.org

Texas Electric Cooperatives
Martin Bevins
P.O. Box 9589
Austin, TX 78766-9589
Phone: (512) 454-0311 ext. 220
Fax: (512) 467-9442
E-mail: bevins@texas-ec.org

Area Schools

Abernathy ISD
Aaron Waldrip, super
806.298.4940
505 7th St.
Abernathy, TX 79311

Aspermont ISD
Zach Morris, super
(940) 989-3355 Superintendent and Business Office
(940) 989-2707 high school
P.O. Box 549
Aspermont, TX 79502

Childress ISD
Carl Taylor, super
(940) 937-2501

800 Ave. J NW
Childress, TX 79201

Chillicothe ISD

Todd Wilson, super
(940) 852-5391 ext. 225
P.O. Box 550
Chillicothe, TX 79225

Cotton Center ISD

Ryan Bobo
(806) 879-2160
P.O. Box 350
Cotton Center, TX 79021

Crosbyton ISD

David Rodriguez, super
(806) 675-7331
204 S. Harrison
Crosbyton, TX 79322

Crowell ISD

Jennifer Forsythe, super
(940) 684-1403
P.O. Box 239
Crowell, TX 79227

Frenship ISD

Dr. Michelle McCord, super
(806) 866-9541 ext. 1254
P.O. Box 100
Wolfforth, TX 79382

Guthrie HS

Jodie Reel, super
(806) 596-4466
Po Box 70
301 Jaguar Lane
Guthrie, TX 79236
Jreel@guthriecsd.net

Hale Center ISD

Steven Pyburn, super
(806) 839-2451 ext. 107
Po Box 1210

Hale Center, TX 79041

Idalou ISD

Robert Gibson, super
(806) 892-1900
P.O. Box 1338
Idalou, TX 79329

Jayton-Girard ISD

Layne Sheets, super
(806) 237-2991
700 Madison Ave.
Jayton, TX 79528

Lorenzo ISD

Kayla Morrison, super
(806) 634-5591
Drawer 520
Lorenzo, TX 79343

Lubbock-Cooper ISD

Keith Bryant, super
(806) 863-7100 ext. 1014
13807 Indiana, Ave.
Lubbock, TX 79423
kbryant@lcisd.net

Lubbock ISD (which includes the following 4 high schools)

Dr. Kathy Rollo., super
(806) 219-0070
1628 19th St.
Lubbock, TX 794
superintendent@lubbockisd.org

Coronado High School

Julia Stephen, principal
(806) 219-1129
3307 Vicksburg Ave.
Lubbock, TX 79410
Julia.stephen@lubbockisd.org

Estacado High School

Angelica Wilbanks, principal
(806) 766-1400
1504 E. Itasca Ave.
Lubbock, TX 79403

Lubbock High School
Doug Young, principal
(806) 766-1455
2004 19th St.
Lubbock, TX 79401

Monterey High School
Les 'Jack' Purkeypile, principal
(806) 766-0700
3211 47th St.
Lubbock, TX 79413
lpurkeypile@lubbockisd.org

New Deal ISD
Matt Reed, super
(806) 746-5833
P.O. Box 280
New Deal, TX 79350

Paducah ISD
Gary Waitman, super
(806) 492-2009
902 Goodwin Ave.
Paducah, TX 79248

Patton Springs ISD
Bryan White, super
(806) 689-2220 is the main number. As soon as the message starts, you can dial Ext. 2222 for the superintendent or ext. 224 for the business office.
1261 FM 193
Afton, TX 79220

Petersburg ISD
Dr. Brian Bibb, super
(806) 667-3585
P.O. Box 160
Petersburg, TX 79250

Post ISD

David Foote, super
(806) 495-3343
P.O. Box 70
Post, TX 79356

Quanah ISD
Tom Johnson, super
(940) 663-2281 ext. 400
PO Box 150
Quanah, TX 79252

Ralls ISD
Dr. Nathan Maxwell, super
(806) 253-2509 ext. 4101
810 Ave. I
Ralls, TX 79357

Roosevelt ISD
Dallas Grimes, super
(806) 842-3282
Rt. 1, Box 402
Lubbock, TX 79401

Shallowater ISD
Dr. Anita Hebert, super
(806) 832-4531 ext. 2004
1100 Ave. K
Shallowater, TX 79363

Slaton ISD
Jim Andrus, super
(806) 828-6591
300 S 9th St.
Slaton, TX 79364

Smyer ISD
Chris Wade, super
(806) 234-2935 ext 100
P.O. Box 206
Smyer, TX 79367

Spur ISD
Craig Hamilton, super
(806) 271-3272 superintendent and business office
800 Calvert Ave.
Spur, TX 79370

Wilson ISD
JP Portillo, super
(806) 628-6261

P.O. Box 9
Wilson, TX 79381

Appendix B
Regulatory contacts and reporting procedures

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 3 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: 05/31/2021 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 or 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

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 America 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 systemawareness@nerc.net and/or operations@eisac.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

Form OE -417 instructions:

..\OE417_Form_Instructions_05312021.docx

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