



Filing Receipt

Received - 2023-03-10 11:11:36 AM
Control Number - 53385
ItemNumber - 970

**FARMERS' ELECTRIC COOPERATIVE, OF
NEW MEXICO, INC.**

EMERGENCY OPERATIONS PLAN
(EOP)



Table of Contents

	Page
Executive Summary	3
Approval and Implementation Section	4
Record of Distribution	4
Emergency Contacts	5
Communication Plan	5
Pre-stocking of Supplies	8
Staffing During Emergencies	8
Weather Related Hazards	9
<u>Annexes</u>	
i. Cold Weather Emergency	10
ii. Hot Weather Emergency	15
iii. Load Shed	20
iv. Wildfire	25
v. Hurricane	55
vi. Pandemic and epidemic	56
vii. Cyber Security Incidents	62
viii. IT Business Continuity/Disaster Recovery Plan	76
ix. Physical Security Incidents	90
x. Event Response and Reporting Plan	92
Drills	101
Emergency Operation Plan Activation History	102
Affidavit of CEO/General Manager	103

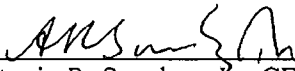
EXECUTIVE SUMMARY

Farmers' Electric Cooperative, Inc. of New Mexico (FEC) was formed in 1938, by its members as an electric cooperative under New Mexico law. FEC provides power to members in Curry, De Baca, Guadalupe, Roosevelt, Quay, Harding and San Miguel Counties in New Mexico and to less than 100 metered accounts along the New Mexico – Texas border in portions of Deaf Smith, Oldham, and Parmer Counties in west Texas. I have served as CEO/General Manager of Farmers' Electric Cooperative since June 1, 2022.

FEC modified its Emergency Operations Plan (EOP) to update Cooperative Emergency Contacts, and Record of Distribution.

Relevant operating personnel are familiar with and have received training on the contents of this Emergency Operations Plan (EOP), and such personnel are committed to following the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency.

FEC maintains a business continuity plan to address returning to normal operations after disruptions caused by an incident.



Antonio R. Sanchez, Jr., CEO/General Manager

I. Approval and Implementation Section

- a. The development of an Emergency Operations Plan (EOP) offers Farmers' Electric Cooperative (FEC) the opportunity to prepare and plan the most efficient means in which to restore it's system in the event of either a small isolated outage or a system wide outage resulting from a major natural disaster or other cause.
- b. The individuals listed below are responsible for maintaining and implementing this EOP and possess the requisite authority to change this EOP.
- c. EOP Revision History

Date	Individual Making Edits	Reason/Comments
04/07/22	Thom Moore, Dir., Member Service or designee	Add pertinent information for FEC
03/10/23	Antonio R. Sanchez, Jr., CEO/CEO/General Manager	Annual Review

- d. As of March 10, 2023, this EOP supersedes all previous EOPs or ERPs.
- e. This EOP was approved on April 7, 2022.
- f. This EOP was most recently updated on March 10, 2023.

II. Record of Distribution

- a. This document has been distributed to the following individuals:

Date of Distribution	Distributed to: Name	Title
03/10/23	Antonio R. Sanchez, Jr.	CEO/General Manager
03/10/23	Barry Bass	Line Superintendent I
03/10/23	Rodrick "Rick" Ragland	Line Superintendent II
03/10/23	Michael McCord	Engineering Manager
03/10/23	Thom Moore	Dir., Member Services
03/10/23	Suzy Howard	Accounting Manager
03/10/23	Helen Jo Wallin	Billing/HR Supervisor
03/10/23	Glenn Barleben	IT Manager

III. Emergency Contacts

COOP Emergency Contacts			
Title	Name	Mobile Phone	Extension
CEO/General Manager	Antonio R. Sanchez, Jr.	575-799-6218	
Line Superintendent I	Barry Bass		
Line Superintendent II	Rodrick “Rick” Ragland		
Engineering Manager	Michael McCord		
Dir., Member Services	Thom Moore		
Accounting Manager	Suzy Howard		
Billing/HR Supervisor	Helen Jo Wallin		
IT Manager	Glenn Barleben		

IV. Communication Plan

COMMUNICATIONS

1. Incoming Call Handling Procedures:

During an emergency, the Cooperative’s telephone system will be staffed around the clock by Cooperative personnel or Answering Service to receive information from customers, emergency authorities, and others. Also, personnel will be on duty during normal business hours to receive outage reports from customers appearing in person.

2. Coordination With Visiting Work Crews:

Visiting work crews will be assigned to work with Farmers’ Electric’s work crews equipped with two-way radios and cellular telephones.

3. Critical Loads:

When telephone service is not available, the Cooperative will attempt to notify critical loads either before or at the onset of an electrical emergency through broadcast radio and television announcements, working with law enforcement officers, emergency operations centers and utility personnel in the field.

4. Reporting Requirements:

The CEO/General Manager will assign responsibilities for reporting to the Public Regulation Commissions, local emergency officials, and others.

**PROGRAM FOR IDENTIFYING AND COMMUNICATING
WITH MEMBERS WITH MAJOR, LIFE-SUSTAINING EQUIPMENT AND
DESCRIPTION OF REGISTRY**

Farmers' Electric Cooperative makes every effort to be aware of members who have life-sustaining electric equipment. It is the responsibility of the members to inform the Cooperative of special medical needs. However, the Cooperative attempts to identify these members by asking new members at the time of establishing an account, whether any person at that service location requires life-sustaining equipment. We also remind members through articles in "Enchantment" magazine and newsletter articles that the Cooperative needs to be informed of special needs.

A sample registration form is found below. This registry is accessible to appropriate personnel including CEO/General Manager, Receptionist, Dispatcher, Director of Member Service, Linemen, and engineering personnel. The list includes map location numbers to allow utility personnel to identify these locations on system maps. Our customer accounting system includes special notations for customers with critical needs, to alert personnel prior to initiating disconnection procedures.

Methods to communicate with these members during emergencies, when telephone service is not available includes visits by linemen and other utility personnel and working through law enforcement officers and emergency medical personnel in the field.

**(CONFIDENTIAL, FOR AUTHORIZED EMPLOYEES ONLY)
REGISTRY OF CUSTOMERS WITH SPECIAL, IN-HOUSE,
LIFE-SUSTAINING EQUIPMENT**

The members of Farmers' Electric Cooperative with special, in-house, life-sustaining equipment are registered on the following form. The CEO/General Manager, Receptionist, Dispatcher, and other appropriate personnel will take extra precautions to minimize service interruptions to these locations. We will also attempt to warn these members in case of emergency and inform them of any planned service interruption.

SUB # _____

REGISTRY OF CONSUMERS WITH LIFE-SUSTAINING EQUIPMENT

ACCOUNT NAME: _____

PERSON ON LIFE SUPPORT: _____

ADDRESS: _____

DIRECTIONS TO HOME: _____

PHONE NUMBER: _____

ACCOUNT NUMBER: _____

BOOK AND SEQUENCE NUMBER: _____

SPECIAL EQUIPMENT: _____

STANDBY GENERATOR: YES _____ NO _____ Watts _____

BATTERY BACKUP: YES _____ NO _____

BATTERY LIFE: _____

ADDITIONAL INFORMATION: _____

V. Pre-stocking of Supplies

In the near-term, FEC keeps adequate material on hand at six warehouse locations throughout our service area. In the long-term, FEC has or is procuring sufficient materials to continue normal new construction activities, complete scheduled maintenance, and system improvements, and to repair poles and equipment damaged by accidents, storms, or wildfires.

VI. Staffing During Emergencies

- The issue of personnel is a major variable in disaster recovery and other emergencies. Assess and evaluate number of personnel available for duty, resources available and location of operation.
- Assess and evaluate availability, condition and needs of employees due to impact on employees' homes and families directly affected by loss of personal property and shelter or pandemic.
- Assess and evaluate the need and process of hiring new employees to fill the spots left by injuries, fatalities, or illness.
- Assess and evaluate third-party vendors: i.e., line crew contractors that may be available to assist.
- Cross-training and job-sharing will assist in mitigating potential losses.
- In the event of an emergency and the potential for loss of personnel, the following items are important to the continuity of service:
 - Safety of employees and their families.
 - Preparation for any loss of personnel.
 - Prioritize business functions.
 - Action plans developed.
- Administration of Cooperative's safety program & policies, emergency preparedness plan and investigations.
- Adhere to federal and state official's mandates and recommendations.
- Assist Accounting Services with records access and management for payroll, benefits, workers' compensation/disability, risk management, certificates of insurance, property, organizational chart, pay rates and board policies.
- FEC participates in a New Mexico Distribution Cooperative Mutual Aid Agreement to provide assistance in the form of manpower and equipment during an emergency.

VII. Weather Related Hazards Identification

- a.
 - Weather forecasts through weather apps and local news
 - Alerts from Texas Division of Emergency Management
 - Alerts from the National Weather Service
 - Information provided by our wholesale power supplier, Western Farmers Electric Cooperative (WFEC)
- b.
 - Identification of available employees
 - One Crew from each of FEC's six service areas always on standby
 - Notification to key individuals
 - Group text

VIII. Annexes:

- a. **Cooperative Annexes:**

i. Cold Weather Emergency

OBJECTIVE

Farmers' Electric Cooperative (FEC) recognizes that temperature extremes can significantly increase total load service requirements on the FEC electric distribution system. System emergencies can originate within the FEC distribution system as well as outside the FEC distribution system including our Transmission Service Provider, Southwestern Public Service Company (SPS) and the greater bulk electric system managed by the Southwest Power Pool (SPP).

The Southwest Power Pool (SPP) is the Reliability Coordinator and Balancing Authority for the area served by Farmers' Electric Cooperative (FEC). FEC's wholesale transmission service supplier, Southwestern Public Service Company (SPS) is the area Generator Operator, Transmission Planner and Transmission Operator.

FEC's Objective is to provide timely response to any operating directives issued by SPS and/or SPP to minimize FEC's load impact to the Bulk Electric System.

In addition, FEC's Objective is to construct, operate, and maintain the FEC distribution system in a manner consistent with sound utility practices in order to provide safe, reliable service to consumers.

SPP SYSTEM ALERT DESCRIPTIONS

Descriptions of common Bulk System Emergency reliability events are provided below in increasing order of severity:

Advisories raise awareness and do not require general audiences to take action. SPP member utilities should follow applicable procedures. Energy Emergency Alerts indicate all available generation has been committed to meet region-wide demand. As conditions worsen, voluntary conservation or service interruptions may be necessary to prevent uncontrolled outages.

Normal Operations: SPP has enough generation to meet demand and available reserves, and it foresees no extreme or abnormal threats to reliability.

Weather Advisory: Declared when extreme weather is expected in SPP's reliability coordination service territory.

Resource Advisory: Declared when severe weather conditions, significant outages, wind-forecast uncertainty and/or load-forecast uncertainty are expected in SPP's balancing authority area.

Conservative Operations Advisory: Declared when SPP determines there is a need to operate its system conservatively based on weather, environmental, operational, terrorist, cyber or other events.

Energy Emergency Alert Level 1: Declared when all available resources have been committed to meet obligations, and SPP is at risk of not meeting required operating reserves.

Energy Emergency Alert Level 2: Declared when SPP can no longer provide expected energy requirements, or when SPP foresees or has implemented procedures up to, but excluding, service interruptions to maintain regional reliability.

Energy Emergency Alert Level 3: At this level, SPP is utilizing operating reserves such that it is carrying reserves below the required minimum and has initiated assistance through its Reserve Sharing Group. SPP foresees or has implemented firm load obligation interruption. Before requesting an EEA 3, SPP will have already provided the appropriate internal notifications to its Market Participants.

Restoration Event: Defined as a major or catastrophic grid outage which could be a total or partial regional blackout, island situation or system separation.

EVENT RESPONSE PROCEDURE

Bulk Electric System (BES) (SPS and/or SPP) Initiated Events:

There is potential for a Cold Weather Emergency to originate outside the FEC distribution system, through our Transmission Service Provider, SPS and/or through the SPP. FEC will receive operating messages regarding Bulk-System Emergencies through SPS.

SPS Transmission Emergency Operations Personnel responsible for communicating with FEC maintain current contact information for FEC CEO/General Manager, Line Superintendent 1, Line Superintendent 2 and Manager of Engineering.

Upon receiving notice from SPS that the SPP has issued a **Conservative Operations Advisory**, FEC shall begin issuing voluntary load conservation appeals as outlined in FEC's Communications Plan.

FEC Personnel, upon receiving an **Energy Emergency Alert Level 3**, shall implement the required load shed without delay, and within 30 minutes in accordance with FEC's Load Shed Plan.

When notified by SPS that the requirement for load shed has been lifted, FEC Personnel shall return the FEC system to normal operations in an expedient manner.

FEC System Operations:

The failure of certain FEC components, such as a substation transformer or transmission circuit, can impact large numbers of consumers over an extended period.

Substations:

To ensure reliable operation of substations and the transmission system FEC shall:

1. FEC operations personnel shall visually inspect each substation at a minimum of one-time per month and record data on the station inspection form. Operations personnel shall also check readings and gauges any other time they are at a particular substation. Any deficiencies shall be noted on the inspection form and communicated directly to the Line Superintendent so that corrective action can be scheduled.
2. FEC engineering personnel shall track transformer loading to be used in conjunction with load forecasting to ensure the transformer capacity is sufficient to meet peak load requirements.
3. Most substations have automatic cooling fans mounted to the transformer designed to turn the fans on when the transformer temperature rises to a predetermined value. As a safety mechanism, FEC operations personal shall manually turn the transformer cooling fans on at the beginning of June and leave the fans running through the first of September.
4. In the case of a failed substation transformer, it may be possible to restore service from other substations/circuits.

Transmission System:

FEC operates 267 miles of 69kV transmission line. Much of this system is "looped" so that a damaged segment may be isolated, and service restored in a relatively short period of time. The damaged segment can remain de-energized for repairs.

1. FEC operations personnel shall visually inspect 100 percent of the transmission network in each of ten-months out of the year. Any deficiency shall be recorded and reported directly to the Line Superintendent so that corrective action can be taken.
2. Line sections that have been damaged shall be repaired immediately, pending weather conditions, to restore they system to normal operations.

Distribution System:

Ice-Storms and Snowstorms present unique challenges for distribution operations. Significant damage can occur in a relatively short period of time and access to damaged line sections can be difficult due to snow and mud.

FEC receives advance notice of approaching ice and snow events from our wholesale power supplier, Western Farmers' Electric Cooperative (WFEC). Based on potential storm impacts in the FEC service area FEC shall consider activation of pre-emptive portion of the Emergency Restoration Plan (ERP).

COMMUNICATIONS WITH CONSUMERS

During a System Emergency it is important to activate the Communication Plan to keep consumers informed of operating conditions and efforts to maintain or restore service.

FEC Customer Service Representatives (CSRs) will be provided with relevant information to communicate to consumers as they call into the office. Relevant information may include:

1. Status and nature of a Load Shed event
2. Collection of outage data
3. Advise consumers of energy saving measures including the FEC website

FEC shall also provide information on energy saving tips through our website, FECNM.org; FEC newsletter "*Power Source*"; and through our state-wide publication "*enchantment*" magazine.

EVENT REPORTING PROCEDURE

Management Personnel shall be responsible for reporting to the New Mexico Public Regulation Commission (NMPRC) and Texas Public Utility Commission (TPUC).

Reports shall be filed in accordance with reporting requirements in FEC Policy EOP-004-1, Event Response and Reporting Plan.

PRE-EVENT PLAN REVIEW

This Plan shall be periodically reviewed with Operations Personnel and those with Management Reporting Responsibility.

POST-EVENT PLAN REVIEW

Following a Cold Weather Emergency Event, FEC management personnel shall conduct meetings to review lessons learned from the Event. Review shall include sufficiency of supplies and personnel available to meet the conditions experienced. In addition, a review of all relevant internal and external communications shall be reviewed to ensure relevant information was received and communicated to effectively manage the Event.

DATA RETENTION

FEC shall keep data related to all incidents subject to reporting under this Plan for a period of five-years.

REFERENCE DOCUMENTS:

NMPRC Rule; 17.9.560.15 E. (4) NMAC

TPUC Rule; 16.2.25 (C) 25.53

VERSION HISTORY

Version	Date	Action	Change Tracking
1	3/22/2022	New Plan	New Plan
2	3/10/2023	Update	

ii. Hot Weather Emergency

OBJECTIVE

Farmers' Electric Cooperative (FEC) recognizes that temperature extremes can significantly increase total load service requirements on the FEC electric distribution system. System emergencies can originate within the FEC distribution system as well as outside the FEC distribution system including our Transmission Service Provider, Southwestern Public Service Company (SPS) and the greater bulk electric system managed by the Southwest Power Pool (SPP). The failure of certain FEC components, such as a substation transformer or transmission circuit, can impact large numbers of consumers over an extended period.

The Southwest Power Pool (SPP) is the Reliability Coordinator and Balancing Authority for the area served by Farmers' Electric Cooperative (FEC). FEC's wholesale transmission service supplier, Southwestern Public Service Company (SPS) is the area Generator Operator, Transmission Planner and Transmission Operator.

FEC's Objective is to provide timely response to any operating directives issued by SPS and/or SPP to minimize FEC's load impact to the Bulk Electric System.

In addition, FEC's Objective is to construct, operate, and maintain the FEC distribution system in a manner consistent with sound utility practices in order to provide safe, reliable service to consumers.

SPP SYSTEM ALERT DESCRIPTIONS

Descriptions of common Bulk System Emergency reliability events are provided below in increasing order of severity:

Advisories raise awareness and do not require general audiences to take action. SPP member utilities should follow applicable procedures. Energy Emergency Alerts indicate all available generation has been committed to meet region-wide demand. As conditions worsen, voluntary conservation or service interruptions may be necessary to prevent uncontrolled outages.

Normal Operations: SPP has enough generation to meet demand and available reserves, and it foresees no extreme or abnormal threats to reliability.

Weather Advisory: Declared when extreme weather is expected in SPP's reliability coordination service territory.

Resource Advisory: Declared when severe weather conditions, significant outages, wind-forecast uncertainty and/or load-forecast uncertainty are expected in SPP's balancing authority area.

Conservative Operations Advisory: Declared when SPP determines there is a need to operate its system conservatively based on weather, environmental, operational, terrorist, cyber or other events.

Energy Emergency Alert Level 1: Declared when all available resources have been committed to meet obligations, and SPP is at risk of not meeting required operating reserves.

Energy Emergency Alert Level 2: Declared when SPP can no longer provide expected energy requirements, or when SPP foresees or has implemented procedures up to, but excluding, service interruptions to maintain regional reliability.

Energy Emergency Alert Level 3: At this level, SPP is utilizing operating reserves such that it is carrying reserves below the required minimum and has initiated assistance through its Reserve Sharing Group. SPP foresees or has implemented firm load obligation interruption. Before requesting an EEA 3, SPP will have already provided the appropriate internal notifications to its Market Participants.

Restoration Event: Defined as a major or catastrophic grid outage which could be a total or partial regional blackout, island situation or system separation.

EVENT RESPONSE PROCEDURE

Bulk Electric System (BES) (SPS and/or SPP) Initiated Events:

There is potential for a Hot Weather Emergency to originate outside the FEC distribution system, through our Transmission Service Provider, SPS and/or through the SPP. FEC will receive operating messages regarding Bulk-System Emergencies through SPS.

SPS Transmission Emergency Operations Personnel responsible for communicating with FEC maintain current contact information for FEC CEO/General Manager, Line Superintendent 1, Line Superintendent 2 and Manager of Engineering.

Upon receiving notice from SPS that the SPP has issued a **Conservative Operations Advisory**, FEC shall begin issuing voluntary load conservation appeals as outlined in FEC's Communications Plan.

FEC Personnel, on receiving an **Energy Emergency Alert Level 3**, shall implement the required load shed without delay, and within 30 minutes in accordance with FEC's Load Shed Plan.

When notified by SPS that the requirement for load shed has been lifted, FEC Personnel shall return the FEC system to normal operations in an expedient manner.

FEC System Operations:

Substations:

To ensure reliable operation of substations and the transmission system:

1. FEC operations personnel shall visually inspect each substation at a minimum of one-time per month and record data on the station inspection form. Operations personnel shall also check readings and gauges any other time they are at a particular substation. Any deficiencies shall be noted on the inspection form and communicated directly to the Line Superintendent so that corrective action can be scheduled.
2. FEC engineering personnel shall track transformer loading to be used in conjunction with load forecasting to ensure the transformer capacity is sufficient to meet peak load requirements.
3. Most substations have automatic cooling fans mounted to the transformer designed to turn the fans on when the transformer temperature rises to a predetermined value. As a safety mechanism, FEC operations personnel shall manually turn the transformer cooling fans on at the beginning of June and leave the fans running through the first of September.
4. In the case of a failed substation transformer, it may be possible to restore service from other substations/circuits.

Transmission System:

FEC operates 267 miles of 69kV transmission line. Much of this system is "looped" so that a damaged segment may be isolated and service restored in a relatively short period of time. The damaged segment can remain de-energized for repairs.

1. FEC operations personnel shall visually inspect 100 percent of the transmission network in each of ten-months out of the year. Any deficiency shall be recorded and reported directly to the Line Superintendent so that corrective action can be taken.
2. Line sections that have been damaged shall be repaired immediately, pending weather conditions, to restore they system to normal operations.

COMMUNICATIONS WITH CONSUMERS

During a System Emergency it is important to activate the Communication Plan to keep consumers informed of operating conditions and efforts to maintain or restore service.

FEC Customer Service Representatives (CSRs) will be provided with relevant information to communicate to consumers as they call into the office. Relevant information may include:

1. Status and nature of a Load Shed event
2. Collection of outage data
3. Advise consumers of energy saving measures including the FEC website

FEC shall also provide information on energy saving tips through our website, FECNM.org; FEC newsletter "*Power Source*" and through our state-wide publication "*enchantment*" magazine.

EVENT REPORTING PROCEDURE

Management Personnel shall be responsible for reporting to the New Mexico Public Regulation Commission (NMPRC) and Texas Public Utility Commission (TPUC).

Reports shall be filed in accordance with reporting requirements in FEC Policy EOP-004-1, Event Response and Reporting Plan.

PRE-EVENT PLAN REVIEW

This Plan shall be periodically reviewed with Operations Personnel and those with Management Reporting Responsibility.

POST-EVENT PLAN REVIEW

Following a Hot Weather Emergency Event, FEC management personnel shall conduct meetings to review lessons learned from the Event. Review shall include sufficiency of supplies and personnel available to meet the conditions experienced. In addition, a review of all relevant internal and external communications shall be reviewed to ensure relevant information was received and communicated to effectively manage the Event.

DATA RETENTION

FEC shall keep data related to all incidents subject to reporting under this Plan for a period of five-years.

REFERENCE DOCUMENTS:

NMPRC Rule; 17.9.560.15 E. (4) NMAC

TPUC Rule; 16.2.25 (C) 25.53

VERSION HISTORY

Version	Date	Action	Change Tracking
1	3/22/2022	New Plan	New Plan
2	3/10/2023	Update	

iii. Load Shed

OBJECTIVE

To comply with the North American Electric Reliability Corporation (NERC) and/or Southwest Power Pool (SPP) Regional Reliability Standards. NERC has been designated as the Electric Reliability Organization by the Federal Energy Regulatory Commission (FERC). Standard IRO-001 requires that Reliability Coordinators have the authority, plans, and agreements in place to immediately direct reliability entities within their Reliability Coordinator Area to re-dispatch generation, reconfigure transmission, or reduce load to mitigate critical conditions to return the system to a reliable state. The Southwest Power Pool (SPP) is the Reliability Coordinator for the area served by Farmers' Electric Cooperative (FEC).

PROCEDURE

The Standard provides that the SPP shall have clear decision-making authority to act and to direct actions to be taken by FEC and others within the SPP Reliability Coordinator area to preserve the integrity and reliability of the Bulk Electric System. For FEC this is likely to take the form of load reduction.

It is most likely that any request to reduce load on the FEC system will come from Southwestern Public Service Company (SPS), and FEC's response must be taken without delay, and within 30 minutes.

Implementation/activation of FEC's load shed program (**Attachment 1 of this Policy**) will be given by the FEC Line Superintendent(s), CEO/General Manager, or individual designated in their absence.

In the event that FEC has determined that actions required by SPP and/or SPS cannot be physically implemented or unless such actions would violate safety, equipment, or regulatory or statutory requirements, the FEC Line Superintendent(s), CEO/General Manager, or individual designated in their absence shall immediately inform the SPP and/or SPS of the inability to perform the directive so that the SPP and/or SPS may implement alternate remedial actions. Contact information for SPS is contained in **Attachment 2 of this Policy**.

CURTAILMENT PRIORITIES

During times of emergency or generation shortage Farmers' Electric Cooperative may choose to curtail or terminate service to our members. In addition, a schedule or rotating blackouts may be implemented. These procedures would begin with services least critical to the preservation of human life.

The following is a list of consumer categories beginning with the first loads to be considered for curtailment or termination:

1. Irrigation accounts
2. Commercial establishments
3. Industrial Plants
4. Residential Consumers
5. Water treatment facilities
6. Homes with electrical life-supporting equipment
7. Hospitals and emergency care facilities

RESTORATION OF SERVICE PRIORITIES

Cooperative personnel will concentrate repair efforts beginning with services most critical to the preservation of human life. The following is a list of services in the order that they would receive attention.

1. Hospitals and emergency care facilities
2. Homes with electrical life-support equipment
3. Water treatment facilities
4. Residential consumers
5. Industrial plants
6. Commercial establishments
7. Irrigation loads

In addition to priorities concerning community health and safety, crews will be assigned to defined areas. Generally, crews will concentrate on a given feeder, working to the end or to a sectionalizing point, and the returning to restore service on single phase lines or taps off the feeder. Restorations will be done systematically, avoiding pressure from individuals for special attention. However, one or more crews may be assigned to locations where special hazards exist or where especially critical loads require immediate attention. When not on special assignment, these crews may be used to repair individual services.

TRAINING

This Policy, and FEC's load shed program shall be reviewed by Operations Personnel once each calendar year.

DATA RETENTION

In order to confirm that FEC did comply with SPP and/or SPS directives, FEC shall keep all evidence that could include written log of SPP and/or SPS directives and written record of FEC response including date and time associated with load shed activities.

In addition, FEC shall keep all evidence in support of any inability to comply, and that FEC communicated this inability immediately to the SPP and/or SPS.

This data shall be kept a minimum of two years.

VERSION HISTORY

<u>Version</u>	<u>Date</u>	<u>Action</u>	<u>Change Tracking</u>
0	2/20/2009	Effective Date	New
1	12/27/2010	Revise Annual Review Language	Revision
2	07/07/2017	Update NERC Standard Reference	Revision

Attachment 1

Emergency Response Plan for Load-Shedding at the Request of SPP and/or Wholesale Power Provider

In the event that the Southwest Power Pool (SPP) or our wholesale power provider requests FEC to shed load, FEC shall respond immediately, without delay, and implement Load-Shed within 30 minutes of request.

A Load Shed request would most likely occur during our peak summer months. For FEC, irrigation load during the summer months of June, July, August, and September creates our peak, and in an emergency, when asked to shed load, irrigation would be our most likely targeted load.

Bumping some of our more loaded irrigation circuits would shed considerable load. As affected members call in their outages, FEC staff shall inform consumers of the reason and need for the Load-Shed and the possibility of revolving outages. FEC shall monitor these circuits as they start to load up again, and if necessary, FEC shall bump other irrigation circuits on an as needed, revolving basis.

If a longer duration of time is requested by SPP and/or our wholesale power provider, FEC shall accomplish Load-Shed on a revolving time schedule depending on the amount of load that needs to be shed. FEC shall take reasonable care to avoid turning off hospitals, nursing homes, schools, government offices, municipal water supplies, prisons, airports, and other critical need loads.

Rural feeders that serve primarily irrigation and dairy loads could be turned off for a few hours on a revolving time schedule. Most of the dairies on FEC have back-up generators and any load shedding involving the dairies would be a coordinated effort with the dairy receiving some warning before power was lost to the greatest extent possible. **However, FEC shall shed the required load within the 30-minute time constraint.**

Circuits that could be bumped or turned off include:

██████████	Circuit #1	Peak load – 8.4 MW
██████████	Circuit #2	Peak load – 4.4 MW
██████████	Circuit #2	Peak load – 7.9 MW
██████████	Circuit #1	Peak load – 5.8 MW
██████████	Circuit #2	Peak load – 2.5 MW
██████████	Circuit #6 ██████████	Peak load – 5.6 MW

Attachment 2

SPS Contact Information

Transmission Control Center Manager	Kyle McMenamin	██████████
Transmission Control Center Assistant Manager	Mike Harrison	██████████
Operations / Outage Coordination Engineer	Brittany Gray	██████████
Outage Coordination Engineer	Mike Rebstock	██████████
Network Reliability Leader	Mike Mills	██████████
Network Reliability Leader	Jerrold Loven	██████████
Transmission Control Center	Transmission Operator (24/7)	██████████
Transmission Control Center	Transmission Operator (24/7)	██████████
Transmission Control Center	Emergency Cell Number	██████████
Cell phones not in use unless there is a phone system failure	Alternate Emergency Cell Number	██████████
Transmission Operations Control Center	Toll Free Customer Call-In Number	██████████

Distribution Control Center	Joey Zahn (Manager)	[REDACTED]
	Dago Rodriguez (Supervisor)	[REDACTED]
	North Desk	[REDACTED]
	South Desk	[REDACTED]
	New Mexico	[REDACTED]
Transmission Line Work Request	BJ Hatfield (Construction Mgr)	[REDACTED]
	Matt Winfield (Supervisor)	[REDACTED]
	Blaine Kirkpatrick (NM Superintendent)	[REDACTED]

List Updated 09/28/2015, 9/30/2015 & 10/8/2015.

List Updated 10/03/2016, 9/25/2017, 9/24/2018, 9/10/2019

It is recognized that the names of individuals assigned as Manager or Team Lead will change over time.

SPP RC and BA Contact Numbers:

SPP RC 501-614-3900, Option 1 - 501-804-6580

RC desk cell phone (Chenal) – 501-804-6580

RC desk cell phone (Maumelle) – 501-804-6583

security@spp.org

SPPEvents@spp.org

SPP BA 501-614-3900, Option 2 - 501-804-3064

BA desk cell phone – 501-804-3064

balancing@spp.org

Table of Contents

1	<u>Introduction/Executive Summary</u>
1.1	<u>Purpose of the Plan</u>
1.2	<u>Objectives of the WMP</u>
1.3	<u>Utility Profile and History</u>
1.4	<u>The Service Area</u>
2	<u>Overview of Utility's Fire Prevention Strategies</u>
3	<u>Utility Asset Overview</u>
4	<u>Risk Analysis and Risk Drivers</u>
4.1	<u>Fire Risk Drivers Related to Construction and Operations</u>
4.2	<u>Fire Risk Drivers Related to the Service Area</u>
4.3	<u>Key Risk Impacts</u>
4.4	<u>Wildfire History and Outlook</u>
4.4.2	<u>Wildland Urban Interface</u>
4.5	<u>Fire Threat Assessment Mapping</u>
5	<u>Wildfire Prevention Strategy and Programs</u>
5.1	<u>Transmission and Distribution System Operational Practices</u>
5.1.1	<u>De-energization – Public Safety Power Shutoff</u>
5.1.2	<u>Recloser Operational Practices</u>
5.2	<u>Infrastructure Inspections and Maintenance</u>
5.2.1	<u>Definition of Inspection Levels</u>

[5.2.2 Safety Patrol Inspections of Transmission and Distribution Lines](#)

[5.2.3 Detailed Inspections of Transmission and Distribution Lines](#)

[5.2.4 Wood Pole Testing and Inspection](#)

[5.2.5 Substation Inspections](#)

[5.3 Vegetation Management \(VM\)](#)

[5.3.1 Vegetation to Conductor Clearance](#)

[5.3.2 Vegetation Trimming Standards](#)

[5.3.3 VM Trimming and Inspection Schedule](#)

[5.3.4 Hazard Trees](#)

[5.3.5 Controlling Incompatible Vegetation](#)

[5.4 Fire Mitigation Construction](#)

[5.4.1 Avian Protection Program](#)

[5.5 Emerging Technologies](#)

[6 Emergency Response](#)

[6.1 Preparedness and Response Planning](#)

[6.1.1 Emergency Management Communication and Coordination](#)

[6.1.2 Jurisdictional Structure](#)

[6.1.3 Public Agency and Customer Communications for Outages](#)

[6.1.4 Community Outreach](#)

[6.2 Restoration of Service](#)

[6.2.1 Service Restoration Process](#)

[7 Performance Metrics and Monitoring](#)

[7.1 Plan Accountability](#)

[7.2 Monitoring and Auditing of the WMP](#)

[7.2.1 Identifying Deficiencies in the WMP](#)

[7.3 Performance Metrics](#)

[7.4 Programmatic QA/QC processes](#)

[7.4.1 Transmission and Distribution System Inspection QC Process](#)

[7.4.2 Vegetation Management QC Process](#)

[7.5 Plan Approval Process](#)

[7.5.1 Public Comment](#)

[7.5.2 Board Presentation](#)

[Appendix A: Plan and Mapping Disclaimers](#)

Table of Tables

[Table 1. Mitigation Strategies/Activities](#)

[Table 2. Asset Overview](#)

[Table 3. Activities That Address Wildfire Risk Factors](#)

[Table 4. Inspection Program Summary](#)

[Table 5. Performance Metrics \(Optional\)](#)

Table of Figures

[Figure 1. Service Area \(EXAMPLE\)](#)

[Figure 2. Historic Wildfire Perimeters 2000-2019 \(Example\)](#)

[Figure 3. Wildland Urban Interface \(EXAMPLE\)](#)

[Figure 4. Service Territory WHP Overview \(EXAMPLE\)](#)

[Figure 5. General Land Ownership \(EXAMPLE\)](#)

Template key

Red text=Instructional Information

Black text=Sample Language

1 Introduction/Executive Summary

Since the state of New Mexico does not currently have Wildfire Mitigation Plan (WMP or Plan) requirements, this plan was developed to be consistent with current industry best management practices. While WMP requirements are under development and will vary by state, the plans in general are likely to direct utilities to develop operational policies and practices to prevent, prepare for and respond to wildfire events. WMPs are likely to be evaluated or updated on an annual basis and may be subject to board approval.

Fire mitigation plays an essential role in FEC's operational practices. Its existing policies, programs and procedures are designed to directly or indirectly manage or reduce this risk. Over the years, FEC has adopted additional fire mitigation programs to adjust to changes in the burning environment, adopted technological advances and improved operational practices to further mitigate the potential for ignitions and more effectively respond to apex wildfire risk conditions.

Purpose of the Plan

The Plan describes the FEC's strategies, programs, and procedures to mitigate the threat of electrical equipment ignited wildfires, and addresses the unique features of its service territory, such as topography, weather, infrastructure, grid configuration, and areas most prone to wildfire risks. This includes the maintenance of its transmission and distribution (T&D) assets as well as the management of vegetation in the ROWs that contain these assets.

FEC's Board of Directors reviews, and approves the Plan as needed, while the Manager is responsible for its implementation. Primary accountability for plan implementation resides with the Line Superintendent.

Objectives of the WMP

The main objective seeks to implement an actionable plan to create increased reliability and safety while minimizing the likelihood that FEC assets may be the origin or contributing factor in the ignition of a wildfire. The mitigation programs and strategies will comply with current and anticipated New Mexico State law, and National Electric Safety Code (NESC) regulations and guidelines. To help develop the Plan, FEC compared emerging technologies that not only reduce the likelihood of a service interruption, but also minimize the risk of ignition from the fault causing the outage.

The secondary objective is to measure, through the annual evaluation of certain performance metrics, the effectiveness of the specific wildfire mitigation strategies. Where a particular action, program component or protocol proves unnecessary or ineffective, FEC will assess whether modification or replacement is suitable.

Utility Profile and History

- FEC founded in 1938, the second cooperative established in New Mexico

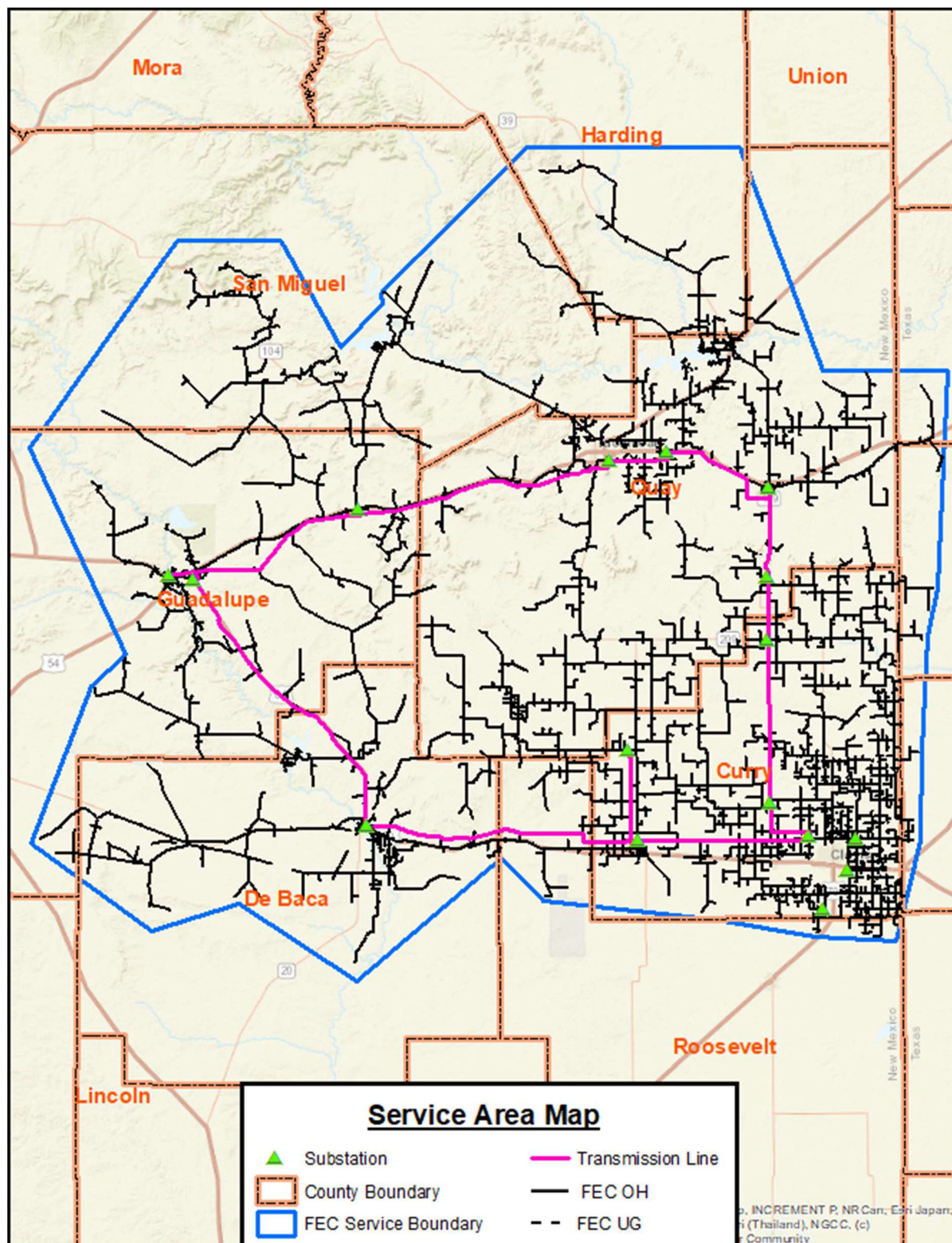
- FEC serves 13,400 Active metered Accounts
- FEC, headquartered in Clovis, with branch offices in Fort Sumner and Santa Rosa, is a member-owned and controlled electric distribution cooperative providing service to some 7,200 members (approximately 13,400 active meters) including portions of counties of Curry, De Baca, Guadalupe, Harding, Quay, Roosevelt, and San Miguel in New Mexico, and portions Deaf Smith, Oldham, Bailey and Parmer counties along the Texas border.
- Communities served include rural areas around Clovis & Tucumcari, and the communities of Melrose, House, Fort Sumner, Santa Rosa, Grady, San Jon & Logan
- FEC provides service over more than 4,300 miles of transmission & distribution line, spanning roughly 11,000 square miles of service territory – 3 meters per mile of line. Service crews are disbursed throughout the service area, stationed in 6 separate locations.
- FEC serves a diversified membership base with roughly 24% of sales to Farm and Residential; 23% Irrigation; and 53% Small Commercial/Large Power & Industrial loads. Our largest member, SW Cheese, represented 26% of total sales in 2021
- FEC is governed by a 7-member board of Trustees, each elected by the membership to serve a three-year term with a staggered re-election process. Trustees meet monthly to review operations and financial data; however, Trustees are not responsible for day-to-day oversight of operations.
- Day-to-day business leadership is provided by the following Department Positions:
 - CEO/General Manager, responsible for general oversight;
 - Director of Member Services, responsible for communications and direct customer relations;
 - Manager of Accounting; responsible for accurate and timely accounting of financial assets;
 - Manager of Engineering; responsible for coordination system planning and system continuity;
 - Customer Services & Human Resource Manager, responsible for customer billing and information systems as well as Human Resource responsibilities;
 - Information Technology Director, responsible for computer/data system performance and security;
 - Line Superintendent 1, responsible for day to day operations, overall reliability, system planning, materials supplies, and transportation.
 - Line Superintendent 2, also responsible for day to day operations, overall reliability, system planning, materials supplies, and transportation

The Service Area

- FEC, headquartered in Clovis, with branch offices in Fort Sumner and Santa Rosa with warehouses in Melrose, San Jon and Logan. Located on main highways US 60/US 70/US 84,
- US HWY 54, Interstate 40

- FEC provides service to counties of Curry, De Baca, Guadalupe, Harding, Quay, Roosevelt, and San Miguel in New Mexico, and portions of Deaf Smith, Oldham, Bailey, and Parmer counties along the Texas border
- FEC has roughly 11,000 square miles of service territory
- FEC topography consist of farm and ranch land to native grasses very few trees and abundance of succulent plants
- FEC service are climate consist of high desert with an average rain fall of 17 inches per year and an average temperature of 58deg, 92 being the hottest and 23 being the coldest
 -
- **Service area boundary map (Figure 1),**
 - The map below shows the boundaries of the area served by this Cooperative. The service area encompasses some 10,500 square miles. No change in boundaries is foreseen at this time. The map shows the railroad lines, and federal and state highways. Also, the Cooperative serves the Ute and Conchas Reservoirs on the Canadian River, and the Sumner Reservoir and the Santa Rosa Dam on the Pecos River

Figure 1. Service Area



Overview of Utility's Fire Prevention Strategies

This WMP integrates and interfaces with FEC's existing operations plans, asset management, and engineering principles, which are themselves subject to change. Future iterations of the WMP will reflect any changes to these strategies and will incorporate new best management practices as they are developed and adopted.

Table 1 summarizes FEC's five mitigation components with associated programs and activities that support FEC's ongoing commitment to wildfire prevention and mitigation.

Table 1. Mitigation Strategies/Activities

DESIGN AND CONSTRUCTION
Strategic undergrounding of distribution lines – N/A
Field recloser to vacuum-type breaker change-out program - NO
Covered jumpers and animal guards - YES
Non-expulsion fuses in select high-risk areas - NO
Avian protection construction standards - NO
Increase overhead wire spacing to reduce wire to wire contact - NO
Substation perimeter fencing for security and protection - YES
INSPECTION AND MAINTENANCE
Infrared inspections of substation equipment - YES
Unmanned Aerial Vehicle (UAV) T&D line inspections - YES
UAV IR and LiDAR inspection program - NO
Wood pole intrusive inspection and testing - YES
Enhanced T&D vegetation right-of-way maintenance - YES
INSPECTION AND MAINTENANCE (cont.)
Distribution system line patrols and detailed inspections - YES
T&D system vegetation management program - YES
Increased removal rate of undesirable trees on right-of-way's - NO

Enhanced vegetation management prior to fire season - NO
Thermal imaging cameras - YES
Enhanced line patrols during fire season - NO
OPERATIONAL PRACTICES
Work procedures and Fire Hazard training for persons working in locations with elevated fire risk conditions - NO
Community outreach/wildfire safety awareness - YES
Contractor/staff safety training and orientation for vegetation management work - YES
Alternate recloser practices during fire weather - NO
Fire suppression equipment on worksite during fire season - NO
Provide liaison to county offices of emergency services (OES) during fire event - NO
SITUATIONAL AWARENESS
Weather Monitoring in the service area - YES
Utility-owned weather stations - NO
Monitoring active fires in the Southwest - NO
RESPONSE AND RECOVERY
Pre-emptive de-energization protocols - NO
Coordination with local Department of Emergency Management - NO
Customer assistance programs for post-disaster recovery - YES
Line patrols before re-energization - YES
Emergency Restoration Plan - YES

Utility Asset Overview

- FEC is headquartered in Clovis with satellite offices in Ft Sumner, Santa Rosa, warehouses in Melrose, San Jon, and Logan

- FEC does not own or control any electrical generation resources and is an all-requirements wholesale purchaser of electrical energy from Western Electric Cooperative, headquartered in Anadarko, Oklahoma
- FEC has 2 interchanges, 2 switching stations and 14 substations
- FEC consist of 261 miles of transmission line with a voltage of 69kV, 3747 miles of overhead primary line with a voltage of 14.4 or lower, 263 miles of secondary overhead, 76 miles of primary underground, 28 miles of secondary underground

Table 2 provides a high-level description of FEC's T&D assets.

Table 2. Asset Overview

ASSET CLASSIFICATION	ASSET DESCRIPTION
Transmission Line Assets	Approximately 261 miles of conductor, transmission structures and switches at 69 kilovolt (kV).
Distribution Line Assets	Approximately 3747 miles of overhead (OH) and 76 miles of underground (UG) conductor, cabling, transformers, voltage regulators, capacitors, switches, lined protective devices operating at or below 14.4kV.
Substation Assets	Major equipment such as power transformers, voltage regulators, capacitors, reactors, protective devices, relays, open-air structures, switchgear and control houses in 18 substation/switchyard facilities.

Risk Analysis and Risk Drive

Fire Risk Drivers Related to Construction and Operations

FEC staff evaluated other utility's fire causes and applied its own field experience to determine the critical potential risk drivers. The categories listed below were identified as having the potential for causing powerline sparks and ignitions:

- Equipment/facility failure
- Foreign contact

- Vehicle impact
- Standard expulsion fuses
- Cross-phasing
- Age of assets
- Vandalism

Fire Risk Drivers Related to the Service Area

- Accessibility
- Climate
- Vegetation Types / fuels
- Tree mortality / tree failure
- Lightning
- Fire Weather
- Heavy Winds
- Ice

Key Risk Impacts

Ignitions caused by the aforementioned RDs have many possible outcomes. The list below outlines some of the worst-case scenarios and consequences:

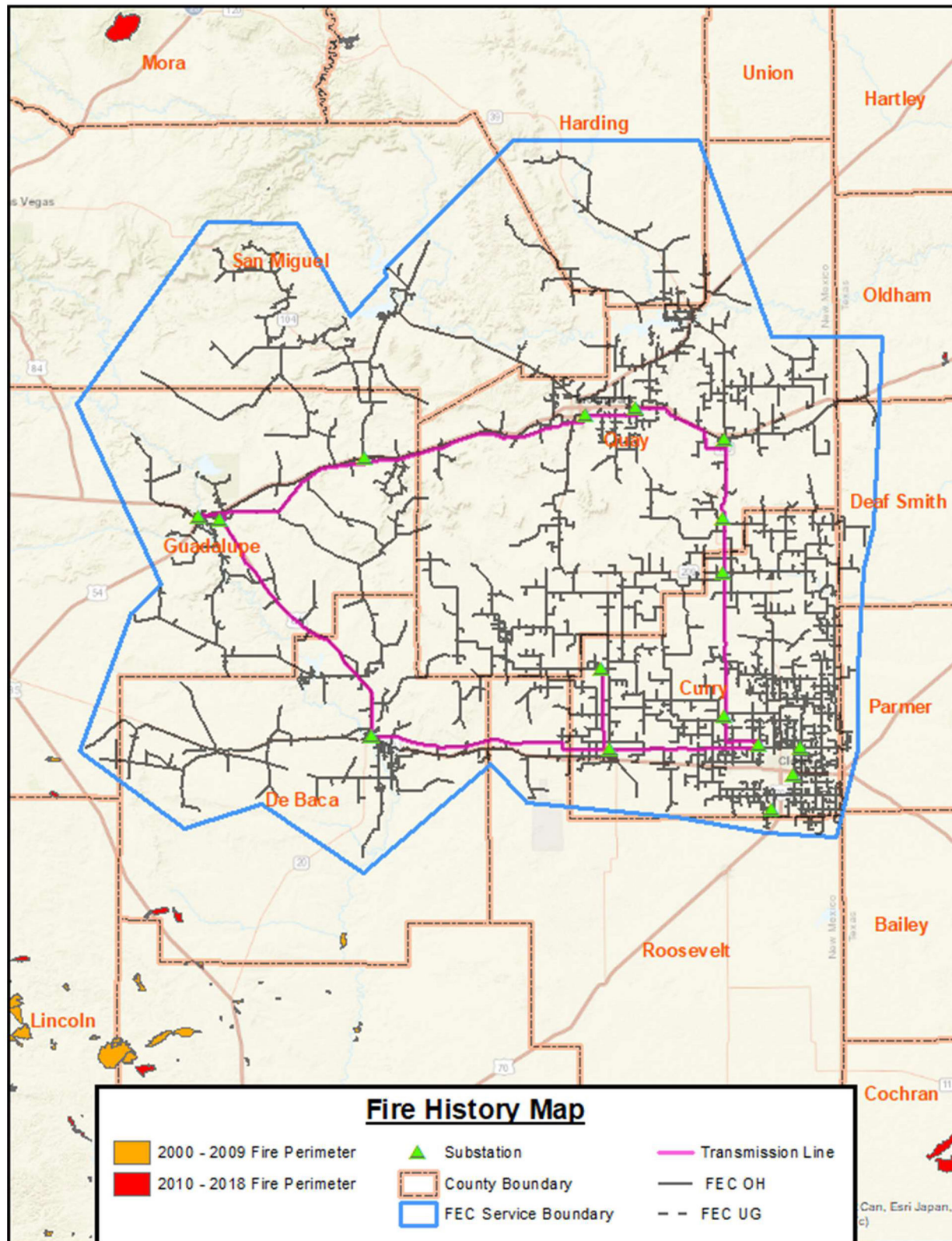
- Personal injuries or fatalities to the public, employees, and contractors
- Damage to public and/or private property
- Damage and loss of FEC owned infrastructures and assets
- Impacts to reliability and operations
- Damage claims and litigation costs, as well as fines from governing bodies
- Damage to FEC's reputation and loss of public confidence

Wildfire History and Outlook

From late fall to early spring, due to lack of rain and increase of wind, is usually FEC's fire season.

Un-grazed grasses and high winds are the main causes.

Figure 2. Historic Wildfire Perimeters 2000-2019 (Example)



1.1.2 Wildland Urban Interface

The United States Forest Service (USFS) defines the wildland urban interface (WUI) as a place where humans and their development meet or intermix with wildland fuel. Communities that are within 0.5 miles of the zone are included. According to the USDA Forest Service, the area considered WUI has expanded 39% in New Mexico from 1990 to 2010, with the number of homes increasing by 53.6%¹. There are now over 615,000 homes in New Mexico located in the WUI².

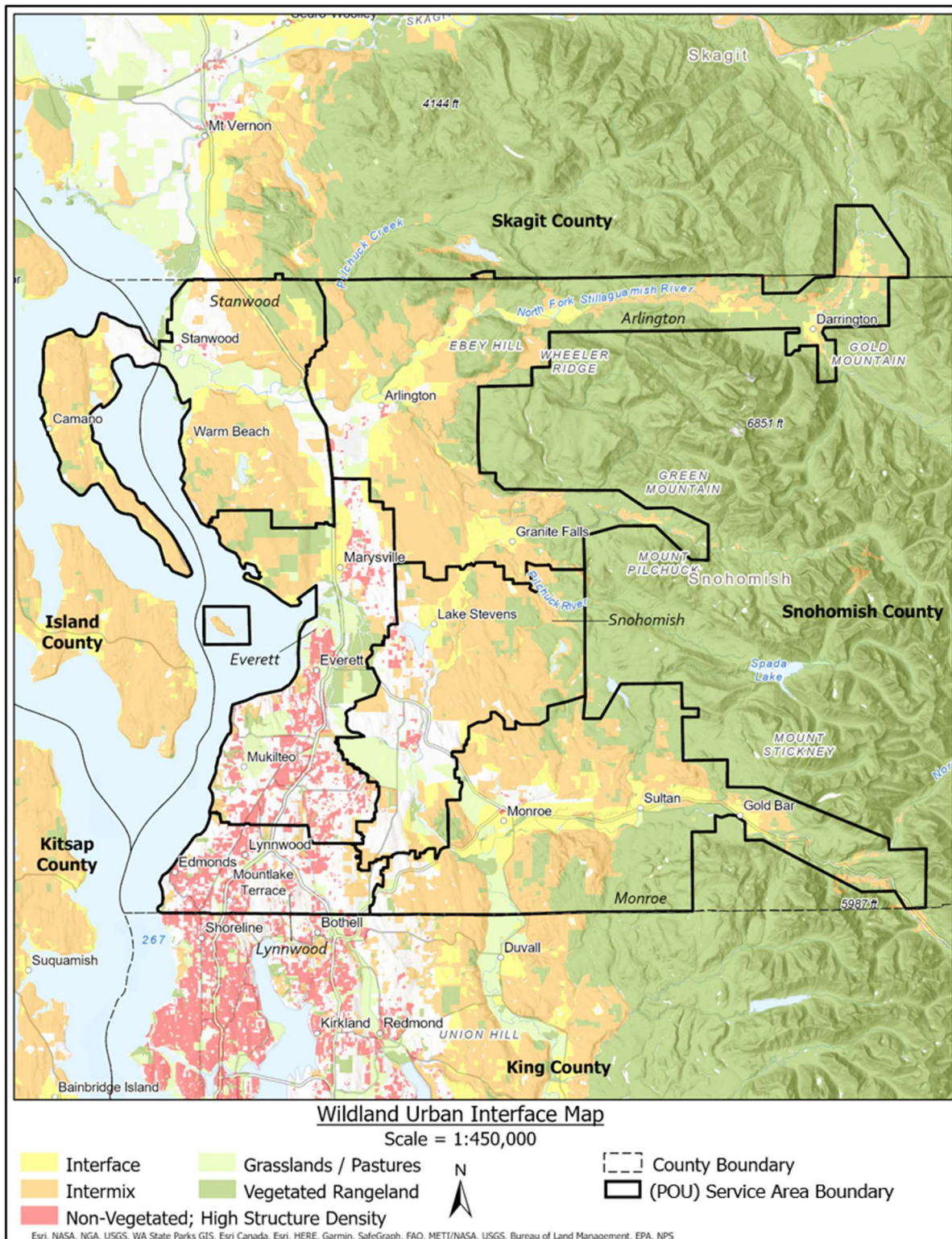
The WUI is composed of both interface and intermix communities. The distinction between these is based on the characteristics and distribution of houses and wildland vegetation across the landscape. Intermix WUI refers to areas where housing and wildland vegetation intermingle, while interface WUI refers to areas where housing is in the vicinity of a large area of dense wildland vegetation. Figure 3 illustrates the distribution of WUI areas in the service area.

The USFS has established five classes of WUI in its assessment:

- **WUI Intermix:** Areas with ≥ 16 houses per square mile and ≥ 50 percent cover of wildland vegetation
- **WUI Interface:** Areas with ≥ 16 houses per square mile and < 50 percent cover of vegetation located < 1.5 miles from an area ≥ 2 square miles in size that is ≥ 75 percent vegetated
- **Non- WUI Vegetated (no housing):** Areas with ≥ 50 percent cover of wildland vegetation and no houses (e.g., protected areas, steep slopes, mountain tops)
- **Non-WUI (very low housing density):** Areas with ≥ 50 percent cover of wildland vegetation and < 16 houses per square mile (e.g., dispersed rural housing outside neighborhoods)
- **Non-Vegetated or Agriculture (low and very low housing density):** Areas with < 50 percent cover of wildland vegetation and < 128 houses per square mile (e.g., agricultural lands and pasturelands)

¹ https://www.nrs.fs.fed.us/data/wui/state_summary/

Figure 3. Wildland Urban Interface (EXAMPLE)



Fire Threat Assessment Mapping

This section will discuss the risk map methodology used in this plan. The language provided describes the USFS-developed dataset used for creating Wildfire Hazard Potential (WHP) risk maps. Guidance for WHP map development using the Esri ArcGIS mapping web portal, can be found on the NMREC Wildfire Mitigation SharePoint site. Develop service territory overview risk map and as many higher resolution detail maps as needed to represent the “Low” and “Moderate”, and “High” risk zones. (example map shown in Figure 3).

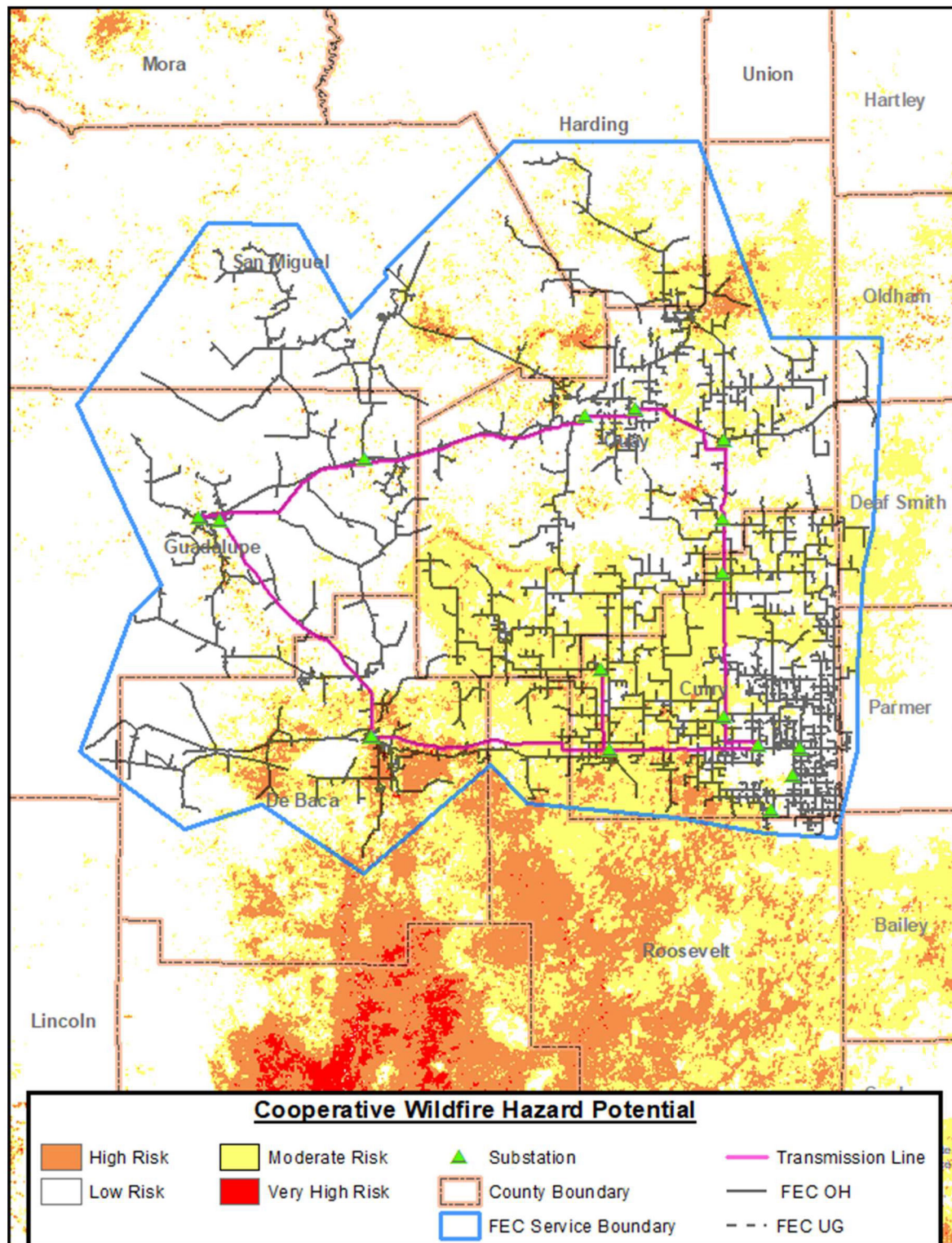
A key element of the WMP is the wildfire risk mapping used to determine the service territory areas that have increased potential for wildfire. These areas contain risk factors such as extreme topography, fuels accumulation, vegetation types, tree mortality, etc. The maps are used to identify areas that may require enhanced vegetation management, shortened inspections intervals, alternative inspection methods or equipment replacement.

The wildfire risk maps are derived from a 270- meter resolution raster geospatial product created by the USDA/USFS, Fire Modeling Institute. The specific dataset used is the Wildfire Hazard Potential³ (WHP), Version 2018⁴. The 2018 WHP publication is the second edition of the WHP product and depicts landscape conditions of the conterminous United States as of 2012. It was built upon spatial datasets of wildfire likelihood and intensity using the Large Fire Simulator (FSim), as well as spatial fuels and vegetation data from Landfire 2012 and point locations of historic fire occurrence (ca. 1992-2013). The objective of the map was to depict relative potential for wildfire that would be difficult for suppression resources to contain and for long-term strategic fuels management planning.

³ Product citation: Dillon, Gregory K. 2015. *Wildfire Hazard Potential (WHP) for the conterminous United States (270-m GRID)*, version 2018 continuous. 2nd Edition. Fort Collins, CO: Forest Service Research Data Archive. <https://doi.org/10.2737/RDS-2015-0047>

⁴ Versions prior to 2014 were known as the *Wildland Fire Potential* map. The FSim products used to create the 2018 version of WHP can be found in Short et al. 2016. Dillon, Gregory K.; Menakis, James; Fay, Frank. 2015.

Figure 1. Service Territory WHP Overview (EXAMPLE)



Wildfire Prevention Strategy and Programs

FEC does not have a recloser operation policy in place for wildfire mitigation.

Table 3. Activities That Address Wildfire Risk Factors

RISK FACTOR	MITIGATION ACTIVITY
Fuel Source	<ul style="list-style-type: none"> • Comprehensive vegetation management program • Enhance vegetation Line Inspections • Enhanced ROW maintenance and clearing specifications • Enhanced inspection intervals and spot checks in high-risk areas • Selective use of non-expulsion fuses N/A • Enhanced tree removal efforts • Current limiting fuses
Extreme Weather	<ul style="list-style-type: none"> • National weather service monitoring • USFS/WADNR IFPL monitoring • Alternate recloser settings in fire prone areas N/A • FEC-owned weather station pilot program • Pole mounted camera pilot program N/A • Preemptive power shutdown during ongoing wildfires • Emergency preparedness community outreach and education
Contact with Foreign Objects	<ul style="list-style-type: none"> • Increased wildlife guards • Avian Protection construction standards • Insulated equipment • Covered Jumpers • Underground conversion of distribution lines • Hazard tree removal
Equipment Failure	<ul style="list-style-type: none"> • Routine Maintenance • Design and construction standards to reduce ignition sources • Transmission line detailed inspections and annual patrols • Distribution line routine patrols • De-energizing or alternate settings of lines during certain conditions N/A • Infrared inspections of substation equipment • Wood pole test and treatment program • UAV inspections on all transmission circuits

Field Work

- FEC worker/contractor education on fire ignition sources
- Tailgate meetings before fieldwork
- USFS fire restriction level monitoring N/A

Transmission and Distribution System Operational Practices

De-energization – Public Safety Power Shutoff

A Public Safety Power Shutoff (PSPS) preemptively de-energizes power lines during high wind events combined with hot and dry weather conditions. When considering de-energization, FEC examines the impacts on fire response, water supply, public safety, and emergency communications.

FEC considers the external risks and potential consequences of de-energization while striving to meet its main priority of protecting the communities and members we serve. They include:

- Potential loss of water supply to fight wildfires due to loss of production wells and pumping facilities.
- Negative impacts to emergency response and public safety due to disruptions to the internet and mobile phone service during periods of extended power outages.
- Loss of key community infrastructure and operational efficiency that occurs during power outages.
- Medical emergencies for members of the community requiring powered medical equipment or refrigerated medication. Additionally, the lack of air conditioning can negatively impact medically vulnerable populations.
- Negative impacts on medical facilities.
- Traffic congestion resulting from the public evacuation in de-energized areas can lengthen response times for emergency responders.
- Negative economic impacts from local businesses forced to close during an outage.
- The inability to open garage doors or motorized gates during a wildfire event can lead to injuries and fatalities.

The risks and potential consequences of initiating a PSPS are significant and extremely complex. (FEC currently does not have a PSPS policy in place.)

Based on the above considerations, FEC reserves the option of implementing a PSPS when conditions dictate. While FEC believes the risks of implementing a PSPS far outweigh the chances of its electric overhead distribution system igniting a catastrophic wildfire, the PSPS provides a last resort tool and another mitigation option in a potential crisis.

On a case-by-case basis, FEC has historically and will continue to consider de-energizing a portion of its system in response to a known public safety issue or response to a request from an outside emergency management/response agency. Any de-energizing of the lines is performed in coordination with key local partner agencies, however, the final determination is made by FEC.

Recloser Operational Practices

FEC does not have a recloser operation policy in place for wildfire mitigation.

Infrastructure Inspections and Maintenance

Recognizing the hazards of equipment that operate high voltage lines, FEC maintains a formal inspection and maintenance program for distribution, transmission, and substation equipment. The Manager of Engineering and Operations oversee most of the time-based system inspection programs. The Manager of Engineering oversees the wood pole inspection program. FEC currently patrols its system regularly. Table 4 summarizes the inspection schedule for all assets, while the following sections outline inspection practices for the utility.

Table 4. Inspection Program Summary

ASSET CLASSIFICATION	INSPECTION TYPE	FREQUENCY
Overhead Transmission	Safety Patrol Inspection	<u>8 months out of year</u>
	Detailed Inspection	<u>As Needed</u>
	Wood Pole Testing	<u>On a 10 year Cycle</u>
	Lidar Inspections	<u>NA</u>
Overhead Distribution	Safety Patrol Inspection	<u>Yearly</u>
	Detailed Inspection	<u>As Needed</u>
	Wood Pole Testing	<u>On a 10 year cycle</u>
	Lidar Inspections	<u>NA</u>
Underground Distribution	Safety Patrol Inspection	<u>Yearly</u>
Substation	Routine Inspection	<u>Monthly</u>

Definition of Inspection Levels

1. **Safety Patrol Inspection:** A simple visual inspection of applicable utility equipment and structures designed to identify obvious structural problems and hazards. Patrol inspections may be carried out in the course of other company business.
2. **Detailed Inspection:** Individual pieces of equipment and structures are carefully examined, visually and through use of routine diagnostic testing.
3. **Intrusive Pole Inspection:** Inspections involving the movement of soil, taking samples of the wood pole for analysis, and/or using more sophisticated diagnostic tools beyond visual inspections.

Safety Patrol Inspections of Transmission and Distribution Lines

Beyond our 8 out of 12 month scheduled transmission line inspection and our annual distribution line inspection, trained employees examine powerlines, poles, and substations on a daily basis; performing visual inspection of applicable utility equipment and structures designed to identify obvious structural problems and hazards.

Detailed Inspections of Transmission and Distribution Lines

FEC uses a contractor for T&D pole inspections, visual and drone. The information given to FEC from contractor is uploaded to our utility system mapping software and is given a priority from 1 to 3, 1 being high priority. A FEC qualified employee is then sent to each structure for review and sets up jobs with local line crew, once crew has completed repairs, work done is then documented through same mapping software and updated on the maps.

Wood Pole Testing and Inspection

To maintain FEC wood poles, a formal Wood Pole Assessment Plan was initiated with the goal to inspect 10% of the system each year. The pole inspection program also includes visual inspections of non-wood poles. Wood pole inspections are carried out on a planned basis to determine whether they have degraded below National Electric Safety Code (NESC) design strength requirements with safety factors.

A third-party contractor inspects and tests all poles on a cycle meeting the interval recommended in RUS Bulletin 1730B-121. Circuits are identified, mapped, and scheduled for inspection and testing using latest industry standards and practices.

Substation Inspections

The Preventive Maintenance Plan provides for regular inspections of FEC substations. Qualified personnel will use prudent care while performing inspections following all required safety rules to protect themselves, other workers, the general public, and the system's reliability.

The monthly substation inspection involves a thorough look at the system to confirm that there are no structural or mechanical deficiencies, hazards, or tree trimming requirements. Individual pieces of

equipment and or structures receive careful visual examination and routine diagnostic tests as appropriate.

Vegetation Management (VM)

FEC contracts out tree trimming, as well as maintains ROW in house, on an as need basis. Trimming standards and clearance specifications are based off RUS specs.

Vegetation to Conductor Clearance

FEC will meet the minimum standards for conductor clearances from vegetation to provide safety for the public and utility workers, reasonable service continuity and fire prevention. As an operator of electric supply facilities, FEC's VM program will keep appropriate records to ensure that timely trimming is accomplished to maintain the designated clearances. These records will be made available for RUS O&M inspections upon request.

FEC has an operational and management responsibility and is required by State and Federal Agencies to maintain the right of way, under or around its power lines. To lessen the liability of fire and safety hazard due to live, dead or leaning trees and vegetation, FEC crews work on an ongoing effort to clear any such hazard by removing any tree or brush that are directly under the power line and considered a problem. Trees or vegetation that is outside of the power line but is encroaching inside the ROW shall be trimmed or removed as needed.

Patrols are scheduled to ensure all lines are inspected for vegetation hazards on an annual timeline.

During tree work, contractors aim to achieve a minimum standard clearance, unless otherwise directed by FEC VM staff and all overhanging limbs are removed. The contractor also clears vegetation from FEC's service drops and pole climbing space on an as needed basis.

The following are optimal clearance dimensions or trimming operations:

- Minimum standard clearance under neutrals
- Minimum standard clearance in transmission ROW

Vegetation Trimming Standards

FEC's contractors follow American National Standards Institute (ANSI) A300 concepts and utility directional pruning, which supports proper pruning/tree health while achieving and maximizing the pruning cycle. The VM program was developed with RUS, ANSI A300, ANSI C2, National Electrical Safety Code (NESC)⁵, And FAC 003-4 standards in mind.

⁵ Rules 012,013 and 218

VM Trimming and Inspection Schedule

FEC personnel and contractors perform annual, ground-based, inspections of tree conductor clearances and hazard tree identification for FEC ROWs and easements. FEC contracts full-time tree trimming crews for year-round vegetation management work. FEC line crews also address vegetation concerns in response to service calls or field observations. Proactive maintenance during routine operations and prompt action during emergency events maintain system reliability, a safe work environment, and reduces fire danger. Any VM issues that cannot be immediately handled by the line crews are referred to the VM contractor for priority trimming. Scheduled patrols ensure all lines are inspected for vegetation hazards and systematically trimmed. On-going, year-round field patrols identify targeted areas for vegetation pruning or removal and ensure compliance with state and federal regulatory requirements.

Hazard Trees

A subset of Danger Trees⁶, A Hazard Tree is defined as any tree or portion of a tree that is dead, rotten, decayed or diseased and which may fall into or onto the overhead lines or trees leaning toward transmission and distribution facilities. These trees are sometimes located beyond the easement or ROW. Any tree that is located outside of the ROW and is deemed a hazard tree will be removed or topped to make safe for conductors.

A hazard tree will have one or more of the following characteristics:

- Dead or dying - all dead or dying trees along, or outside the FEC right-of-way may be removed depending on the height of tree and the direction of the lean.
- Leaning trees - trees that have such a lean toward the right-of-way that they cannot be trimmed without removing the tops and slanting the tree back. Removal depends on height and species of the tree and direction of the lean.

Large areas of the service area have been affected by bark beetle infestation, causing many trees in the service area to become hazard trees. No danger or hazard trees are cut or removed if it cannot make contact with the conductors or structures or cause adjacent trees to fall into the power lines.

Controlling Incompatible Vegetation

In addition to the annual patrols by FEC field staff observing and reporting on incompatible uses and encroachments, FEC make efforts to educate public and private landowners about incompatible vegetation that can pose risks if planted under or near conductors. FEC's website provides guidance on "Right Tree/Right Place", as well as answers to tree trimming frequently asked questions.

Fire Mitigation Construction

FEC does not have a fire mitigation line construction policy.

⁶ As defined by ANSI 300 Part 7 standards

Avian Protection Program

FEC installs cover-up on all new construction, transformers, underground risers, and sectionalizing equipment.

FEC uses wood or fiberglass mounting equipment brackets on new construction

FEC is currently moving to avian friendly framing of new structures.

Emerging Technologies

FEC will continue to explore new technologies and best management practices. Future pilot projects will serve to evaluate the effectiveness of emerging technologies while controlling unwarranted expenditures on unproven methods. FEC may elect to integrate these technologies or practices into its ongoing maintenance programs based on the outcomes. These technologies include, but are not limited to non-expulsion fuses, thermal imaging cameras, FEC-owned weather stations, electronic reclosers, and fire protective coatings for wood poles.

Emergency Response

Preparedness and Response Planning

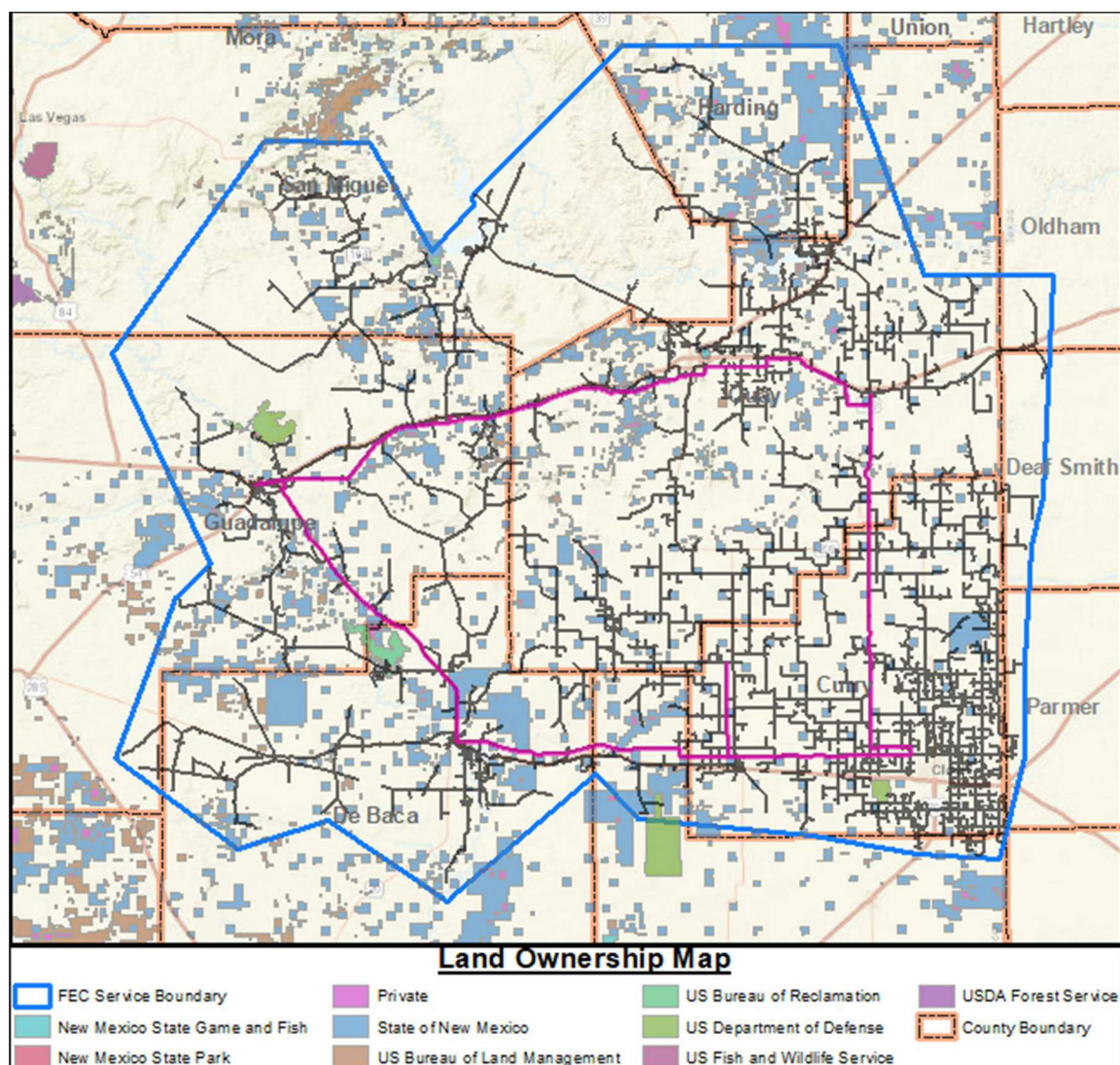
FEC strives to minimize the impacts of all disruptive events regardless of size or scope. FEC makes a conscious effort to practice annual outage sceneries using their ERP as a guide. After going through these yearly tabletop exercises, FEC evaluates what might be improved upon. Once we have a consensus, we make the suggested changes to the plan. If FEC has a “real world” event, these are used as learning opportunities as well. If they think something could be improved, the ERP is updated.

Emergency Management Communication and Coordination

In response to active emergencies, FEC coordinates and collaborates with the local Department of Emergency Management (DEM) and relevant state agencies. During such emergencies, FEC provides a utility representative to the county and/or city DEM to ensure effective communication and coordination.

1.1.3 Jurisdictional Structure

Figure 6. General Land Ownership



Public Agency and Customer Communications for Outages

FEC makes every reasonable effort to communicate with customers (members) during planned or unplanned outages.

Unplanned: If the outage is widespread and is trending toward a prolonged outage, our communications department will reach out to our local media partners (radio, newspaper, etc.) and bring them up to date on the current outage situation(s). If a restoration time can reasonably be calculated, we will share that as well. Given this same scenario, FEC would also use social media platforms such as Facebook to notify and update our members.

Planned: FEC approaches planned outages differently than unplanned. Unplanned is more of a reactive response versus planned being proactive. There are several ways we notify our members of a planned outage. Some seem to work better than others but, FEC chooses to utilize multiple outlets

in order to get the very best coverage and change to effectively, “get the word out.” At approximately two weeks out, FEC does the following:

- Call and ask local radio stations to do Public Service announcements and/or paid radio adds explaining dates, times, and expected durations of such outages
- Call local newspapers (provide same information as above)
- Upload alert on Cooperative webpage
- Personally call members on Life-Sustaining equipment
- Run social media campaigns (facebook/Instagram) using zip code targeting
- Contact local emergency services providers
- Call or visit critical load locations (wastewater, city infrastructure, etc.)
- Call and communicate with assisted living facilities
- If time allows, get the planned outage alert in the Cooperative newsletter
- Use local line personal to get the word via word or mouth

Community Outreach

FEC through its Customer Service Representative uses FEC webpage, radio, local newspaper, and social media to inform customers of current and upcoming events.

Restoration of Service

If an outside emergency management/emergency response agency requests a power shutdown, or if FEC elects to de-energize segments of its system due to extreme weather, FEC staff will patrol the affected portions of the system before the system can be re-energized. Suspect equipment or distribution lines that cannot immediately be patrolled will remain de-energized until FEC staff can do so. Poles and structures damaged in a wildfire must be assessed and rebuilt as needed prior to re-energization. Periodic customer and media updates of restoration status prior to full restoration will be made.

Service Restoration Process

After a wide-spread outage, FEC work crews take the following steps before restoring electrical service after a de-energization event. These measures intend to protect the worker, members, the public, and the system’s reliability.

- **Patrol:** Crews patrol every de-energized line to ensure no hazards have affected the system during the outage. If an outage is due to wildfire or other natural disasters, as soon as it is deemed safe by the appropriate officials, crews inspect lines and equipment for damage, foreign contacts and estimate equipment needed for repair and restoration. Lines located in remote and rugged terrain with limited access may require additional time for inspection. FEC personnel assist in clearing downed trees and limbs as needed.
- **Isolate:** Isolate the outage and restore power to areas not affected.
- **Repair:** After the initial assessment, FEC staff meet to plan the needed work. Rebuilding commences as soon as the affected areas become safe. Repair plans prioritize substations and

transmission facilities, then distribution circuits serving the most critical infrastructure needs. While the goal to reenergize all areas is as soon as possible, emergency services, medical facilities, and utilities receive first consideration when resources are limited. Additional crew and equipment are dispatched as necessary.

- **Restore:** Periodic customer and media updates of restoration status before full restoration are posted on social media platforms and FEC's website. After repairs are made, power is restored to homes and businesses as quickly as possible. Members, local news, and other agencies receive notification of restored electric service.

Performance Metrics and Monitoring

Plan Accountability

Staff responsibility for plan implementation and general communications is described below:

- The Board of Directors makes policy decisions relative to the utility – they will be responsible for approving and adopting the Wildfire Mitigation Plan.
- The CEO/General Manager directs management staff responsible for operations, customer service and finance.
- The Manager of Engineering and Operations is responsible for the overall execution of the WMP. Staff will be directed as to their roles and responsibilities in support of the plan.
- The Director of Member Services is responsible for communicating with public safety, media outlets, public agencies, first responders, local Office of Emergency Management and health agencies during an emergency or planned maintenance outages.
- The CEO/General Manager determines when and how to notify outside agencies in cases of wildfire emergency events.
- FEC's Manager of Engineering and Operations will be responsible for monitoring and auditing the targets specified in the WMP to confirm that the objectives of the WMP are met, as well as the implementation of the plan in general.

Monitoring and Auditing of the WMP

The WMP will be reviewed annually for the purpose of updating the plan as needed to reflect knowledge gained in the preceding year and modified accordingly. A more formal review will be done every 4 years in coordination with FEC's business planning.

Identifying Deficiencies in the WMP

The General Manager or their designee will be responsible for ensuring that this WMP meets all public agency guidelines to mitigate the risk of its assets becoming the source or contributing factor of a wildfire. Staff responsible for assigned mitigation areas have the role of vetting current procedures and recommending changes or enhancements to build upon the strategies in the WMP. Either due to unforeseen circumstances, regulatory changes, emerging technologies or other rationales,

deficiencies within the WMP will be sought out and reported to the Board of Directors in the form of an updated WMP on a 4-year basis.

The CEO/General Manager or their designee will be responsible for spearheading discussions on addressing any plan deficiencies and collaborating on solutions when updating the WMP. At any point in time when deficiencies are identified, the Supervisors or their delegates are responsible for making the appropriate policy adjustments. FEC staff and qualified stakeholders are encouraged to bring any potential deficiencies to the attention of the CEO/General Manager. The CEO/General Manager, along with the appropriate staff, will evaluate each reported deficiency, and if determined to be valid, shall record the deficiency for further action.

Performance Metrics

Table 5. Performance Metrics

METRIC	RATIONAL	INDICATOR	MEASURE OF EFFECTIVENESS
Red Flag Warning (RFW) days in service area	Used to adjust annual variation in criteria	Number of RFWs during analysis cycle	N/A
Utility caused ignitions	Demonstrates the effectiveness of the plan	Count of events	Reduction or no material increase
Ignitions in "High" WHP tier	Assess system hardening efforts in critical areas	Count of events	Reduction in the general trend of events
Power line down in "High" WHP tier* during fire season	Assess system hardening efforts in critical areas	Count of events	Reduction in the general trend of events
Faults in "High" WHP tier	Assess system hardening efforts in critical areas	Count of events	Reduction or no material increase
Vegetation-caused Outage during fire season	Assess VM program work schedules/QC process	Count of events	Reduction or no material increase
Vegetation-caused ignition	Assess VM program work schedules/QC process	Count of events	Reduction or no material increase

Bare line contact with vegetation	Assess VM program work schedules/QC process	Number of contacts recorded	Reduction or no material increase
--	---	-----------------------------	-----------------------------------

Programmatic QA/QC processes

Transmission and Distribution System Inspection QC Process

Appropriate department inspects all work is performed before invoices are signed

Vegetation Management QC Process

Appropriate department inspects all work is performed before invoices are signed

Plan Approval Process

Public Comment

Board Presentation

Operations will present the Wildfire Mitigation Plan to the CEO/General Manager, who will then present to FEC's Board of Directors for approval and adoption of the plan.

Appendix A: Plan and Mapping Disclaimers

WILDFIRE MITIGATION PLAN DISCLAIMER

The information provided in this report was developed by FEC staff and is intended for FEC's internal planning purposes only. FEC does not warrant the accuracy, reliability, or timeliness of any information in this report, and assumes no liability for any errors, omissions, or inaccuracies in the information provided. FEC shall not be held liable for losses caused by using this information. Portions of the data may not reflect current conditions. Any person or entity who relies on any information obtained from this report, does so at their own risk. This report is presented solely for internal use AS-IS by FEC staff. FEC make no representations or guarantees expressed or implied regarding the accuracy or completeness of the report.

WMP MAPPING DISCLAIMER

Maps in this report were created from multiple datasets from various, public, and private sector sources and may include utility Geographic Information System (GIS) data. The geographic information contained in the map(s) is not to be used as a "legal description" or for any purpose other than general planning and reference. Every effort has been made to ensure the accuracy of the map(s), but errors in source documents do occur and inherent mapping ambiguities are not shown.

Maps are for information purposes only and may not represent actual current conditions. End users assume all liabilities incurred by them, or third parties, as a result of their reliance on the information contained in the map(s). FEC, including, without limitation, its employees, agents, representatives, officers, and directors, may not be held responsible or liable in any way for any information and/or data, or lack thereof, provided in the map(s). Information and/or data included in the map(s) is used solely at the discretion of the recipient.

FEC makes no claims, representations, or warranties, expressed or implied, concerning the validity or accuracy of this data. FEC assumes no liability for any errors, omissions, or inaccuracies in the information provided regardless of their cause. FEC produced maps are not to be copied or distributed without permission.

v. Hurricanes

FEC COOP does not serve load in an area affected by hurricanes, therefore that requirement of 25.53(e)(1)(F) does not apply and is not addressed in this EOP.

vi. Pandemic and epidemic

OBJECTIVE

While it is not possible to predict when or if a pandemic (influenza/coronavirus) situation will occur, or how long it will last, this document addresses a general overview of the plan for such an incident. Influenza/Coronavirus pandemic planning by nature emphasizes health aspects in continuity planning, but the overall purpose of the plan is to maintain business activities and operations.

The Pandemic Preparedness Plan covers aspects of business continuity in the event of a pandemic situation. Other events that have the potential to disrupt business activities and operations are covered in additional documents including, but not limited to, the Emergency Restoration Plan (ERP).

POLICY

PLAN PHASES:

The plan consists of the following phases:

- Preparedness and Communication
- Surveillance and Detection
- Response and Containment
- Recovery and Documentation

The plan relies heavily on Federal, State, and Local health and government officials and the orders issued by those officials to determine which phase we are in and what specific actions to take. The below actions are guidelines but subject to change based on the recommendations of federal, state and local health and government officials and the needs of the Cooperative to maintain its business continuity or other concerns.

	Transmissibility and Risk to Humans	Pandemic Plan Activities
Phase 1	Risk to humans is low	<ul style="list-style-type: none"> • Employees are educated to ensure pandemic awareness. • Coordinate planning with critical infrastructure providers • Test the pandemic plan to assess readiness and strengthen as needed.
Phase 2	Risk to humans is moderate and building	<ul style="list-style-type: none"> • Educate key suppliers • Continue all phase 1 activities • Initiate communication plan with employees and customers • Commence social distancing/remote access, telework and outposts as necessary • Develop payment plan communications to highlight the features of on-line payment, pre-payment and drop box, if applicable
Phase 3	Risk to humans is prevalent	<ul style="list-style-type: none"> • Communicate phase change with employees and customers • Continue all phase 2 activities except increase situational awareness • Raise level of pandemic awareness • Initiate specific PPE training sessions • Implement supplies stockpile strategy
Phase 4	Isolated clusters of < 25 people and lasting < 2 weeks. Risk to humans is substantial	<ul style="list-style-type: none"> • Communicate phase change with employees and customers • Continue all phase 3 activities • Ensure that all staff know what to do to prevent personal and family infection • Implement pandemic web site/alerts • Implement travel restrictions and quarantine if applicable • Implement close surveillance
Phase 5	Larger clusters > 25 people and lasting > 2	<ul style="list-style-type: none"> • Communicate phase change with employees and customers • Continue all phase 4 activities • Continuous situational surveillance

	weeks. Risk to humans is extreme	
Phase 6	Risk to humans is at maximum	<ul style="list-style-type: none"> • Minimize impact of Pandemic • Continue all phase 5 activities • Implement full personal protective and containment measure if applicable • Assess sufficiency of plan measures daily and adjust as needed.

Preparedness and Communication

FEC shall implement the following to be prepared for a potential pandemic event and its related communication contingencies.

- Mobile communications for getting instructions to staff.
- Each department should refer to their own business continuity/disaster recovery plan if appropriate.
- Department Managers maintain a current roster of their employees with their contact information. They will notify their employees should there be a situation that would impact the performance of their normal job duties and provide them with necessary instructions.
- Key employees are authorized and approved to have remote access, allowing them to maintain daily operations without physically being onsite. They are to check their email, text, and voicemail regularly to ensure that important messages are retrieved, and business is conducted in a timely and appropriate manner.
- Employees with remote access will be required to test their connectivity on a regular basis, working with the IT Department to identify and correct any potential connectivity issues in advance.
- FEC shall create a culture of infection control in the workplace that is reinforced prior to the annual influenza season including:
 - Information about recommended practices to reduce the spread of infection
 - Distribution of adequate infection control supplies including hand sanitizers and disinfecting wipes.
 - Instructions on proper procedures for cleaning high-touch surfaces including keyboards, telephones, doorknobs, etc.
- FEC encourages employees and their families to consult with medical professionals regarding recommendations on immunizations/vaccinations. Medical insurance coverage may provide coverage for specific immunizations/vaccinations.

Surveillance and Detection

Pandemic Response Team shall:

- Monitor staffing levels (including contractor/mutual aid levels) to ensure that available resources do not fall below critical levels.
- Each department should refer to their own ERP recovery plan.
- Monitor local health advisories to determine when the optimal time approaches to begin shifting key staff to working remotely to reduce contact with possible infected staff.
- Determine when it becomes appropriate to reduce the availability of services at a specific location, such as front desk operations, collections contact, field personnel contact with the public.
- Determine when it becomes appropriate to close the office.
- Educate all employees as to influenza/coronavirus symptoms and become proactive at directing infected staff to medical facilities for treatment at the employee's own expense/insurance.
 - Any employer directed time off due to symptoms will require the employee to utilize available PTO. If PTO time is unavailable, the missed hours will be unpaid unless deemed otherwise by the Human Resources Manager.

Response and Containment

Should a potential pandemic influenza/coronavirus outbreak occur, FEC shall:

- Communicate initial notification to all employees.
- Activate mobile communications to inform staff of company guidelines and keep all employees updated on the situation.
- Communicate periodic updates through the use of mobile/electronic communications.
- Each department should refer to their own ERP recovery plan if appropriate.
- Have key staff begin working remotely to minimize contact with others, including the rerouting of phone extensions to ensure all incoming calls and messages are received in a timely manner.
- Communicate any changes in services (front desk, appointment only, closure) to the customers by posting lobby and door signs and posting a notice on the website home page, as directed by Communications.
- Have signage posted at all entrances to the facility advising staff and visitors not to enter if they have influenza/coronavirus symptoms.

- Department managers will advise employees not to come to work when they are feeling ill, particularly if they are exhibiting any influenza/coronavirus symptoms and to consult a health care provider, if necessary, at employee's own expense.
- Any employer directed time off due to symptoms will require the employee to utilize available PTO. If PTO is unavailable the missed hours will be unpaid unless deemed otherwise by the Human Resources Manager.
- Advise staff members that have been told to stay home to stay in contact with management through regular telephone and email.

Recovery and Documentation

Once the pandemic situation subsides and the staff is healthy enough to report back to work at normal (pre-pandemic) levels:

- FEC shall resume its usual day-to-day business operations at all locations.
 - Remote staff will be instructed to return to their normal workstations and job responsibilities.
 - Mobile communications will be placed in standby status.
- Communication will be updated to reflect "business as usual" status.

Follow-up documentation will be maintained as part of FEC's disaster recovery records, making note of significant lessons learned, actions taken, and recommended changes in procedures for future pandemic situations. In addition, the Pandemic Response Team will document all ongoing and routine testing and preparedness planning efforts to ensure FEC is able to respond quickly and efficiently in the event of a pandemic disaster.

Actions Taken if an employee has symptoms or tests positive for the pandemic disease or virus:

The Cooperative will rely on Federal, State, and Local Health and Government Official guidelines to determine the course of action to take if an employee of FEC has symptoms of and/or tests positive for the pandemic disease or virus but reserves the right to deviate from those guidelines based on the needs of FEC to sustain its business continuity or other concerns.

RESPONSIBILITY

The Pandemic Response Team is responsible for oversight, implementation, and maintenance of this document. Should it be necessary to implement this plan, this team will work together with department managers to ensure that minimal business interruptions occur.

Pandemic Response Team members include:

- CEO/General Manager, HR/CS Manager, Director, Member Services, Accounting Manager, Engineering Manager, Information Technologies Manager, and Line Superintendent(s).

REVIEWED

New, Implemented, May 6, 2020

Reviewed/Revised March 10, 2023

vii. Cyber Security Incidents

TABLE OF CONTENTS

Introduction

Purpose

Scope

Maintenance of Plans

Cybersecurity Incident Mitigation Plan

Cybersecurity Incident Response Plan

Scope

Definitions

Roles, Responsibilities, and Teams

Incident Response Methodology

Appendix A – Executive Response Team

Appendix B – Guidelines for Incident Response

Introduction

Purpose

This document outlines the plans for responding to and handling cybersecurity incidents at Farmers' Electric Cooperative (FEC) Inc., including defining the roles and responsibilities of all participants, the overall characterization of cybersecurity incident response, relationships to other company policies and procedures, and guidelines for reporting requirements.

Due to the everchanging cybersecurity landscape and wide variety of incidents that could face Electric Cooperatives, along with the rapid development of cybersecurity threats against the Electricity Industry, its data, networks, and systems, this document is designed to provide guidance in reacting to cybersecurity incidents, determination of their scope and risk, and ensuring an appropriate response to cybersecurity incidents, including isolation and containment of the incident, timely restoration of affected systems, communication of incidents to the appropriate stakeholders, and reducing the risk of the incident from re-occurring.

Anyone suspecting a possible cybersecurity incident should disconnect their device from the network immediately and contact the following persons in the following order:

Information Technology Manager – Glenn Barleben – [REDACTED]

Engineering Manager (IT Backup) – Michael McCord – [REDACTED]

Member Services Director – Thom Moore – [REDACTED]

Billing/HR Manager – Helen Jo Wallin – [REDACTED]

Scope

These plans apply to all company computers, mobile devices, data, and networks of Farmers' Electric Cooperative Inc. and any person or device accessing these systems or data. The Information Technology (IT) Manager acts on behalf of FEC and will request cooperation and assistance in investigating and resolving incidents from FEC Staff, employees, and members as required. If the IT Manager is absent and/or needs assistance in an emergency, the Engineering Manager will assist as needed and/or serve as the backup for the IT Manager throughout this plan and takeover any roles the IT Manager is unable to perform as needed. The IT Manager will also work closely with the Engineering Manager, the CEO/General

Manager, the Member Services Director, the Human Resources Manager, and any other members of Staff and/or employees throughout the investigation and resolution of incidents as necessary.

Maintenance of Plans

The IT Manager is responsible for the maintenance and revision of this document and the plans that are included, both annually and/or as needed. The IT Manager will consult with all Staff including the CEO/General Manager, along with any third parties that FEC works with to confirm the accuracy of this document.

Cybersecurity Incident Mitigation Plan

To prepare for and mitigate cybersecurity incidents and all the cybersecurity vulnerabilities and threats that are constantly evolving, FEC will use the following steps to mitigate cybersecurity incidents:

Cybersecurity Incident Mitigation

1. Risk Assessment

There is a cybersecurity risk assessment conducted at least once a year using the “**RC3 CYBERSECURITY SELF-ASSESSMENT TOOL**” and/or any other cybersecurity assessment tools that FEC has access to. This process is the responsibility of the IT Manager and the Engineering Manager (if needed). Depending on the results, upgrades and adjustments are made as needed, as quickly as possible, to correct any issues that are found and to successfully mitigate known risks and vulnerabilities.

2. Network Access Controls

FEC follows best practices when it comes to trust and user access privileges. Users are assigned rights with an as little as possible approach, depending on their job function. The IT Manager is responsible for assigning rights and access. The Engineering Manager serves as the IT Manager’s backup in case of an emergency.

3. **Cybersecurity Awareness**

FEC utilizes a “**Cybersecurity Awareness**” program. Random emails and tests are generated and sent out to all employees to test an employee’s wit and to see how they handle the email, if they click on attachments or links, etc. IT monitors this process and generates reports as needed that show what action a user took. If a user failed the phishing email test, the IT Manager will provide input and training to them along with information about the current email they opened, how to identify fraudulent emails, and what they should do if they receive one.

4. **Multiple Layers**

There are hardware firewalls and appliances in place, along with multiple layers of network security that are configured to protect FEC’s network from outside malicious traffic, only allowing specific ports, devices, and networks access to the internal network, monitoring and limiting communications both in and out, along with network segmentation. These layers are updated accordingly following best practices and guidelines from multiple entities.

5. **Software Firewall and Antivirus**

Software firewall rules, group policies, and antivirus/malware protection are used on all company computers at FEC. FEC uses third party endpoint detection and response (EDR) to monitor and protect all systems on the network. The software firewall rules are managed by the IT Manager. These rules are adjusted on an as needed basis, following best practices and recommendations from multiple IT cybersecurity entities including E-ISAC. Antivirus logs are checked daily to make sure that antivirus is functioning properly and that there are no reports or alerts of malicious activity etc.

6. **Web Filtering**

FEC utilizes web filtering to block users from navigating to malicious, unproductive, or inappropriate websites. This list is updated automatically and manually daily as needed following best practices, including any recommendations from E-ISAC and others.

7. **Patch Management**

FEC manages and monitors [REDACTED] Updates, updates for all applicable software used on the network, and updates for all devices including firmware and more.

8. **Network Monitoring**

Logs are checked and monitored daily at FEC by the IT Manager and there are also automated notifications sent out as well. █████ logs are checked for anything out of the ordinary including but limited to security logs. Firewall reports and logs are also checked daily for any malicious activity, along with bandwidth checks etc., to make sure there is nothing malicious or out of the ordinary. Real time packet captures are performed from firewalls, switches, and various machines on the network for malicious traffic. Logs from antivirus central management are checked as well, to make sure everything is operating normally on all devices. If there is evidence of even a small issue, it is treated as a possible cybersecurity incident, and a detailed check is performed by the IT Manager, along with isolation of the machine and a thorough scan and check of the device and its logs, to make sure it is clean of an infection. If there is malicious traffic, activity, etc., or if a machine is found to be infected or has strange behaviour, the **Cybersecurity Incident Response Plan** is to be used immediately.

Cybersecurity Incident Response Plan

This plan outlines the general tasks for **Cybersecurity Incident Response**. Due to the ever-changing nature of incidents and attacks upon the Electric Industry, this incident response plan may be supplemented by specific internal guidelines, standards, and procedures as they relate to the use of security tools, technology, and techniques used to mitigate, investigate, and resolve incidents.

Cybersecurity Incident Response

Scope

The IT Manager represents all FEC provided Information Systems and Cooperative Data including data residing in cloud-based services. FEC operates in a partially de-centralized environment with certain systems being managed and monitored by third party entities maintaining their own IT staffs. To the extent possible, during a cybersecurity incident investigation, the CISO will attempt to coordinate investigation efforts with all third parties involved as necessary ensuring the security of all Cooperative systems and data in relation to the activities in support of the Cooperative. Specific actions and resources utilized in the investigation of an incident will be in alignment with the type, scope, and risk of the threat to Cooperative systems and data.

Evidence Preservation

The primary goals of incident response are to contain the scope of an incident and reduce the risk to Cooperative systems and data and to return affected systems and data back to an operational state as quickly as possible. The ability to quickly return systems to operational may at times be hampered by the collection of data necessary as evidence in the event of an exposure of data.

Operational-Level Agreements

In today's world, many individuals are dependent upon technology and have expectations about the availability of systems and data for themselves and the constituents they serve. The interruption of services can cause a hardship and the CISO will cooperate with the affected groups to ensure downtime is minimized. However, FEC leadership supports the priority of investigation activities where there is significant risk, and this may result in temporary outages or interruptions, but is necessary to ensure pertinent information is gathered, the risk is fully isolated, the risk is fully resolved, and the risk is fully stopped so the incident does not occur again.

Training

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, exercised, and evaluated for process improvement. FEC staff inside and outside of IT will be periodically trained on procedures for reporting and handling incidents to ensure there is familiarity with the process and with the responsibilities of the **IT Incident Response Team (ITERT)**. These exercises may take the form of either external or internal training including tabletop exercises.

Incident Response Phases

The Incident Response process encompasses six phases including preparation, detection, containment, investigation, remediation, and recovery. These phases are defined in **NIST SP 800-61** (Computer Security Incident Handling Guide). In the execution of responding to an incident, the **ITERT** will focus on the **detection, containment, investigation, remediation, and recovery** of the specific incident.

1. Preparation

Preparation for incident response includes those activities that enable the Cooperative to respond to an incident and include the creation and review of policies, standards and guidelines supporting incident response, security, and technology related tools, effective

communication plans and governance. Preparation also implies that the departments across the Cooperative have implemented the controls necessary to enable the containment and investigation of an incident. As preparation happens outside the official incident process, process improvements from prior incidents should form the basis for continuous improvement at this stage.

2. Detection

Detection is the identification of an event or incident whether through automated means with security tools or notification by an inside or outside source about a suspected incident. This phase includes the declaration and classification of the event/incident.

3. Containment

Containment of an incident includes the identification of affected hosts or systems and their isolation or mitigation of the immediate threat. Communication with affected parties is established at this phase of incident response.

4. Investigation

Investigation is the phase where the CISO determines the priority, scope, risk, and root cause of the incident.

5. Remediation

Remediation includes the repair of affected systems and services, utilizing backups if necessary, addressing residual attack vectors against other systems, communication, and instructions to affected parties and an analysis that confirms the threat has been contained.

If the **CISO** or **Privacy Officer (IT Manager)** reasonably believe that an exposure of regulated data may have occurred, the **CISO** or **Privacy Officer** will contact the **CEO/General Manager** and **Director of Member Services** to provide situational information in determining a proper response at this stage. Apart from any formal reports, the after-action analysis will be completed at this stage.

6. Recovery

Recovery is the analysis of the incident for possible procedural and policy implications. Recovery also includes the incorporation of any "**lessons-learned**" from the handling of the incident into future exercises and/or training initiatives.

Definitions

Cybersecurity Event

An event is an exception to the normal operation of IT infrastructure, systems, or services. Events may be identified using automated systems, system logs, reported violations or issues to the IT Manager, or during normal system reviews by the IT Manager including system degradation or disruptions. An example of an event could be a report of a suspicious email, unusual computer behaviour, service disruption, etc. It is important to note that not all events become incidents. Also, depending on the event, it may be advisable to disconnect a device from the network immediately.

Cybersecurity Incident

An incident is an event that, as assessed by the IT Manager, violates FEC's Acceptable Use Policy, Access Control Policy, Confidential Data Policy, an/or other FEC policies, standards, or Code of Conduct, or that threatens the confidentiality, integrity, or availability of Information Systems or Cooperative Data. An example of what could be considered a cybersecurity incident is a known malware/virus infection, ransomware attack, or any event that the IT Manager identifies as an incident after investigation. If an event is deemed a cybersecurity incident, that device or process should be disconnected from the network immediately.

Roles, Responsibilities, and Teams

Chief Information Security Officer (CISO)-

Throughout the course of this plan, the **IT Manager** will serve as the **CISO**, which is broadly responsible for:

1. Coordinating efforts to manage an information security incident.
2. Ensuring the prompt investigation of a security incident.
3. Determining what Cooperative data may have been exposed.
4. Securing and isolating any compromised systems to prevent further damage.
5. Providing guidance to Cooperative Staff, employees, members, stakeholders, and any third parties involved as necessary.

Privacy Officer

Throughout the course of this plan, the **IT Manager** will also serve as the **Privacy Officer**, which is broadly responsible for:

1. Coordinating efforts to manage regulatory requirements and notifications.
2. With assistance from the Engineering Manager and Director of Member Services, along with members of Staff, reviewing applicable federal and state laws, and developing appropriate course of action to comply with such laws in the event a cybersecurity incident occurred.
3. Ensuring all aspects of cybersecurity incident management are completed.
4. Contacting and Cooperative Lawyers and/or cybersecurity insurance if necessary.

Incident Response Coordinator

Throughout the course of this plan, the **IT Manager**, and/or the **Engineering Manager**, or the **Member Services Director** will act as the **Incident Response Coordinator**, which is broadly responsible for:

1. Directing efforts to gather appropriate information.
2. Providing expertise in the procedural aspects of gathering information and documentation of process.
3. Updating the **CISO** and other leadership as necessary.

Incident Response Handler

Throughout the course of this plan, the **IT Manager** and **Engineering Manager** will act as the **Incident Response Handlers**, which are broadly responsible for:

1. Gathering data from systems
2. Providing specific expertise in technology and data
3. Entering appropriate data for Incident Management including procedural information.

The Corporate Emergency Response Team – (CERT)

The Corporate Emergency Response Team has direct responsibility for **managing** the overall cybersecurity incident **effort** including **providing** the IT recovery teams with the support they require to restore affected computers, devices, and infrastructure. The **CERT** shall be comprised of the following members (note: other members may be asked to collaborate where appropriate):

- Antonio R. Sanchez, Jr., CEO/General Manager
- Suzy Howard, Accounting Manager
- HJ Wallin, Office Manager
- Thom Moore, Director of Member Services
- Michael McCord, Engineering Manager
- Glenn Barleben, IT Manager
- Barry Bass, Line Superintendent I
- Rodrick “Rick” Ragland, Line Superintendent II

IT Emergency Response Team – (ITERT)

The **IT Emergency Response Team (ITERT)** consists of multiple teams listed below that are comprised of FEC Staff members and/or employees with the authority to **assist and to make key decisions** in managing a cybersecurity incident. The overall **ITERT** shall be comprised of the following members (note: other members may be asked to collaborate where appropriate):

- Glenn Barleben, IT Manager
- Michael McCord, Engineering Manager
- Stephan Teonchuk, Meter Data Analyst
- Vani Puppala, GIS Specialist
- Helen Jo Wallin, Billing Manager/HR Manager
- Thom Moore, Director of Member Services

The IT Recovery Teams

These teams have direct responsibility for **restoring** the affected computers, devices, and infrastructure for the Cooperative. Specific teams and the general responsibility of each team includes:

Network Team – This team is responsible for providing access to the FEC wide area network from the cold site, the recovery team's site, and for the business units located at various temporary sites.

██████ Team – This team is responsible for restoration and availability of the CIS Servers and Web Servers and the applications residing on them.

Server Team – This team is responsible for the restoration and availability of the local servers and the applications residing on them.

Members of the above three areas are:

- Glenn Barleben, IT Manager
- Michael McCord, Engineering Manager
- Helen Jo Wallin, Billing/HR Manager
- Vani Puppala, GIS Specialist
- Stephan Teconchuk, Meter Data Analyst

Desktop Team – This team is responsible for providing IT with the desktop equipment and software they need to facilitate recovery efforts and for business continuity purposes.

Administrative Team – This team provides the other IT teams with the support they require to facilitate the recovery effort. This includes office equipment and supplies, coordinating travel plans, and coordinating with the Corporate Team where necessary.

Members of the above two areas are:

- Helen Jo Wallin, Billing/HR Manager
- Michelle Hammonds, Receptionist

Appendix A – IT Emergency Response Team (ITERT)

The **ITERT** is responsible for actions such as communication, information sharing, and minimizing impact from a cybersecurity incident. As Cooperative responses to each incident may vary, this section provides an overview of those actions that the ITERT may take in responding to a cybersecurity incident.

1. Once it is determined that enough information about the situation and the extent of the exposure has been collected, the IT Manager will collaborate with the CEO/General Manager and Staff to determine if the incident rises to the level of a security breach. If this is determined, appropriate members of the ITERT should work together to determine what, if any, level of notification is required, how individuals impacted by the exposure should be notified and what, if any, services should be offered to the individuals impacted by the cybersecurity incident to help protect themselves from potential or actual identity theft. As part of this analysis, the Privacy Officer will coordinate with the CEO/General Manager and Staff to review applicable state and federal privacy, data security and breach notification laws and a plan of action to comply with applicable requirements of such laws.
2. If it is determined that notification and credit monitoring protection is appropriate and/or required, the Privacy Officer may engage the Cooperative's designated vendor to provide notification and credit monitoring services on the Cooperative's behalf. When applicable, the Cooperative may engage with FEC's cyber-liability insurance carrier for assistance. Unless an exception is determined to be appropriate by the ITERT, the office or department responsible for the data that was lost or exposed shall be responsible for the costs associated with remediating the exposure, including but not limited to notification and credit monitoring services.
3. Where required by state and or federal law, the Privacy Officer will coordinate with the CEO/General Manager and Staff and/or the Director of Member Services to ensure that appropriate state (NM or TX, or any other applicable state) and/or federal government entities (e.g., state attorneys general, other state agencies, FTC, DHHS, E-ISAC) are notified of the exposure, who has been impacted, and the Cooperative's course of action related to managing the exposure of data.
4. Where appropriate, the ITERT will contact the Office of the Attorney General (through the AG's Privacy and Data Security Department), the Governor's Office and/or any other appropriate State Officials to inform them about the data exposure.
5. Where necessary or appropriate, the ITERT will expeditiously collaborate to develop press releases, letters to affected individuals (by email and/or U.S. post). Where appropriate, the CISO will coordinate with Member Services to create web page(s) with information regarding the exposure and how individuals can take steps to protect themselves.

6. The ITERT will also designate a single point of contact to address questions/concerns of individuals concerned about the exposure. The ITERT may decide to set up a special toll-free phone number line for individuals to call with questions/concerns or to utilize services provided by FEC's cyber-liability insurance carrier, when applicable. The Privacy Officer will ensure that appropriate offices are made aware of the single point of contact to whom questions/concerns should be directed.
7. While managing and remediating the exposure, as expeditiously as possible:
 0. The Privacy Officer will work with Accounting and the department responsible for the costs of remediating the exposure to process necessary paperwork to engage the Cooperative's designated vendor to provide notification and/or credit monitoring services.
 1. The Privacy Officer will work with the vendor to process any appropriate paperwork (i.e., SOW, PO, etc.) to engage the vendor's services.
 2. The Privacy Officer will work with appropriate Cooperative Staff, the CEO/General Manager and the vendor to draft notification letters, and where appropriate, FAQ's regarding the incident.
 3. The Privacy Officer and/or CISO will work with appropriate Cooperative Staff to collect the names and last known addresses of individual who will need to be notified.
 4. Notification letters will be sent to impacted individuals or organizations by First Class Mail, email and/or other methods required by law.
 5. Press releases will be finalized and issued by FEC IT and Member Services where appropriate. The main Cooperative website will include a link to the news release.
 6. A special website, containing information regarding the exposure, how to get more information, and how to protect one's credit, may be posted as appropriate by FEC IT and Member Services.
 7. A mechanism for logging calls and/or inquiries received, as well as responses and/or assistance given, shall be created, and implemented.
 8. Once proper notifications have been sent and posted and the matter has been contained and handled, debriefing meeting(s) should be held with all of the individuals involved in the incident investigation, management and remediation. Additional follow-up activities should occur as appropriate.

Appendix B – Guidelines for Incident Response

Each incident presents a unique set of challenges and problems. This section provides some common guidelines for preferred actions in these types of events. For any issues outside of these guidelines, the CISO or CEO/General Manager should be consulted.

Incidents within Chain of Command

In incidents where a member of the ITERT team, their leadership or the leadership of the Cooperative is being investigated, appropriate resources will be selected to remove any conflicts of interest at the direction of or in conjunction with either the CEO/General Manager or the Board of Trustees.

Interactions with Law Enforcement

All communications with external law enforcement agencies are made after consulting with the IT Manager, Staff, and Director of Member Services.

Communications Plans

All public communications about an incident or incident response to external parties outside of Farmers' Electric Cooperative are made in consultation with the CEO/General Manager and Director of Member Services. Private communications with other affected or interested parties should contain the minimum information necessary as determined by the Incident Coordinator or Chief Information Security Officer (IT Manager).

Privacy

FEC respects the privacy of all individuals, and wherever possible the incident response process should be executed without knowledge of any individual identities until necessary.

Documentation, Tracking and Reporting

All incident response activities will be documented to include artifacts obtained during any investigation. As any incident could require proper documentation for law enforcement action, all actions should be documented, and data handled in an appropriate manner to provide a consistent chain of custody for the validity of the data gathered.

Escalation

At any time during the incident response process, the Chief Information Security Officer (IT Manager) may be called upon to escalate any issue regarding the process or incident.

**viii. IT Business Continuity/Disaster Recovery Plan
Recovery Procedures:**

IT Business Continuity/Disaster Recovery Manual

Issued by

Information Technology Department

Updated April 2022

1st drafted December 2005

Table of Contents

Section I Manual Overview

Maintenance of the Manual

The Periodic Comprehensive Review

The Semi-Annual Review

Updating of the Manual

Distribution of the Manual

Section II Disaster Recovery Plan Overview

Purpose

Scope of the Plan

Assumptions

Business Continuity Site

Section III Testing the Disaster Recovery Plan

Testing the Disaster Recovery Plan

Section IV Initial Disaster Response

Appraisal of the Situation

Declaration of a Disaster

Disaster Recovery Timeline

Day 1 Day 2 Day 3 Day 4 Day 5 Day 6 Day 7 Day 8 Day 9

Section V Disaster Recovery Teams

Team Structure and Duties

The Corporate Team (Emergency Response

Team – ERT) The IT Recovery Team

Team Procedures

Section VI Lists

Contacts and Key Suppliers for Office Services and Information Technology

Section I Manual Overview

Maintenance of the Manual

Maintenance of the Disaster Recovery Manual is divided into three categories:

- A periodic comprehensive review
- A semi-annual review
- Updating of the manual

Each of these categories is detailed below.

The Periodic Comprehensive Review

The periodic comprehensive review of the Disaster Recovery Manual is the responsibility of the Information Technology (IT) Manager. It will be completed during the test of the plan and will be complete no later than one month after the test. This will help ensure an accurate Disaster Recovery Manual in case there is a disaster, and for the periodic disaster recovery tests. (See section III – Testing the Disaster Recovery Plan).

The following portions of the manual will be covered by the periodic review:

- Manual Overview section
- Printing the manual
- Overview of the Disaster Recovery Plan section
- Initial Disaster Response section
- Disaster Recovery Testing section

The Semi-Annual Review

The IT Manager will be responsible for coordinating the semi-annual review of the manual and making the required changes to the manual. The IT Manager will maintain the most current version on the company's intranet site for all other staff to review and suggest revisions or corrections.

The following portions of the manual will be covered by the semi-annual review:

- Office equipment list
- Documentation
- Cold site procedures
- Infrastructure restoration procedures
- Network restoration procedures
- Applications restoration procedures
- Desktop restoration procedures
- Equipment lists
- Forms list
- Vendor Contact list (including printing and filing)
- FEC Employee list (including printing and filing)
- Reproduction of the Disaster Recovery Plan on CD

Updating of the Manual

Lists and procedures in the IT Disaster Recovery manual will be maintained in their electronic format as changes occur on the company's intranet site enabling access by all staff members.

Distribution of the Manual

Hard copies of the following documents:

- 'IT Disaster Recovery Manual' within the IT Manager office
- 'IT Disaster Recovery Vendor List' within the IT Managers office
- FEC Employee List for Disaster Recovery' within the IT Managers office will be printed and filed as follows:
 - In the office of the IT Manager
 - In the on-site storage vault
 - In the home of the IT Manager

The complete manual (made up of all documents in the IT Disaster Recovery folder) will be maintained in an electronic format at the following sites:

- IT Managers laptop (master copy)
- FEC intranet site (replicated copy)
- Offsite-Plateau (replicated copy)

On an annual basis, copies of the entire Disaster Recovery Procedures will be copied onto a CD or flash drive and stored in the on-site storage vault, in the IT Managers office, and at the IT Managers home.

Individual team members should have hard copies of the manual just in case. They will be able to access the most recent document or the entire manual from the company's intranet site at any time.

At the time of a disaster an entire manual may be printed from one of the CD or flash drive copies maintained at the three locations listed above.

In case of a disaster, the Disaster Recovery Management team leader (IT Manager) will retrieve a copy of the hard copy manual from the on-site storage vault or alternate storage facility. (Obtain the backup from Plateau if none of the other facilities are available). The team leader will use one

copy to start disaster recovery efforts (including printing the entire Disaster Recovery Manual). Once printed, sufficient copies will be reproduced in the most efficient manner to provide to each team. This will be done at any available local office supply, if impossible in company's facilities. The current local office supplies to use would be OfficeMax or Hollands Office Supply in Clovis.

Section II

Disaster Recovery Plan Overview

Purpose

The purpose of this Disaster Recovery Plan is to provide procedures for the orderly recovery of the corporate data processing services for FEC in the event of a disaster destroying or severely impairing the current data processing services. It is meant to minimize further losses to FEC.

The objectives of the plan include:

- Assist in maintaining business continuity during a disaster
- Protect data integrity and ensure system survivability
- Restore the data processing function as quickly as possible
- Satisfy audit and legal requirements

The benefits of having a Disaster Recovery Plan include:

- Protect assets and minimize economic loss
- Assist the decision-making process during a disaster
- Minimize employee disruption and stress during a disaster
- Minimize delays and errors during the recovery effort

Scope of the Plan

This Disaster Recovery Plan was written specifically for recovering the data processing infrastructure for which the Information Technology Department has primary responsibility as located at the Farmers Electric Cooperative (FEC) headquarters building. It does not cover the recovery of data processing infrastructure located at any of the other company locations, nor does it cover departmental computing located at the headquarters building.

The plan does cover the restoration of the software and historical data for applications residing on the company's [REDACTED] and supporting servers for which the IT department has primary responsibility. This does not include the **business continuity** or **contingency plans** for which the business units are responsible. Business continuity plans and/or business contingency plans will be referenced in the plan where available to provide a cross-reference. While IT is not responsible for the development or implementation of these business continuity plans or contingency plans, IT will assist with the implementation of these plans as outlined in the plans.

Assumptions

This plan covers the "worst case" scenario, which assumes the destruction of the FEC headquarters building and all the data processing and communications infrastructure located in the building. In a disaster of lesser severity, only portions of the plan may need to be implemented. It will be up to the IT Disaster Recovery Management Team to determine what portions of the plan will be implemented.

Upon receiving direction from the **Corporate Disaster Recovery Management Team**, the **IT Disaster Recovery Management Team** will activate the appropriate procedures.

This plan assumes the availability of replacement [REDACTED] equipment and software services from [REDACTED] who supplies FEC with our current [REDACTED], supporting servers, and support services. As of 04/2022, that equipment is the [REDACTED], the [REDACTED], the [REDACTED], and supporting [REDACTED] servers [REDACTED].

Business Continuity Site

A cold site will be equipped to handle short-term business continuity for FEC. Electrical and data communications services will be secured to prepare the facility for potential use as a site for business continuity by a subset of the FEC workforce for the short term.

A cold site will need to be secured to accommodate the equipment and services required to maintain business continuity. The cold site will also accommodate workstations and printers for business continuity. Final preparation of the facility will take place at the time of the disaster dependent upon the details of the disaster. Procedures for the preparation of the cold site facility are maintained in the document – **Cold Site Facility Preparation**.

Section III

Testing the Disaster Recovery Plan

In order to have an effective Disaster Recovery Plan it must be tested on a periodic basis. The results of the test will confirm our planning, procedures, and time estimates. All inconsistencies encountered during the test will be used to update the plan.

Testing of the plan ensures that:

- The Disaster Recovery Plan is complete and viable
- The materials and data are available to process critical applications at an alternate site
- The system software, applications, and data can be restored
- We are in compliance with audit and legal requirements

Disaster recovery testing will be scheduled as needed depending on changes to equipment and or software.

The following are the procedures that will be tested:

- **Network connectivity**

Sufficient networking equipment will be obtained from vendor(s) which will provide LAN connectivity and VPN for [REDACTED], printers, and desktop/laptop PC's.

Will make sure [REDACTED] firewall and network switches are up and going as well, or order, locate, and restore a replacement firewall and network switches and load the backup configuration (kept on emergency flash drive) from current firewall/network switches.

At least two desktops/laptops and a file server will be connected to the test network. (Preferably multiple physical servers, rebuilding our failover cluster if necessary)

Connectivity to the internet will be tested; this will provide VPN access to our remote sites and test system availability into our [REDACTED]. It should also allow e-mail, website, and local intranet access to [REDACTED] domain.

[REDACTED]

Upon declaration of disaster, will order, locate, and restore a replacement [REDACTED] from most recent backup tapes (if applicable). Since [REDACTED] is [REDACTED], will make sure that [REDACTED] is up and going first by assembling physical servers (up to 3) as necessary, then will use offsite Acronis backups located at [REDACTED] to get the latest "image" of our [REDACTED], rebuild if necessary, and start up [REDACTED] and confirm connectivity.

Will establish a connection to our network both local and via Virtual Private Network and test the availability of the system remotely.

- [REDACTED] and [REDACTED]

Upon declaration of disaster, replacement servers will be obtained from vendor(s) and restored from most recent backup tape.

The system will be connected to the network using the off-site test disaster recovery network.

Remote access to the servers will be tested.

- Desktop/laptop PC's

A current model with the hard drive formatted will be utilized for the test.

The PC will be loaded with the required operating system and desktop applications.

The PC will then be connected to the network using the test disaster recovery network. The PC will then be tested to assure that access to all servers on the network is possible and that access to all applications is available.

Section IV

Initial Disaster Response

Appraisal of the Situation

Execution of this plan assumes that the **Corporate Disaster Recovery Team** has declared a disaster and has given direction to the **IT Disaster Recovery Management Team**. It assumes that general assessment of the disaster has been completed, and that information has been relayed to the IT Disaster Recovery Management team. The precise timing of assessment involvement by IT Team members is dependent upon the decision of the Corporate Disaster Recovery Management Team.

Access to employee telephone numbers is found on the FEC Employee List as filed in the on-site storage vault or on the company's intranet site. A list can also be printed from the CD/Flash drive filed in the on-site storage vault, company's off-site storage.

The IT Disaster Recovery Management team leader will immediately implement the Disaster Recovery procedures as outlined in this manual. A copy of the IT Disaster Recovery manual (this document) can be retrieved from the on-site storage vault or alternate storage avenues by FEC authorized personnel. If the on-site storage vault or alternate storage avenues are not available, a copy can be reprinted from Plateau. This procedure will guide the team through an appraisal of the situation and the decisions that must be made.

Declaration of a Disaster

The IT Disaster Recovery Management leader, with input from the team, is responsible for deciding whether to activate the cold site and what portions of the IT Disaster Recovery Plan to implement as per the IT Disaster Recovery Management procedure. The team will also be responsible for deciding if and when to activate the remaining teams.

Disaster Recovery Timeline

Every emergency will be different; thus, this timeline is only provided as a guideline and a suggested sequence of events. It is up to the IT Disaster Recovery Management Team to monitor the timeline and sequence of events and make changes appropriate to the real disaster.

Below is a timeline estimate without a warm site agreement.

Day 1

- Corporate Disaster Recovery Management Team activated by team leader.
- CEO/General Manager/CEO notified of the disaster.
- A disaster is declared, and the Corporate Disaster Recovery Plan is implemented.
- IT Disaster Recovery documents are printed, reproduced, and distributed for review.
- IT Disaster Recovery Teams are activated.
- Corporate Facilities Team and IT Recovery personnel determine extent of disaster and feasibility of salvaging equipment for immediate use or availability of equipment at warehouses and other FEC sites.
- The recovery site is contacted, and the disaster is declared.
- Preparation of the cold site begins.
- [REDACTED] and supporting [REDACTED] servers equipment vendors notified for salvage determination assistance.
- IT Disaster Recovery teams review and update recovery plans as necessary.
- IT Disaster Recovery teams create draft purchase orders with the Procurement Team and update/reprioritize them as necessary; discuss equipment delivery quantities and dates. Create priority list for use during final order.

Day 2

- Salvage determination of [REDACTED] and supporting [REDACTED] completed.
- Procurement orders for network equipment, [REDACTED] mainframe, [REDACTED], desktop PCs, and printers, with associated equipment, according to the priority list determined during purchase order drafting on day 1, delivery destination, delivery dates and quantities.
- IT Disaster Recovery personnel along with recovery tapes and offsite backups are deployed to recovery site.
- Arrange for vendor support (if needed) in setting up the IT equipment at the cold site.

- Begin preparing the cold site for occupancy by business unit personnel see *Cold Site Facility Preparation Details*.
- Corporate Team and the IT Administrative Team assist the recovery teams with equipment, supplies and transportation.

Day 3

- Initial [REDACTED], [REDACTED], are delivered and/or rebuilt to the cold site where setup and restoration commences.
- Networking hub(s) and firewall device delivered and configured
- Limited network connection becomes available from the local area network.
- First six network-attached PCs are delivered to the recovery teams.
- Cold site preparations are completed.

Day 4

- Internet access becomes available at the temporary worksite(s).
- [REDACTED] Applications team starts application recoveries.
- Additional network-attached desktop PCs are delivered to the recovery teams.
- [REDACTED] arrives and setup commences [REDACTED]
- [REDACTED] will be restored from offsite backup located at [REDACTED].
- [REDACTED] delivered to the cold site where setup and restoration commences.

Day 5

- Desktop PCs are delivered to the temporary worksite(s) and connected to the network.
- [REDACTED] operating system restoration commences.
- Database recovery commences.
- Additional desktop PCs are delivered to the cold site

Day 6

- [REDACTED] becomes operational and connected to the network.
- Additional file servers are delivered to the cold site where setup and restoration commences.
- Databases ready for use

Day 7

- [REDACTED] system restoration completed and connected to the network.
- Additional desktop PCs are delivered to the cold site.

Day 8

- Additional desktop PCs are delivered to the cold site

Day 9

- All systems in emergency production mode.
- IT teams go into maintenance mode (maintaining systems and assisting in the business units recover efforts).
- **IT Management Team** works with the **Disaster Recovery Management Team** to plan for either or a combination of a long-term temporary work situation, a restoration of the headquarters site, or a move to other site(s) until the headquarters site can be restored.

Section V Disaster Recovery Teams

Team Structure and Duties

To facilitate the disaster recovery effort, teams have been established and each team has been assigned specific functions. (See the team structure diagram in the Team Procedures section of this chapter). Each team has an assigned primary and alternate team leader who is responsible for determining who the other team members that will be needed to accomplish the mission.

Two distinct levels of teams have been established. These two groups are:

The Corporate Team (Emergency Response Team - CERT)

The Corporate teams have direct responsibility for managing the overall disaster recovery effort including providing the **IT recovery teams** with the support they require to restore the data processing infrastructure. This team and their procedures were assembled as a separate project and have been synchronized with the **IT Disaster Recovery Plan**. Specific teams and the general responsibility of each team is documented in the Emergency Response Team checklists and procedures as developed by that team.

Members of Corporate Team are:

Antonio R. Sanchez, Jr., CEO/General Manager
 Helen Jo Wallin, Office Manager
 Glenn Barleben, IT Manager
 Suzy Howard, Accounting Manager
 Barry Bass, Line Superintendent I
 Rodrick "Rick" Ragland, Line Superintendent II
 Michael McCord, Engineering Manager (IT Manager Backup)
 Thom Moore, Member Services

The IT Recovery Team

These teams have direct responsibility for restoring the data processing infrastructure for the Cooperative. Specific teams and the general responsibility of each team includes:

Network Team – This team is responsible for providing access to the FEC wide area network from the cold site, the recovery team's site and for the business units located at various temporary sites.

██████████ **Team** – This team is responsible for restoration and availability of the ██████████ server and the applications residing on it.

██████████ **Team** – This team is responsible for the restoration and availability of the ██████████ and the applications residing on them.

Members of the above three areas are:

Glenn Barleben, IT Manager
 Stephan Teconchuk, Meter Data Analyst
 Michael McCord, Engineering Coordinator
 Vani Puppala, GIS Specialist

Helen Jo Wallin, Billing Manager/HR Manager

Desktop Team – This team is responsible for providing IT and the business units with the desktop equipment and software they need to facilitate recovery efforts and for business continuity purposes.

Administrative Team – This team provides the other IT teams with the support they require to facilitate the recovery effort. This includes office equipment and supplies, coordinating travel plans, and coordinating with the Corporate Teams where necessary.

Members of the above two areas are:

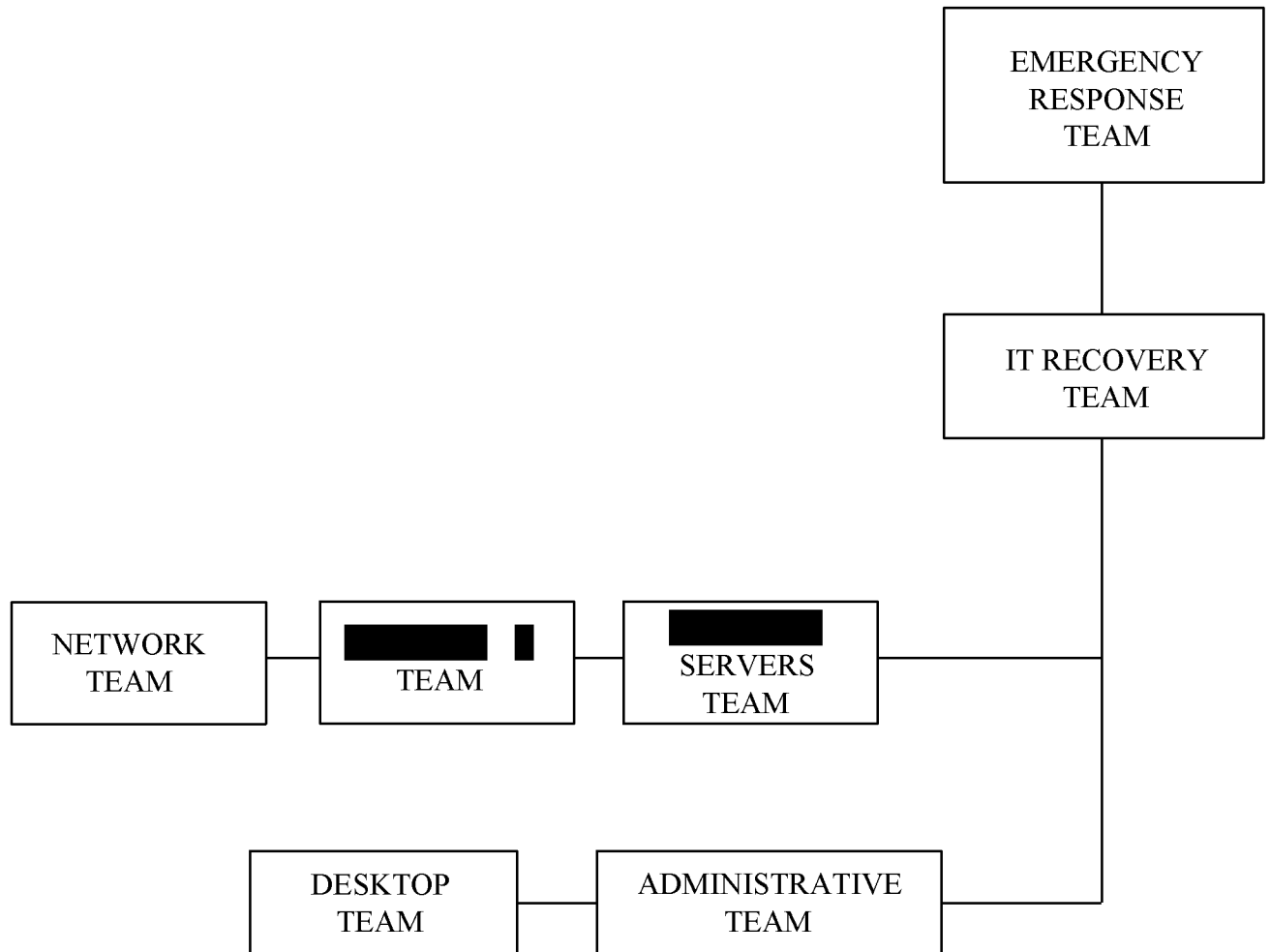
Helen Jo Wallin, Billing Manager/HR Manager

Michelle Hammonds, Receptionist

Team Procedures

The predefined guidelines and procedures will be provided to each team. These are meant to provide guidance to the team leader and the team during an emergency. It does not, nor can it, cover all possibilities of an emergency. Also, it only covers the worst-case scenario, which may not be the existing condition. Therefore, it is the responsibility of the team leader to modify and improvise the procedure as necessary during a disaster. The Team Leader in most cases will be the IT Manager. If the IT Manager is unavailable due to illness, etc., the Engineering Manager will serve as the backup for the IT Manager if necessary and/or assist the IT Manager with procedures that the IT Manager is unable to perform.

Disaster Recovery Team Organizational Chart



Section VI

Contacts and Key Suppliers for Office Services and Information Technology:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Media Contacts:

Quay County Sun

PO Box 1408
Tucumcari NM 88401
(575) 461-1952

Clovis News Journal

521 Pile St.
Clovis NM 88102-1689
(575) 763-3431

De Baca County News

PO Box 448
Fort Sumner NM 88119
(575) 355-2462

KSSR Radio

2828 Historic Rt 66
Santa Rosa NM 884735
(575) 472-5777

KTNM Radio

901 S Date
Tucumcari NM 88401
(575) 461-0522

KWKA Radio

South of Clovis
Clovis, NM 88101
(575) 219-6246

KIJN Radio

PO Box 458
Farwell, TX
(806) 481-3318

KAMR - TV

Amarillo, TX
(806) 383-3321

KVII - TV

Amarillo, TX
(806) 373-1787

Portales News Tribune

101 E 1st St
Portales, NM 88130
(575) 356-4481

The Communicator

241 S. 4th Street
Santa Rosa NM 88435
(575) 472-3555

State Line Tribune

PO Box 255
Farwell TX 79325
(806) 481-3681

KICA Radio

10th & Sycamore
Clovis NM 88101
(575) 763-4500

KSMX Radio

208 E Grand
Clovis NM 88101
(575) 763-4649

KCLV Radio

1900 N Thornton St
Clovis, NM 88101
(575) 769-1780

KSEL Radio

42437 US HWY 70
Portales, NM 88130
(575) 359-1759

KFDA - TV

Amarillo, TX
(806) 383-2226

KOAT - TV

Albuquerque, NM
(505) 884-7777

KOB - TV
Albuquerque, NM
(505) 243-4411

KENW - TV
Portales, NM
(575) 562-2112

ix. Physical Security Incidents

On-Site Emergency Response Protocol

Protect and secure employees and people on-site:

Fire:

In case of fire, every person in the building will be informed by means of the intercom to proceed to their designated exits. These exits can be found at multiple locations throughout the building. Maps of the building and exits are located at strategic points to help guide people to those exits. Before exiting, the dispatcher will call 911 after the announcement to evacuate has been given. The fire extinguishers in the building are only to be used in aiding people in the evacuation process. They are not to be used in fighting the fire!

Tornado:

In case of a tornado warning, either by radio or the city's civil defense warning sirens, every person in the building will be informed by means of the intercom to proceed to the building's basement. In lieu of a basement, employees would be instructed to go to the center of the building away from any windows and take cover. Once in the basement or center of building, all persons are to remain there until it has been established by either radio or the city's warning system that the threat has passed.

Robbery:

In case of a robbery, all individuals within sight of the perpetrator(s) will comply with their demands. If an employee is out of sight of the act, but is aware there is a robbery occurring, and can safely dial the telephone without being detected, that employee should dial 911. Otherwise, the dispatcher will notify the authorities after the perpetrator (s) has left the facility.

Bomb Threat:

In case of a bomb threat, all persons will be notified to evacuate the building through designated exits. Notification will be done by an employee walking around the facility and informing all individuals to evacuate. **At no time will the facilities phone system be used!** Before evacuation, all radios will be turned off. Once everyone is outside and at a safe distance away, a designated person will call 911 via a cell phone. All threats, be they verbal and in person, by phone, or by note will be taken seriously. If the threat is from an individual that is physically present, then all

persons that are within sight of the perpetrator(s) should comply with whatever is asked of them. Once the perpetrator(s) has left the facility, then all persons remaining in the facility should exit it in an orderly fashion. If it is determined that it is still not safe to evacuate the facility, then the dispatcher should dial 911, via cell phone, and all persons will remain where they are until it is deemed safe to evacuate.

x. Event Response and Reporting Plan

OBJECTIVE

To comply with the North American Electric Reliability Corporation (NERC) and/or Southwest Power Pool (SPP) Regional Reliability Standards. NERC has been designated as the Electric Reliability Organization by the Federal Energy Regulatory Commission (FERC). Standard EOP-004 requires the reporting of events that jeopardize the operation of the Bulk Electric System.

The Southwest Power Pool (SPP) is the Reliability Coordinator and Balancing Authority for the area served by Farmers' Electric Cooperative (FEC). FEC's wholesale transmission service supplier, Southwestern Public Service Company (SPS) is the area Generator Operator, Transmission Planner and Transmission Operator.

Requirement R1: Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-4 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).

Measure M1: Each Responsible Entity will have a dated event reporting Operating Plan that includes protocol(s) and each organization identified to receive an event report for event types specified in EOP-004-4 Attachment 1 and in accordance with the entity responsible for reporting.

Requirement R2: Each Responsible Entity shall report events specified in EOP-004-4 Attachment 1 to the entities specified per their event reporting Operating Plan by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 PM local time will be considered the end of the business day).

Measure M2: Each Responsible Entity will have as evidence of reporting an event to the entities specified per their event reporting Operating Plan either a copy of the completed EOP-004-4 Attachment 2 form or a DOE-OE-417 form; and some evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 PM local time will be considered the end of the business day).

(NOTE) Certain conditions require reporting to DOE within one-hour of Incident. Any DOE filing (OE Form 417) shall also be filed simultaneously with NERC, SPP and NMPRC.

EVENT RESPONSE AND REPORTING PROCEDURE

SECTION 1: Operations Personnel Response and Reporting

Safety:

When a **Human Caused Event** is suspected, exercise extreme caution; do not attempt to remove any suspicious device or approach suspicious persons.

Isolate affected infrastructure and restore system operation if possible. Preserve the scene for Law Enforcement investigative purposes.

Inspections of energized equipment must only be performed by qualified personnel of FEC. All relevant safety equipment must be worn during the inspection process, including but not limited to, hard hats, safety glasses, and hot work gloves where needed. Only authorized personnel are allowed inside the fence line of any substation that is owned and controlled by FEC.

Recognition of an Actual or Suspected “Human Caused” Event or Action:

A **Human Caused Event** is defined as the intentional, deliberate operation or miss-operation, or attempted operation of transmission or distribution infrastructure including conductors, structures, substations, and communications equipment; and/or intentional, deliberate destruction or attempted destruction of transmission or distribution infrastructure including conductors, structures, substations, and communications equipment. Discovery of a suspicious device in close proximity to critical infrastructure including substation equipment is considered a **Human Caused Event** and includes vandalism.

All Human Caused Events and Vandalism affecting substation infrastructure shall be reported to local Law Enforcement Authorities.

Response and Reporting Process for Field Personnel:

When a Human Caused Event is suspected, exercise extreme caution; do not attempt to remove any suspicious device or approach suspicious persons.

Contact authorities in the following order: Local Law Enforcement, FEC Supervisory Personnel (Line Superintendent #1, Line Superintendent #2, Manager of Engineering and CEO/General Manager).

Isolate affected infrastructure and restore system operation if possible. Preserve the scene for Law Enforcement investigative purposes.

Response and Reporting Process for Management Personnel (Line Superintendent #1, Line Superintendent #2, Manager of Engineering, Director of Member Service and CEO/General Manager):

Verify that local Law Enforcement has been contacted.

Determine if a Human Caused Event has in fact occurred and if the Event appears to be an isolated act of vandalism.

If the Event appears to have greater impact than an isolated act of vandalism:

Contact all FEC service personnel to alert them to the situation and perform site inspections of other substation infrastructure.

Contact all local Law Enforcement Agencies in the FEC service area and inform them of the Event.

Contact SPS Transmission Dispatch to alert SPS of the Event.

Contact New Mexico Rural Electric Cooperative Association (NMRECA) to alert them of the Event.

If FEC management receives a report of a wide-area **Human Caused Event** from other sources including SPS, Law Enforcement, FBI, or neighboring utility, FEC management shall alert FEC Operations Personnel.

SECTION 2: Management Personnel Event Reporting to NERC, DOE, SPP and NMPRC

FEC Employees responsible for submitting Reports to NERC, DOE, SPP and NMPRC:

As determined by FEC, or at the request of SPP or SPS, FEC personnel, including the CEO/General Manager, Director of Member Services, Manager of Engineering, Line Superintendent #1, and Line Superintendent #2, and additional personnel as required by the FEC Line Superintendent #1 or Line Superintendent #2 shall cooperate and assist in the investigation process and required reporting.

Definitions:

Facility - An FEC Facility is as defined in the NERC Glossary of Terms as “A set of electrical equipment that operates as a single Bulk Electric System element such as a line, generator, shunt compensator, transformer etc.

Bulk Electric System (BES) – Utilizing the NERC Glossary of Terms as updated August 2019. The BES definition does not include facilities used in the local distribution of electric energy.

It is FEC’s determination that all of FEC’s potential BES elements are in fact facilities used in the local distribution of electric energy as they are designed and operated to receive energy from wholesale suppliers and distribute that energy to end use retail consumers. Therefore, FEC facilities currently will not reach the “Threshold for

Reporting”, to NERC and the SPP, for any event listed for a Distribution Provider in Attachment 1 of the Standard.

FEC shall still provide reports to DOE and NMPRC as outlined below.

Attachment 2-EOP-004, NERC Event Reporting Form

National Electric Reliability Corporation (NERC) “Event Reporting Form”; requires filing of the completed EOP-004 Attachment 2 Form or a DOE-OE-417 Form by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity’s next business day (4 PM local time will be considered the end of the business day). File copy (PDF) of OE-417 to systemawareness@nerc.net and cc to esisac@nerc.com; or Fax to 404-446-9770; or by voice 404-446-9780, Option 1.

Events that require reporting to NERC:

1. Damage or destruction of an FEC BES Facility that results from actual or suspected intentional human action.
2. Physical threat to an FEC BES Facility or BES Control Center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility.
3. Suspicious device or activity at an FEC BES Facility.
4. **(Note) DOE OE-417 Form can be filed with NERC instead of NERC Form**

Attachment 3; EOP-004, contains DOE reporting requirements and DOE Form OE-417.

Department of Energy (DOE) Form OE-417; must be filed within 60 minutes of known beginning of event. Form can be filed electronically or by Fax. Online Form available www.oe.netl.doe.gov/oe417.aspx or (PDF) to doehqeoc@oem.doe.gov or Fax 202-586-8485. File updates every 24 hours until event is resolved and final report is due within 72 hours of event resolution.

Events that require reporting to DOE:

1. Physical Attack that causes major interruption or impact
2. Actual or suspected cyber or communications attacks on power system
3. Public Appeals to reduce demand/load
4. Complete failure of electric system

SPP Reporting Requirements and Reporting Contacts:

Southwest Power Pool (SPP); requires the filing of the NERC Reporting Form or OE-417 Form simultaneously with DOE and NERC. SPP prefers electronic filing (PDF) to sppevents@spp.org

Events that require reporting to SPP:

1. Any event reported to NERC using Form filed with NERC.

New Mexico Public Regulation Commission (NMPRC) Contacts:

New Mexico Public Regulation Commission (NMPRC); requires the filing of a report simultaneously with NERC and SPP. Report can be made by telephone 1-855-554-2005 and provide information as prompted by the automated system. Reports can also be filed by email to utility.outage@state.nm.us.

Events that require reporting to NMPRC:

Events of more than 30 minutes duration, affecting:

- a. Any event reported to NERC & SPP using Form filed with NERC
- b. More than 10% of Peak Load (9 MW)
- c. Substantially all of a New Mexico Municipality
- d. Customers larger than 1 MW

Within two (2) hours of the commencement of a major interruption of service (or no later than 9:00 AM the following business day for outages occurring after 4:00 PM or on a weekend), the utility division of the commission shall be notified telephonically or by e-mail of the occurrence with a brief description of the occurrence.

Information to be provided in the 2-hour report:

1. Name of Utility
2. Areas Affected
3. Number of Affected Consumers
4. Time the Outage Occurred
5. Reason for the Outage and Other Relevant Details (as known)
6. Length of Outage if Known or Anticipated Length of Outage
7. Reporting Individual's Name and Phone Number

Within three (3) business days a written report shall be filed with the records division of the commission. The written report shall contain the pertinent information on the outage including, but not limited to, time of occurrence, duration, cause, facilities affected, MW of load lost, MWH of lost sales, estimated number of consumers affected, municipalities and counties wholly or partially interrupted, and actions taken by the utility to correct and prevent recurrence of the outage.

ANNUAL REVIEW

This Policy shall be reviewed with Operations Personnel and those with Management Reporting Responsibility once each calendar year. Included in the annual review will be a review of the list of events and threshold for reporting contained in Attachment 1 of the Standard.

DATA RETENTION

FEC shall keep data related to any incident since the date of the last Audit, including evidence of reporting an event, copy of the completed EOP-004 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of recognition.

REFERENCE DOCUMENTS:

1. Attachment 1, Event Reporting Contact Information
2. Attachment 2, NERC Event Reporting Form
3. Attachment 3, DOE Criteria and Reporting Form

VERSION HISTORY

Version	Date	Action	Change Tracking
1	6/22/2009	Procedure Revisions	Revised
2	12/21/2009	Revise R2 Statement, Page 1	Revised
3	12/27/2010	Include Annual Review Provision	Revised
4	08/06/2013	Revise Policy & Reporting	Revised
5	08/20/2013	Spelling Correction	Revised
6	12/05/2013	Major Revision	Revised
7	01/15/2014	NMPRC Reporting Change	Revised
8	01/25/2017	Move Contact Info To Attachment	Revised
9	07/07/2017	Update NERC Standard Reference	Revised
10	12/17/2019	Update To NERC Standard EOP-004-4	Revised

Attachment #1 Event Reporting Contact Information

Contact information listed below shall be verified one each calendar year by one or more employees listed as responsible for submitting reports under this Plan.

Clovis Police Department:	575-763-9472
Curry County Sheriff Department:	575-769-2335
Tucumcari Police Department:	575-461-2280
Quay County Sheriff Department:	575-461-2720
Santa Rosa Police Department:	575-472-3605
Guadalupe County Sheriff Department:	575-472-3711
De Baca County Sheriff Department:	575-355-7433
New Mexico State Police: (Clovis)	575-763-3427
(Santa Rosa)	575-472-3388
(Tucumcari)	575-461-3300
SPS Transmission Operator (Amarillo, TX):	[REDACTED]
NMRECA Statewide Office:	505-982-4671

NERC:

[REDACTED]

DOE:

[REDACTED]

SPP:

[REDACTED]

NMPRC:

505-827-4463 Fax
505-827-4500 Voice – Utility Division

Contact information verified 09-10-2019, by personal telephone contact and email conducted by Antonio R. Sanchez, Jr., CEO/General Manager.

EOP-004 Attachment 2: Event Reporting Form		
Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net , Facsimile 404-446-9770 or voice: 404-446-9780.		
Task		Comments
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/>
4.	Event Identification and Description: <div> <div> (Check applicable box) <input type="checkbox"/> Damage or destruction of a Facility <input type="checkbox"/> Physical Threat to a Facility <input type="checkbox"/> Physical Threat to a control center <input type="checkbox"/> BES Emergency: <div> <input type="checkbox"/> public appeal for load reduction <input type="checkbox"/> system-wide voltage reduction <input type="checkbox"/> manual firm load shedding <input type="checkbox"/> automatic firm load shedding </div> <input type="checkbox"/> Voltage deviation on a Facility <input type="checkbox"/> IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) <input type="checkbox"/> Loss of firm load <input type="checkbox"/> System separation <input type="checkbox"/> Generation loss <input type="checkbox"/> Complete loss of off-site power to a nuclear generating plant (grid supply) <input type="checkbox"/> Transmission loss <input type="checkbox"/> unplanned control center evacuation </div> <div> Written description (optional): </div> </div>	

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net , Facsimile 404-446-9770 or voice: 404-446-9780.

Task		Comments
	<input type="checkbox"/> Complete loss of voice communication capability <input type="checkbox"/> Complete loss of monitoring capability	

Attachment 3 – DOE OE-417 Form

U.S. Department of Energy Disturbance Reporting Requirements

The U.S. Department of Energy (DOE), under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. DOE collects this information from the electric power industry on Form OE-417 to meet its overall national security and Federal Energy Management Agency's Federal Response Plan (FRP) responsibilities. DOE will use the data from this form to obtain current information regarding emergency situations on U.S. electric energy supply systems. DOE's Energy Information Administration (EIA) will use the data for reporting on electric power emergency incidents and disturbances in monthly EIA reports. In addition, the data may be used to develop legislative recommendations, reports to the Congress and as a basis for DOE investigations following severe, prolonged, or repeated electric power reliability problems.

Every Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity must use this form to submit mandatory reports of electric power system incidents or disturbances to the DOE Operations Center, which operates on a 24-hour basis, seven days a week. All other entities operating electric systems have filing responsibilities to provide information to the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity when necessary for their reporting obligations and to file form OE-417 in cases where these entities will not be involved. EIA requests that it be notified of those that plan to file jointly and of those electric entities that want to file separately.

Special reporting provisions exist for those electric utilities located within the United States, but for whom Reliability Coordinator oversight responsibilities are handled by electrical systems located across an international border. A foreign utility handling U.S. Balancing Authority responsibilities, may wish to file this information voluntarily to the DOE. Any U.S.-based utility in this international situation needs to inform DOE that these filings will come from a foreign-based electric system or file the required reports themselves.

Form OE-417 must be submitted to the DOE Operations Center if any one of the following applies (see Table 1-EOP-004-4 — Summary of NERC and DOE Reporting Requirements for Major Electric System Emergencies):

1. Uncontrolled loss of 300 MW or more of firm system load for more than 15 minutes from a single incident.
2. Load shedding of 100 MW or more implemented under emergency operational policy.
3. System-wide voltage reductions of 3 percent or more.
4. Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
5. Actual or suspected physical attacks that could impact electric power system adequacy or reliability; or vandalism, which target components of any security system. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
6. Actual or suspected cyber or communications attacks that could impact electric power system adequacy or vulnerability.
7. Fuel supply emergencies that could impact electric power system adequacy or reliability.
8. Loss of electric service to more than 50,000 customers for one hour or more.
9. Complete operational failure or shut-down of the transmission and/or distribution electrical system.

The initial DOE Emergency Incident and Disturbance Report (form OE-417 – Schedule 1) shall be submitted to the DOE Operations Center within 60 minutes of the time of the system disruption. Complete information may not be available at the time of the disruption. However, provide as much information as is known or suspected at the time of the initial filing. If the incident is having a critical impact on operations, a telephone notification to the DOE Operations Center (202-586-8100) is acceptable, pending submission of the completed form OE-417. Electronic submission via an on-line web-based form is the preferred method of notification. However, electronic submission by facsimile or email is acceptable.

An updated form OE-417 (Schedule 1 and 2) is due within 48 hours of the event to provide complete disruption information. Electronic submission via facsimile or email is the preferred method of notification. Detailed DOE Incident and Disturbance reporting requirements can be found at: <http://www.oe.netl.doe.gov/oe417.aspx>.

Drills

- a. A drill shall be conducted annually to test this EOP if the EOP is not implemented in response to an incident within the last 12 months. (Keep records of all drills conducted.)
- b. This EOP will be revised as needed after each drill.
- c. At least 30 days prior to at least one drill each year, FEC will notify commission staff by email or other written form, of the date, time, and location of the drill.

Emergency Operation Plan Activation History

This section sets forth each incident in the prior calendar year that required COOP to activate its EOP and a summary of the circumstances that required activation. This information along with a summary after-action report, including lessons learned and an outline of changes made to the EOP as a result, if any, will be filed with the annual EOP submittal to the Public Utility Commission of Texas.

AFFIDAVIT OF
Antonio R. Sanchez, Jr., CEO/General Manager
(Affidavit of Entity's Highest-Ranking Official)

Antonio R. Sanchez, Jr., of lawful age, being duly sworn upon oath states as follows:

1. I am the CEO/General Manager of Farmers' Electric Cooperative, Inc. of New Mexico ("FEC"). I have served in this position since June 1, 2022.
2. FEC was formed in 1938, by its members as an electric cooperative under New Mexico law. FEC provides power to members in Curry, De Baca, Guadalupe, Roosevelt, Quay, Harding and San Miguel Counties in New Mexico and to less than 100 metered accounts along the New Mexico – Texas border in portions of Deaf Smith, Oldham, and Parmer Counties in west Texas.
3. Relevant operating personnel are familiar with and have received training on the contents of this Emergency Operations Plan (EOP), and such personnel are committed to following the EOP except to the extent deviations are appropriate as a result of specific circumstances during the course of an emergency.
4. This EOP has been reviewed and approved by the appropriate executives.
5. Required emergency activation drills have been conducted.
6. This EOP or an appropriate summary has been distributed to local jurisdictions as needed.
7. FEC maintains a business continuity plan to address returning to normal operations after disruptions caused by an incident.
8. FEC's emergency management personnel, designated to interact with local, state, and federal emergency management officials during emergency events have completed NIMS training, specifically IS-100.c, IS-200.c, IS-700.b and IS-800.d.

Antonio R. Sanchez, Jr.

Antonio R. Sanchez, Jr., CEO/General Manager
Farmers' Electric Cooperative, Inc.
of New Mexico

Subscribed and sworn to before me this 10th day of March, 2023.

Sharon Joann Tipton

Notary Public

Seal

STATE OF NEW MEXICO
NOTARY PUBLIC
SHARON JOANN TIPTON
Commission No: 1073579
Commission Expires: March 22, 2026

My commission expires: March 22, 2026