

Appendix I

ESCC - Assessing and Mitigating the Novel Coronavirus (COVID-19): A Resource Guide

Sequester schedule	2 weeks / 12-hour shifts	2 weeks / 12-hour shifts	6 days / 12-hour rotating shifts	14 days / 12-hour shifts	<p>Put criteria in place for employee "At Home Reserve" with protocols to follow away from work to ensure health.</p> <p>Employees at home regardless of classification are paid straight time.</p> <p>Maintain list of potential people to supplement operators (e.g., retirees).</p> <p>Non-sequestered employees paid their regularly scheduled hours to stay home.</p> <p>Sequestered employees paid for all hours inside the plant (straight time for regularly scheduled shift, time-and-a-half for all other hours).</p> <p>Next sequester crew identified and monitored.</p>
--------------------	--------------------------	--------------------------	----------------------------------	--------------------------	--

Mutual Assistance for Generation Considerations

This section is designed to provide requesting and responding investor-owned electric companies, public power utilities, independent power producers, and electric cooperatives guidance on considerations for mutual assistance when needed to continue generation plant operations during the COVID-19 pandemic.

Specific guidance for traditional mutual assistance during this pandemic can be found in the “Mutual Assistance Considerations” portion of this Resource Guide.

Regardless of the method of staffing generation plant control rooms, the safety and health of all employees is the priority. Site-specific and company-specific training will be required to operate any generation plant.

Mutual assistance normally is used to help restore electric service to customers and typically is focused on transmission and distribution infrastructure. The COVID-19 pandemic has motivated generation entities to consider the use of mutual assistance for generation plant operation.

Considerations for Fossil, Gas, Nuclear, and Renewable Generators:

Personnel

Consider the use of existing employee work stoppage plans as a resource in planning for the use of personnel not currently assigned to plant operation.

- Keep a central list of all employees with skills who can be called from corporate/tech support (such as former operators or plant engineers/managers) and use that list for consistent communications across the fleet.
- Maintain a list of retirees or other individuals with relevant qualifications who could be called upon to help operate the control room first, prior to reaching out to another company/utility.
 - Consider recent control-board-trained operators (retired, transferred, etc.) for temporary employment.
 - Share retiree list, including qualifications, with other companies for operators.
 - Keep in mind retirees likely will fall into a higher-risk group for COVID-19.
- Consider the use of third-party contractor operators to supplement plant operators, keeping in mind they may lack familiarity with the site and will require additional training and supervision.
- Create a thorough list of experience and qualifications needed to operate a particular unit. Important details include fuel type, OEM technology, DCS type, environmental controls, certifications, etc. Consider proactively sharing this information internally within your company first and then with neighboring companies.
 - Provide sufficient detail from manufacturers (Emerson Ovation, GE Mark VI, ABB, Honeywell, etc.) without exposing proprietary information.
- Subject to maintaining compliance with pertinent regulatory requirements and NERC Reliability Standards, if reserves permit and the system operator concurs, consider optimizing fleet operations and removing non-committed units from dispatch. Transfer qualified operations

Appendix I

ESCC - Assessing and Mitigating the Novel Coronavirus (COVID-19): A Resource Guide

personnel from non-running units to other higher priority units to supplement the operational workforce.

- Maintain an active list of qualified operators who have recovered from COVID-19 and who can return to the workplace. A returning worker should meet CDC requirements for returning to work.

<https://www.cdc.gov/coronavirus/2019-ncov/healthcare-facilities/hcp-return-work.html>

- Make specific requests when seeking mutual assistance for generation control room personnel. Details should include generation type, fuel type (fossil, hydro, single-cycle gas, combined-cycle gas, nuclear, renewable) as well as equipment and process descriptions, etc.
- Consider proactively developing a Mutual Assistance Agreement with strategic companies within the region or system.

Operations

- Subject to maintaining compliance with pertinent regulatory requirements and NERC Reliability Standards, safely shut down and lay up units not committed for dispatch and/or reserve margins based on load forecasts and other business considerations.
- Consider leaving units in extended or planned maintenance outages in that state as long as possible. Operators at these offline sites could be considered available for a site responding to pandemic challenges.
- Consider shifting operation control to remote operation room to limit onsite operators where possible. This may create additional cybersecurity vulnerabilities that will need to be mitigated; coordination with cybersecurity and IT teams will be important.

Specific Consideration for Nuclear Generation

- Nuclear power plants hold robust emergency plans that define indefinite coping strategies for managing the asset in all conditions, including their minimum staffing requirements. Due to regulations, mutual aid is managed by each license holder.

Lodging and Meals

- Incorporate additional employees into sequestering plans if requesting mutual assistance. Considerations should include (but not be limited to) lodging capability, food/snacks/hydration, food restrictions, other personal needs, transportation, etc.
- Additional guidance for lodging and meals for sequestered employees can be found in the “Control Center Continuity” section of this Resource Guide.

Actions to Take if Mutual Assistance for Generation is Triggered

- Review existing mutual assistance agreements to determine if they apply to generation control room personnel and associated indemnification and liability.
- Engage with unions given the pandemic situation and the path forward to supplement the control operator employee base.

- Engage with state and local licensing and commissions for regulatory relief during the pandemic.
- Coordinate with your respective ISO/RTO, TO, and TOP to ensure they are aware of your pandemic plan.
- Identify potential qualified workers who could be called upon to operate a site.
- Consider using the visitor questionnaire from the “Mutual Assistance Considerations” section of this Resource Guide.
- Follow the terms and conditions of existing mutual assistance or mutual aid agreements.

COVID-19 Interim Cleaning and Disinfection Protocol for Generation Control Rooms

Currently, there are no disinfection protocols that have been tested specifically for SARS-CoV-2, abbreviated “COVID-19,” as an emerging viral pathogen. Per current CDC recommendations, evidence suggests that the novel coronavirus may remain viable for hours to days on surfaces made from a variety of materials. CDC disinfection recommendations are linked below; the details noted in this document are not meant to supersede CDC’s guidance:

<https://www.cdc.gov/coronavirus/2019-ncov/community/organizations/cleaning-disinfection.html>

Cleaning of visibly dirty surfaces followed by disinfection is a best practice measure for prevention of COVID-19 and other viral respiratory illnesses in community settings. Following are recommendations from the CDC’s April 1, 2020, guidance on the cleaning and disinfection of rooms or areas where those with suspected or with confirmed COVID-19 have visited. It is aimed at limiting the survival of novel coronavirus in key environments.

Cleaning and Disinfection Protocols

After person(s) suspected to have COVID-19 has been at facility

- Close off areas used by the potentially ill person(s) and wait as long as practical before beginning cleaning and disinfection to minimize the potential for exposure to respiratory droplets. Open outside doors and windows to increase air circulation in the area. If possible, wait up to 24 hours before beginning cleaning and disinfection.
 - Due to criticality, some areas (i.e., control rooms) may require immediate disinfection and operation from remote locations such as DCS rooms.
 - When cleaning the control room, have all operations personnel operate the unit from the DCS room. Before operations personnel depart the control room, have them deenergize all keyboards and mice (removing batteries.) This will prevent the risk of cleaning personnel tripping the unit.
 - Before the contractor begins cleaning the control room, show them the areas that are not to be cleaned, such as red E-Stop push buttons.
 - DO NOT use a bleach cleaning solution on any computer equipment. Use a 70% alcohol cleaning solution.

- Cleaning staff should clean and disinfect all areas (e.g., offices, bathrooms, and common areas) used by the potentially ill person(s), focusing especially on frequently touched surfaces.
- Signage and red barricades will be utilized to prevent access to suspected areas.
- Heads-up notifications will be sent to plant personnel as an alert.
- Appropriately trained and approved contract personnel will handle cleaning and disinfection upon plant request.

How to Clean and Disinfect

Surfaces

- If surfaces are dirty, they should be cleaned using a detergent or soap and water prior to disinfection.
- For disinfection, diluted household bleach solutions, alcohol solutions with at least 70% alcohol, and most common EPA-registered household disinfectants should be effective.
 - Diluted household bleach solutions can be used if appropriate for the surface. Follow manufacturer's instructions for application and proper ventilation. Check to ensure the product is not past its expiration date. Never mix household bleach with ammonia or any other cleanser. Unexpired household bleach will be effective against coronaviruses when properly diluted.
- Prepare a bleach solution by mixing:
 - Five tablespoons (1/3 cup) bleach per gallon of water or 4 teaspoons bleach per quart of water.
 - Products with EPA-approved emerging viral pathogens claim icons are expected to be effective against COVID-19 based on data for harder to kill viruses. Follow the manufacturer's instructions for all cleaning and disinfection products (e.g., concentration, application method and contact time, etc.).
 - For soft (porous) surfaces, such as carpeted floor, rugs, and drapes, remove visible contamination if present and clean with appropriate cleaners indicated for use on these surfaces.
 - If the items can be laundered, launder items in accordance with the manufacturer's instructions using the warmest appropriate water setting for the items and then dry items completely.
 - Otherwise, use products with the EPA-approved emerging viral pathogens claims that are suitable for porous surfaces:

<https://www.americanchemistry.com/Novel-Coronavirus-Fighting-Products-List.pdf>

Linens, Clothing, and Other Laundry Items

- Do not shake dirty laundry; this minimize the possibility of dispersing virus through the air.
- Wash items as appropriate in accordance with the manufacturer's instructions. If possible, launder items using the warmest appropriate water setting for the items and dry items

completely. Dirty laundry that has been in contact with a potentially ill person(s) can be washed with other people's items.

- Clean and disinfect hampers or other carts for transporting laundry according to guidance above for hard or soft surfaces.

Personal Protective Equipment (PPE) and Hand Hygiene

- Cleaning staff should wear disposable gloves and gowns for all tasks in the cleaning process, including handling trash.
 - Gloves and gowns should be compatible with the disinfectant products being used.
 - Additional PPE might be required based on the cleaning/disinfectant products being used and whether there is a risk of splash.
 - Gloves and gowns should be removed carefully to avoid contamination of the wearer and the surrounding area. Be sure to clean hands after removing gloves.
- Gloves should be removed after cleaning a room or area occupied by potentially ill persons. Clean hands immediately after gloves are removed.
- Cleaning staff should report breaches in PPE (e.g., tear in gloves) or any potential exposures to their supervisor immediately.
- Cleaning staff and others should clean hands often, including immediately after removing gloves and after contact with a potentially ill person, by washing hands with soap and water for 20 seconds. If soap and water are not available and hands are not visibly dirty, an alcohol-based hand sanitizer that contains 60-95 percent alcohol may be used. However, if hands are visibly dirty, always wash hands with soap and water.
- Follow normal preventive actions while at work and home, including cleaning hands and avoiding touching eyes, nose, or mouth with unwashed hands. Additional key times to clean hands include:
 - After blowing one's nose, coughing, or sneezing.
 - After using the restroom.
 - Before eating or preparing food.
 - After contact with animals or pets.
 - Before and after providing routine care for another person who needs assistance (e.g., a child).

Additional Resources

Nuclear Generation: NRC Issues Instructions for Obtaining Relief from Work Hours Rules

On March 28, 2020, Ho Nieh (Director, Office of Nuclear Reactor Regulation) sent a [letter](#) to the Nuclear Energy Institute outlining a streamlined process for operating nuclear power reactors to obtain exemptions from the requirements of 10 C.F.R. 26.205(d)(1)-(7). The purpose of the exemptions “is to ensure that the control of work hours and management of worker fatigue do not unduly limit licensee flexibility in using personnel resources to most effectively manage the impacts of the COVID-19 [Public Health Emergency]. . . .” The letter provides that if a licensee determines that its staffing levels will be affected by the COVID-19 emergency and no longer can meet the requirements of 10 CFR 26.205(d)(1)-(7), then the licensee should submit an email requesting an exemption to the facility’s NRC project manager (with a copy to the NRC Document Control Desk). The request should be submitted “as soon as practicable and no less than 24 hours before [the licensee] would be out of compliance with the regulations.” All such requests should include the following information:

- a statement that the licensee no longer can meet the work-hour controls of 10 CFR 26.205(d) for certain positions;
- a list of positions for which the licensee will maintain current work-hour controls under 10 CFR 26.205(d)(1)-(d)(7);
- the date and time when the licensee will begin implementing its site-specific COVID-19 Public Health Emergency fatigue-management controls for personnel specified in 10 CFR 26.4(a);
- a statement that the licensee’s site-specific COVID-19 Public Health Emergency fatigue-management controls are consistent with the constraints outlined in this letter and its attachment; and
- a statement that the licensee has established alternative controls for the management of fatigue during the period of the exemption and that, at a minimum, the controls ensure that for individuals subject to these alternative controls:
 - not more than 16 workhours in any 24-hour period and not more than 86 workhours in any 7-day period, excluding shift turnover;
 - a minimum 10-hour break is provided between successive work periods; 12-hour shifts are limited to not more than 14 consecutive days;
 - a minimum of 6-days off are provided in any 30-day period; and
 - requirements are established for behavioral observation and self-declaration during the period of the exemption.

Appendix I

Supply Chain Considerations

Updated: April 16, 2020

Changes since the last version are highlighted in red

This document provides guidance that investor-owned electric and/or natural gas companies, public power utilities, and electric cooperatives can consider for maintaining adequate supply of inputs and physical equipment during this health emergency. Lists were developed for consideration so that both the volumes of the supply chain need, and the geographic location of suppliers can be determined. Clearly, the extent and duration of this emergency will influence the importance of one supply chain component compared to another.

The guidance in this document was collected from organizations across the industry. The intent is to serve as a general information resource and not to set any industry standards. This document is evergreen and will be updated regularly to reflect additional or revised guidance as it is received.

The three sections provided are:

- Supply Chain Considerations for Industry Critical PPE
- Power Delivery Materials
- Bulk Chemicals Needed for Power Generation and Delivery

It is acknowledged that access plays a key role both for organizations and their suppliers in a pandemic. The access issue is covered more fully in the “Access Considerations” section of this Resource Guide.

Supply Chain Considerations for Industry-Critical PPE (UPDATED)

As the novel coronavirus (or COVID-19) pandemic spreads, the electric power industry recognizes that Personal Protective Equipment (PPE) is in short supply even for first responders and the healthcare sector. Energy and other critical sectors now are considering alternatives to keep workers safe while maintaining reliable service. To assist with these efforts, this section of the Resource Guide provides planning considerations and resources to help investor-owned electric and/or natural gas companies, public power utilities, and electric cooperatives meet their PPE needs by identifying:

- Mission critical PPE, cleaning products, and related supplies for the electric power and natural gas industry;

- Non-government vendors/suppliers for PPE;
- Guidance for engaging those suppliers;
- Creative practices for creating alternative PPE and other protective equipment.

While our sector recognizes that the priority is to ensure that PPE is available for workers in the healthcare sector and first responders, a reliable energy supply is required for healthcare and other sectors to deliver their critical services. The Department of Homeland Security (DHS) emphasized the importance of the energy sector, recently releasing an advisory guidance on Essential Critical Infrastructure Workers (ECIW), that includes energy company and utility workers.

In addition, the Electricity Subsector Coordinating Council (ESCC) has identified a subset of highly skilled energy workers who are unable to work remotely and who are mission-essential during this extraordinary time. Consequently, there is a need to elevate the availability of PPE for workers in the energy sector at the federal, state, and local levels.

Personal Protective Equipment Needs

The supply chain tiger team developed the following material list, which summarizes the critical PPE needs for the electric power and natural gas industries. Tier I items are those items that serve an immediate need where critical infrastructure workers are subject to contact. Tier II are items that are not needed at the time of contact but are in the horizon of the planning scenario of nine months and a 40 percent reduction in workforce.

- Tier I:
 - Nitrile gloves
 - Shoe covers
 - Tyvek suits
 - Goggles / glasses
 - Hand sanitizer
 - Dust masks
 - N95 respirators
 - Anti-bacterial soap
 - Trash bags
- Tier II:
 - Anti-bacterial wipes
 - Disposable thermometers
 - Batteries
 - Alcohol wipes
 - Antiseptic wipes

Non-Government PPE Vendors/Suppliers

The key suppliers of PPE include³:

- 3M
- McKesson
- Walmart
- Amazon
- Costco
- Ecolab
- Johnson & Johnson
- Procter and Gamble

Due to regional variations in the availability of PPE, organizations also are encouraged to look to local sources and partners for obtaining PPE. These localized sources may include hospitality wholesalers (Sysco, US Foods) restaurants, malls, and hotels that may have supplies that are not being used. Some organizations also are working with local distilleries to produce disinfectant products.

Energy sector companies and utilities also are encouraged to connect with their local or state energy officials or emergency operations centers to engage in a discussion about the prioritization of PPE needs, access to restricted areas, and testing.

Guidance for Engaging Suppliers and Local Authorities

When contacting vendors and suppliers, organizations should consider the following key points.

- Our sector recognizes that workers in the healthcare and first responders have first priority when it comes to receiving PPE.
- However, the energy industry is a lifeline sector that generates, transmits, and delivers electricity and natural gas to critical services and end-use customers, such as hospitals, clinics and other first responders.
- The Department of Homeland Security emphasized the importance of these workers, and recently released an advisory guidance on Essential Critical Infrastructure Workers (ECIW), that includes energy company and utility workers. That guidance document can be found online at:

<https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce>

- The sector is not looking for PPE for the entire workforce. Rather, we are working to prioritize supplies for mission-essential workers – a subset of highly skilled energy workers who are unable to work remotely and who are mission-essential during this extraordinary time. More information on these mission-essential workers on-line at:

³ Please note that many retailers and suppliers of PPE now only are selling N95 masks to the healthcare sector and government.

https://www.electricitysubsector.org/-/media/Files/ESCC/Documents/ESCC_Mission_Essential_Workforce_2020.ashx

Creative Solutions

With PPE being in short supply and priority being given to health care workers, the energy sector has sought alternative solutions to adequately supply mission essential workers.

- Hand sanitizer formulation:

- WHO Guidance:

- https://www.who.int/gpsc/5may/Guide_to_Local_Production.pdf

- <https://www.ncbi.nlm.nih.gov/books/NBK144054/>

- Bleach-based sanitizing solution:

- <https://www.dhhs.nh.gov/dphs/holu/documents/hom-sani.pdf>

- <https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/cleaning-disinfection.html>

- Industrial products can be used as alternatives to medical supplies, such as face shields and masks:

- Face shields:

- <https://www.grainger.com/category/safety/face-protection>

- Respirator masks with HEPA filters:

- <https://www.buyinsulationproductstore.com/respirators/>

- Guidance for safely reusing N95 masks with proper decontamination.

- Decontamination Methods for Filtering Facepiece Respirators:

- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2781738/>

- Ultraviolet germicidal irradiation (UVGI):

- <https://www.nebraskamed.com/sites/default/files/documents/covid-19/n-95-decon-process.pdf>

- Ethylene oxide (EtO):

- <https://www.cdc.gov/infectioncontrol/guidelines/disinfection/sterilization/ethylene-oxide.html>

- Vaporized hydrogen peroxide (VHP):

- <https://www.draeger.com/Library/Content/article-vhp-pr-9103500-en-us-1702-1-V7-2.pdf>

- <https://www.battelle.org/newsroom/news-details/battelle-deploys-decontamination-system-for-reusing-n95-masks>

Appendix I

- Maximize use of existing stocks:

<https://www.cdc.gov/coronavirus/2019-ncov/hcp/ppe-strategy/face-masks.html>

<https://kingcounty.gov/depts/health/communicable-diseases/disease-control/novel-coronavirus/PPE-shortage.aspx>

- Homemade masks with pockets for HEPA filter inserts:

<https://www.gfclinic.com/approved-pattern-info-for-homemade-masks/>

- CDC recommendations on using cloth face coverings, including ways to make cloth masks. (Note, these may not be appropriate for situations where Fire Retardant face coverings are required.)

<https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/cloth-face-cover.html>

Organizations also should be aware that the Occupational Safety and Health Administration (OSHA) has relaxed some regulatory requirements to permit the extended use and reuse of respirators, as well as the use of respirators that are beyond their manufacturer's recommended shelf life. This guidance can be found online at:

<https://www.osha.gov/memos/2020-04-03/enforcement-guidance-respiratory-protection-and-n95-shortage-due-coronavirus>

Power Delivery Materials List

The purpose of this section is to list frequently used critical electric power transmission and distribution materials needed for continued safe and reliable operations. It is not intended to include critical spares for major pieces of equipment such as large power transformers. While investor-owned electric companies, public power utilities, and electric cooperatives maintain a certain stock level of the materials that they frequently use, normal consumption rates, potential spikes in regional demand driven by storms or hurricane landfalls, or a disruption to transportation networks rapidly could deplete these stocks over a broad area. Maintaining a functional manufacturing and delivery supply chain for these materials will support safe and reliable operations over the planning scenario of nine months and a 40 percent reduction in workforce.

Broad categories

- Cable (bulk) and accessories
- Common supplies
- Conductor (bulk) and accessories
- Gases and chemicals
- Insulators
- Metering items
- Poles, structures, and accessories

- Sectionalizing and protection items
- Specialized hardware
- Street lighting items
- Transformers and accessories
- Substation control room and communication equipment

Cable (bulk) and accessories

- Cable connector block, lv insulated - various types
- Cable outdoor termination kit - various voltages and types
- Cable, fiber optic - various types
- Cable, lv control -various types
- Cable, primary ug - various sizes and voltages
- Cable, quadruplex urd - various sizes
- Cable, triplex urd - various sizes
- Conduit and fittings - various sizes
- Termination, fiber optic - various types
- Ug cable arrester elbow - various voltages and types
- Ug cable elbow - various voltages and types
- Ug cable splice kit - various voltages and types
- Wire, optical ground (opgw) - various sizes

Common supplies

- Batteries, common - various types
- Batteries, power tool - various types
- Indicator bulbs -various types
- Spill absorbent and containment - various types
- Tape, electrical

Conductor (bulk) and accessories

- Conductor, aac - various sizes
- Conductor, acsr - various sizes

- Conductor, insulated aac - various sizes
- Conductor, insulated copper - various sizes
- Conductor, quadruplex - various sizes
- Conductor, triplex - various sizes
- Connector, auto sleeve for aac, acsr, copper - various sizes
- Connector, compression service - various sizes
- Connector, neutral sleeve for cu, acsr - various sizes
- Connector, sleeve for copper - various sizes

Gases and chemicals

- Corrosion inhibitor - various types
- Distilled water
- Gasoline fuel
- Diesel fuel
- Lubricant, dielectric - various types
- Nitrogen gas, bottled
- Sulfur hexafluoride gas, bottled

Insulators

- Insulator, distribution pin - various voltages and types
- Insulator, distribution post - various voltages and types
- Insulator, distribution strain - various voltages and types
- Insulator, distribution suspension - various voltages and types
- Insulator, house knob - various sizes
- Insulator, strain guy - various sizes and ratings
- Insulator, substation post - various types
- Insulator, transmission bell - various types
- Insulator, transmission non-ceramic - various voltages and types and associated hardware
- Insulator attachment/line construction hardware
- Pin, crossarm for insulator

Metering items

- Meter socket and hub - various types
- Meter, watthour - various types

Poles, structures, and accessories

- Crossarm, wood - various sizes
- Ground rod
- Ground strap, copper braided - various sizes
- Guy anchor shaft
- Guy anchor, helix - various types
- Hardware, guying - various types
- Lattice tower member, steel - various types
- Pole, steel - various sizes
- Pole, streetlight - various sizes
- Pole, wood - various sizes
- Wire, guy - various sizes

Sectionalizing and protection items

- Arrester, lightning distribution line - various voltages
- Capacitor, high voltage - various voltages and kvar
- Fuse cutout - various voltages
- Fuse holder, cutout - various sizes
- Fuse link, cutout - various ratings
- Fuse, low voltage control - various ratings and types
- Fuse, substation high voltage - various ratings and types
- Switch, overhead gang operated - various voltages and types
- Switch, overhead single phase - various voltages and types

Specialized hardware

- Armor rod line guard - various sizes

- Brackets, overhead equipment - various types
- Clamp, parallel groove - various sizes
- Clevis assembly, various types
- Deadend clamp - various sizes
- Deadend grip, preformed - various sizes
- Fasteners, distribution line - various types
- Fasteners, transmission line - various types
- Tie wire, aac - various sizes
- Tie wire, bare copper - various sizes
- Tie wire, preformed - various sizes
- Conductor splicing hardware – various sizes

Street lighting items

- Streetlight lamp
- Streetlight luminaire
- Streetlight photocell

Transformers and accessories

- Boxpad, fiberglass padmount transformer - various sizes
- Bushing, padmount transformer - various voltages and types
- Transformer and circuit breaker insulating mineral oil
- Transformer, overhead 1ph - various voltages and kva
- Transformer, padmount 1ph - various voltages and kva
- Transformer, padmount 3ph - various voltages and kva

Substation control room and communication equipment

- Storage battery cells

Bulk Chemicals Needed for Power Generation and Delivery List

The purpose of this section is to list bulk chemicals critical to power generation and delivery. These chemicals are consumed at various rates by power production processes, so maintaining continued reliable access is critical to generate electricity. The manufacturing and delivery supply chain of these chemicals must remain functional for continued reliable power generation.

- Additives
 - Coal
 - Coal Additives
 - Fuel Oil Additives
- Bulk Chemicals
 - Activated Carbon
 - Ammonia
 - Boric Acid
 - Glycol
 - Hydrazine
 - Hydrochloric Acid (HCl)
 - Lignosulfonate
 - Lithium Hydroxide
 - Sodium Bisulfate
 - Sodium Carbonate (Soda Ash)
 - Sodium Hydroxide (Caustic Soda)
 - Sodium Hypochlorite (Bleach)
 - Sulfur and Molten Sulfur
 - Sulfuric Acid
 - Urea
- Bulk Gases
 - Argon (AR)
 - Carbon Dioxide

Appendix I

ESCC - Assessing and Mitigating the Novel Coronavirus (COVID-19): A Resource Guide

- Hydrogen (H₂)
- Nitrogen (N₂)
- Oxygen (O₂)
- Trailer or Tank Rentals
- Bulk Powders
- CEMS (Protocol) Gases
- Cylinder (Bottled) Gases
 - Argon (AR) Cylinder
 - Carbon Dioxide (CO₂) Cylinder
 - Cylinder Rentals
 - Hydrogen (H₂) Cylinder
 - Nitrogen (N₂) Cylinder
 - Oxygen (O₂) Cylinder
 - Propane
 - Sulfur Hexafluoride (SF₆)
- Lime (Hydrated Lime)
- Wastewater Treatment
 - Flocculent
- Water Treatment
 - Demineralizers
 - Mobile Demineralizers Trucks
 - Water Filtration Equipment
 - Water Treatment Systems
- Water Treatment Chemicals
 - Resins
- Water Treatment Services

Natural Gas Delivery Materials List

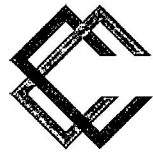
Reliable natural gas delivery depends, in part, on the availability of several components and parts. The availability of these components depends on two key factors: lead times and chokepoints. Natural gas companies typically do not overstock certain components and parts because they tend to be widely available in the market under normal conditions. If these components and parts become in short supply and there are longer lead times for production, the natural gas delivery system could be challenged. In general, the availability of these components and parts also is subject to transportation constraints that can delay delivery. Therefore, both rail and fleet availability can create chokepoints, which, in turn, can create supply chain difficulties.

Long lead time items

- Large diameter valves and accessories
- Electro-fused fittings
- Prefabricated risers
- Prescriptive-based rebuild or maintenance kits for metering and/or regulating stations

Chokepoint items

- Nitrogen – for purging pipes and pressure testing
- Odorant (Mercaptan) – for odorizing natural gas



ESCC

Electricity Subsector
Coordinating Council

ESCC COVID-19 Six-Month Review

AN INTERIM REVIEW OF THE ESCC'S RESPONSE TO THE
COVID-19 GLOBAL PANDEMIC, MARCH-AUGUST 2020

SEPTEMBER 2020

Contents

I. EXECUTIVE SUMMARY	2
II. ESCC PANDEMIC RESPONSE OVERVIEW	4
III. ENGAGEMENT AND COORDINATION WITH THE FEDERAL GOVERNMENT	5
Federal Government Engagement – Accomplishments and Strengths	5
Federal Government Engagement – Opportunities for Improvement.....	6
IV. TIGER TEAM OPERATIONS	8
Tiger Team Operations – Accomplishments and Strengths.....	9
Tiger Team Operations – Opportunities for Improvement	9
V. ESCC COVID-19 RESOURCE GUIDE	11
Resource Guide – Accomplishments and Strengths	12
Resource Guide – Opportunities for Improvement	12
VI. CONCLUSION.....	13
APPENDIX A: ACTION ITEMS	14
APPENDIX B: TIGER TEAM SUBGROUP LEADERSHIP.....	15

I. EXECUTIVE SUMMARY

When coronavirus (or COVID-19) cases began to emerge in the United States earlier this year, the Electricity Subsector Coordinating Council (ESCC) immediately began to engage with its federal government partners to align the industry and government pandemic response efforts and to ensure the resilience of critical electric infrastructure across North America.

Following a series of staff-level engagements between the ESCC Secretariat and the Department of Energy (DOE), the ESCC held its first executive-level coordination call with senior federal government officials in early March. At this point, there were fewer than 200 reported cases of COVID-19 within the United States. These coordination calls bring together executives and government leaders from across the subsector and, when needed, subject matter experts from DOE, the Departments of Homeland Security (DHS) and Health and Human Services (HHS), and the Centers for Disease Control and Prevention (CDC).

Early in the COVID-19 response, the ESCC directed the Secretariat to establish a “Tiger Team” of industry professionals to identify and to help address major potential barriers and challenges during the pandemic. The ESCC Tiger Team, which is led by Southern Company Services Executive Vice President for Operations Stan Connally, includes staff-level representatives from all segments of the industry (investor-owned electric companies, public power utilities, electric cooperatives, federally owned utilities, independent power producers); the Electricity Information Sharing and Analysis Center (E-ISAC); the natural gas and nuclear energy industries; Canadian electric companies; and the federal government.

The Tiger Team has produced a comprehensive Resource Guide that includes tools, resources, and planning considerations for making localized decisions in response to the pandemic. The Resource Guide is updated regularly and is publicly available on the ESCC website, <http://electricitysubsector.org>.

In June, the ESCC began a review process to identify opportunities for enhancing and strengthening the electric power industry’s continued response to this pandemic and to any future incidents that impact the energy grid. Several key themes have emerged from that review process, including:

- **Partnership/Engagement:** While the nature of the COVID-19 pandemic is unlike any recent disasters in North America, ESCC and federal government leaders are using the principles of executive-level engagement from previous incidents to respond to this health emergency. Additional engagement with federal subject matter experts further enhances the industry-government partnership during this pandemic.
- **ESCC COVID-19 Resource Guide:** The ESCC COVID-19 Resource Guide continues to be a central component of the ESCC’s response to COVID-19, and it has been praised by industry, government, and cross-sector partners all over the world as a valuable resource during the pandemic. The Resource Guide should remain central to the ESCC’s pandemic response moving forward, allowing for updates as needed.
- **State and Local Government Outreach:** During the early stages of the pandemic response, the federal government played a critical role in interfacing with state governments on the importance of allocating personal protective equipment (PPE) and testing capabilities to utility

personnel. Additional industry outreach to state and local officials still is needed to enhance their understanding of the critical work performed by mission-essential workers in the electric power industry.

- **Supply Chain and Testing Challenges:** During the early stages of the pandemic, many organizations within the subsector had challenges with obtaining PPE and accessing adequate testing capabilities. To address these issues going forward, the ESCC should consider establishing a standing supply chain team of industry and government experts to build “blue sky” relationships with key suppliers and vendors that would benefit the entire subsector during a major incident.

The ESCC response to the COVID-19 pandemic is ongoing, as the virus continues to spread around the world and across the United States. As the industry sustains a coordinated response alongside partner organizations and the U.S. government, the ESCC will continue to organize collective efforts, to solicit feedback on ongoing initiatives, and to provide tools and resources through the Resource Guide and other materials. This report serves as an interim review of the current state of the ESCC response to COVID-19 and will help inform ongoing efforts during this pandemic or during a resurgence of the virus or a similar health emergency in the future.

II. ESCC PANDEMIC RESPONSE OVERVIEW

The ESCC Secretariat began tracking the coronavirus in late January 2020 in coordination with DOE and participated in several stakeholder calls hosted by DHS and HHS. On February 5, the Secretariat forwarded an E-ISAC bulletin on potential supply chain impacts related to COVID-19 to ESCC stakeholder lists. On March 5, the ESCC co-chairs and members held their first industry-government coordination call. This call included senior leadership from DOE, the Cybersecurity and Infrastructure Security Agency (CISA), and HHS. At this point, there were 164 reported COVID-19 cases in the United States.¹

Over the course of the next several months, subject matter experts from HHS and the CDC joined the industry-government leadership calls to brief on pandemic-related issues, such as testing and contact tracing. The calls also included regular updates from Federal Energy Regulatory Commission (FERC) commissioners and staff, as well as the CEO and staff of the North American Electric Reliability Corporation (NERC), concerning regulatory relief and pandemic response actions taken by FERC and NERC. The calls continued twice a week through May, before transitioning to a once per week cadence in June. By July, the calls were taking place once a month, and they continued into August.

Each ESCC call provides an opportunity for industry and government leaders to address how organizations are responding to the pandemic and to raise any issues or challenges to the group. For example, the calls have covered the need for additional PPE and testing capabilities, as well as workforce sequestration strategies and challenges. The calls also provide a forum for sharing real-time situational awareness, identifying barriers for implementing response plans, and discussing how industry and government can work together to eliminate those barriers.

In early March, the ESCC co-chairs directed the Secretariat to establish a “Tiger Team” of industry professionals to identify and to help address major barriers and challenges. The team is led by Stan Connally, Executive Vice President for Operations at Southern Company Services, and he is supported by the ESCC Secretariat. The Tiger Team includes staff-level representatives from all segments of the industry (investor-owned electric companies, public power utilities, electric cooperatives, federally owned utilities, independent power producers); the E-ISAC; the natural gas and nuclear energy industries; Canadian electric companies; and the federal government. By June, the calls transitioned to once a week, and are now taking place monthly.

The Tiger Team created eight subgroups to focus on specific aspects of the pandemic response. The subgroups are focused on the following topics:

- Control Center Continuity
- Accessing Quarantined and Restricted Environments
- Supply Chain Challenges
- Mutual Assistance Preparation
- Generation Operational Continuity
- IT and Telecommunications Issues
- Responsible Reentry and Return to the Workplace

¹ “Total Number of COVID-19 Cases, by Date Reported,” Centers for Disease Control and Prevention website; <https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/previouscases.html>; Accessed July 9, 2020.

- Internal and External Communications

The subgroups work across the industry to develop and to compile tools, resources, and planning considerations that organizations can use to make localized decisions in response to the pandemic. The groups' work product is funneled into a comprehensive document that is updated regularly. The ESCC Resource Guide, which is publicly available at <http://electricitysubsector.org>, has been praised by electric power industry, government, and cross-sector partners all over the world as a valuable resource during the pandemic.

In late June, the Tiger Team held a series of "hot wash" calls to discuss the ESCC's response, to date, to the pandemic, focusing on three issue areas: 1) engagement and coordination with the federal government; 2) the operation of the Tiger Team and various subgroups; and 3) the development and use of the Resource Guide. Based on the feedback from those calls, the remainder of this report summarizes the ESCC's pandemic response to date and identifies opportunities for improvement.

III. ENGAGEMENT AND COORDINATION WITH THE FEDERAL GOVERNMENT

During a major incident that threatens or impacts the electricity subsector, the ESCC serves as the principal liaison between the federal government and the electric power industry. The ESCC provides high-level situational awareness on response operations and identifies or anticipates industry-wide challenges that could limit the effectiveness of those operations. In turn, the ESCC and government leaders from DOE, DHS, and other federal agencies work together to resolve those challenges quickly. While the nature of the COVID-19 pandemic is unlike any recent disasters in North America, ESCC and federal government leaders are using the principles of executive-level engagement from previous incidents to respond to this health emergency.

Federal Government Engagement – Accomplishments and Strengths

Proactive Outreach from DOE Set the Stage for Productive Industry-Government Coordination

Representatives from across the electric power industry repeatedly have praised DOE leadership and staff for their proactive outreach during the initial response to the COVID-19 pandemic. At the staff level, DOE began engaging with the ESCC Secretariat in late January before COVID-19 cases within the United States started to increase dramatically. DOE has continued that engagement throughout the pandemic response, and, as the Sector Specific Agency (SSA) for the industry, it effectively has represented the subsector's interests within the federal government.

For example, DOE was instrumental in securing and distributing cloth masks and a limited number of test kits from federal government stockpiles. At times, the federal government did not have the resources to meet specific industry needs. In those instances, DOE's leadership and staff provided direct and frank feedback and worked to find alternative sources/methods for industry requests.

Senior-Level Engagement with Government Leaders and Subject Matter Experts Facilitates Effective Coordination with Industry

The COVID-19 pandemic continues to be an unprecedented global health emergency. The response requires coordination and engagement with a wider range of U.S. government agencies and additional expertise beyond the electric power industry's historical interactions with federal partners. To address those needs, the ESCC has engaged proactively with DOE and representatives from HHS and CDC on regular coordination calls with industry leaders.

Early on, federal government representatives provided key subject matter expertise and context on the ongoing pandemic and how the U.S. government's actions would impact the subsector and the economy. For example, during an April 9 ESCC briefing, Admiral Brett P. Giroir, the HHS Assistant Secretary for Health, provided an update to the group on COVID-19 testing. Another ESCC-organized call included CDC representatives who discussed contact tracing. The rapidly evolving nature of the COVID-19 pandemic and the need to adapt quickly, while maintaining operations, makes this type of timely information extremely useful to industry leaders.

DHS/FEMA Coordination Calls Provide a Helpful Cross-Sector Perspective on the Pandemic Response

In 2019, DHS and the Federal Emergency Management Agency (FEMA) created a new Emergency Support Function (ESF) under the National Response Framework focused on cross-sector coordination. As part of the new ESF-14, FEMA and CISA hosted regular coordination calls with all 16 critical infrastructure sectors to discuss the pandemic. The ESCC Secretariat participated in these calls to provide updates on the subsector's response. Representatives from the electric power industry noted that these calls provided a helpful perspective on other sectors' response to this health emergency.

Regulatory Relief Has Provided Needed Flexibility for the Electric Power Industry During the Pandemic

FERC and NERC have played key roles in aiding the electric power industry during the pandemic with discretionary enforcement of some federal regulations. For instance, in April, FERC commissioners approved a request submitted by NERC to defer implementation of seven reliability standards. This, and other efforts, gave the industry additional flexibility to respond to COVID-19, reallocate resources, and maintain a focus on critical operations, while not undermining the safety of workers and the reliability of the energy grid.

Federal Government Engagement – Opportunities for Improvement

Access and Distribution of PPE Could Be Improved

Access to, and distribution of, PPE challenged many organizations early on during the COVID-19 pandemic, creating widespread frustration. Many organizations turned to lower-quality suppliers out of desperation. Going forward, the electricity subsector would benefit from a clearly defined process and timeline for securing and distributing additional quantities of PPE, including from federal, state, and local stockpiles.

Organizations widely have acknowledged that the issues experienced with PPE were largely due to the surging global demand for these resources and the strain placed on global supply chains. Public- and

private-sector efforts to secure this equipment were hampered by the backlog in orders and a limited supply of these resources at the beginning of the pandemic when available stocks already were dedicated to medical personnel.

The ESCC has experienced varying levels of success working with U.S. government agencies and state governments on the PPE issue. While DOE and CISA have tried to help the electricity subsector and have succeeded in securing and shipping some quantities of PPE, challenges have arisen due to competition with other critical infrastructure sectors. At the state level, access to PPE has varied widely from state to state, as some state governments cooperated extensively with utilities to secure PPE, while other state governments took limited or no action on the issue.

To address these issues, the ESCC should consider establishing a standing supply chain team of industry and government experts to build “blue sky” relationships with key suppliers and vendors that would benefit the entire subsector during a major incident. This team could explore the option of stockpiling PPE, including fire-retardant masks, that could be used during a major industry response to wildfires, hurricanes, earthquakes, or other incidents with catastrophic impacts.

“Blue Sky” Outreach to State and Local Leaders Can Help Improve the Understanding of the Electric Power Industry’s Critical Role in the Economy

During the pandemic response, DOE and DHS have played a crucial role in interfacing with state governments on the importance of allocating PPE and testing capabilities to utility personnel. The ESCC has worked closely with DOE and DHS to ensure that industry workers were represented appropriately in CISA’s *Guidance on Essential Critical Infrastructure Workers*. This guidance, while not a federal standard or directive to states, helps state governments decide which workers should be considered for prioritized PPE and/or provided with unrestricted movement and access to restricted areas.

This guidance also underscores why expediting PPE to critical utility workers is essential. One entity reported that it used the CISA guidance when pitching the need for prioritized testing for utility employees to local government officials. In addition, the Secretary of Energy sent two letters to governors of each state/territory underscoring the important role the electric power industry plays in the economy and disaster recovery.

Despite these helpful efforts, some industry representatives indicated that state and local governments still do not understand fully the critical importance of prioritizing PPE and testing for electric industry workers. In addition, it was reported that some states needed background information on how the sequestration of control center staff would help secure grid operations during the pandemic. Entities that began their outreach early in the pandemic response and focused on local officials had the most success. Based on this, the ESCC should consider developing materials for the subsector to use during “blue sky” days to engage with state and local officials and discuss how the work performed by mission-essential workers in the electric power industry is critical.

Initial Availability of Testing Equipment and Sites Was Limited

Many issues have contributed to the extreme difficulties electric power industry organizations encountered when trying to access adequate testing. One big challenge was state and local governments’ strict interpretation of the now-outdated CDC Priority Testing Guidance established in

March, which did not include prioritization of asymptomatic critical infrastructure workers. As a result, some state governments did not prioritize mission-essential workers for testing.

After outreach by DOE to HHS, a limited number of test kits was provided to some electric utilities. Even when test kits were secured, organizations reported issues finding local laboratories that could process test results easily and efficiently. Many of these organizations reported that they could not find a lab within 150 miles that could process the Abbott Rapid ID NOW Test Kits that were provided by HHS. This left some companies unable to conduct tests.

Going forward, utilities recommend better preparation across the ESCC, U.S. government, and state government partners to address the anticipated demand for testing before there is a backlog. Additionally, the ESCC recommends that the federal government focus on prioritizing testing for community lifeline sectors, such as energy, as established by DHS and FEMA.

The Structure of Initial ESCC Calls with Government Leadership Could Have Been Improved

Some industry leaders have noted that the structure of the early ESCC calls with government leadership could have been improved. Instead of focusing on the pandemic response in some of the hardest-hit areas, such as New York and Washington State, the initial calls included reports from other regions of the country. While those reports were informative, more detailed presentations from the early hotspots in the pandemic would have been more helpful to organizations in other regions preparing for an increase in COVID-19 cases. This observation was noted and addressed by the ESCC co-chairs, and the structure of coordination calls was adjusted.

A Streamlined Federal Government RFI Process Would Be Welcomed by Industry

The industry has received several “Requests for Information” (RFIs) from DOE and DHS with quick turnaround times. While the industry understands that federal agencies need information for situational awareness and to make informed decisions regarding federal resources, the short timelines put unnecessary burdens on the organizations, especially as they are responding to the pandemic. A streamlined RFI process would be welcomed by industry.

IV. TIGER TEAM OPERATIONS

The ESCC Tiger Team created a forum in which utilities, federal representatives, and partner organizations can share practices and guidance, receive information, and coordinate joint response efforts. The regular cadence of Tiger Team calls and the subgroup structure have helped to organize joint efforts among industry organizations responding to COVID-19. The Tiger Team and subgroups are a core component of the industry response to the pandemic and have helped guide the drafting of the ESCC Resource Guide. Among the issues identified, industry representatives highlighted the importance of the Tiger Team in fostering an industry-wide sense of common purpose. A notable area of improvement includes the need to broaden the ESCC’s communication across the electric power industry.

Tiger Team Operations – Accomplishments and Strengths

Diverse Participation from Cross-Sector, Canadian, and Government Partners Strengthens the Work of the Tiger Team

Electric power industry organizations from across the United States, both large and small and of every ownership type, participate in the Tiger Team and subgroups and have shared relevant and critical information on their operations and response to COVID-19. Participation by Canadian partners has been well-received, with Canadian representatives noting that they appreciate the inclusion given that the energy grid inherently is a shared asset between the United States and Canada. Additionally, the American Gas Association (AGA) and American Public Gas Association (APGA) have expressed appreciation for participating in the Tiger Team and subgroups, as natural gas distribution utilities face many of the same issues as electric utilities. Staff from the E-ISAC also play an important role on the Tiger Team and have offered valuable contributions to team documents and materials.

The widespread inclusion of various industries and international partners has enhanced the “unity of effort” and the sense of a shared mission among organizations, helping to underscore that the fight against COVID-19 is a collective effort and that all utilities gain from sharing practices and resources through the collaborative efforts organized by the ESCC.

One utility representative noted that ESCC initiatives are seeing a significant boost in participation from across the industry and from partner industries/trade associations, which is a win for the electric power industry overall. Other representatives have suggested that future participation from additional trade organizations in similar industries would be helpful. In addition, expanding outreach to other sector coordinating councils would be beneficial. For instance, the supply chain subgroup has partnered with the Chemical Sector Coordinating Council on some of its work during the pandemic. Accessing the expertise in those councils could help facilitate the efforts of other subgroups and expand the ESCC outreach to other sectors.

The Use of SharePoint Has Improved Tiger Team and Subgroup Coordination

Several Tiger Team participants noted that the SharePoint file sharing and collaboration tool has improved coordination among team members, and they thanked DOE, the National Energy Technology Laboratory (NETL), and Southern Company for their efforts to establish the platform early in the pandemic response. Throughout the pandemic, utilities have been inundated with information and guidance from a range of U.S. government, ESCC, and related authoritative sources. Industry representatives highlighted the importance of SharePoint as a collaborative tool for information sharing, joint drafting, and consensus building.

Tiger Team Operations – Opportunities for Improvement

Communications Gaps Have Limited Some Information Sharing with External Partners

By and large, the ESCC has been lauded for its information sharing efforts during the COVID-19 pandemic. Information developed by the Tiger Team and subgroups is distributed by multiple organizations, including the various trade associations, the E-ISAC, and DOE. Industry representatives

report receiving an extensive flow of information, which has helped to ensure a common understanding of the operating environment in response to COVID-19.

Some gaps in the ESCC's communications to industry have been noted. While the ESCC succeeded in providing early and detailed information on the pandemic response to industry executives, this information took time to cascade down from the executives of some large organizations to staff at operational levels. Similarly, information on ESCC efforts took time to reach utilities that aren't members of (or don't regularly communicate with) a national trade association, but still would benefit from ESCC information sharing and participation in the Tiger Team or a subgroup.

While the challenges of information silos within organizations are beyond the purview of the ESCC, the Council nevertheless should consider broadening its outreach to the subsector. Working with additional industry organizations could help expand partnerships with asset owners that do not traditionally work with the ESCC, but that have a critical role to play in energy grid security and reliability. As the diversity of participation on the Tiger Team and subgroups is a key positive attribute identified by several representatives, developing a broad communications strategy to accompany future Tiger Team efforts is recommended.

As part of this strategy, the ESCC also should consider other channels, such as FEMA's National Business Operations Center (NBEOC) online portal and the U.S. Chamber of Commerce and its state affiliates, for disseminating ESCC messaging and material broadly.

Internal Tiger Team Communications Could Be Improved

Early communications challenges created some confusion within the Tiger Team regarding the topics, leadership, makeup, and logistics for each of the various subgroups. This left some unaware of the purpose of the Tiger Team and subgroups and how best to become involved in the effort. Electric power industry representatives recommend creating marketing materials in the future that highlight the relevant logistical information. Some pointed to the need for better coordination and collaboration at the point of establishing subgroups and their leadership structures. It also was noted that additional communications among subgroups, such as sharing meeting minutes across groups, would improve Tiger Team coordination.

In addition, some noted a lack of clarity regarding how certain ESCC information could be shared. Organizations distribute ESCC updates within their organizations and with partner utilities that may not have ready access to these materials. However, there are concerns about sharing information too broadly. Organizations would benefit from enhanced guidance on how to share information when it is received, including whether the information is intended for wide distribution among industry partners or to the public.

The Tiger Team Should Consider Creating a Health-Focused Subgroup

The ESCC Tiger Team has addressed key health issues relevant to the industry's COVID-19 response and has sponsored coordination calls with industry and external medical professionals who provided important information on testing experiences and protocols. While those calls were widely attended and were helpful, some utility representatives have noted that an additional health and safety-focused subgroup could be created to expand those calls with the medical sector. This group would track health

and safety information and health guidance coming from the U.S. government and would work to amplify that guidance across the industry to ensure wide dissemination.

As noted, the COVID-19 pandemic unfolded differently than traditional crises, and the U.S. government response continues to evolve over the course of the response operation. This evolution partly is reflected in the guidance given by CDC, HHS, and other public health authorities during the pandemic, which continues to be updated as experts gain more information on the characteristics and spread of the virus. Tracking these changes and checking compliance with new and evolving guidelines has required a herculean effort from organizations. Dedicating a subgroup to serve as a point of contact for this information would centralize the industry's understanding of guidelines as they evolve and would provide electric power industry organizations a forum to consider and to respond to health and safety guidance from the U.S. government.

Subject Matter Expertise/U.S. Government Participation on the Tiger Team Should Be Expanded

With the understanding that U.S. government personnel resources are strained due to COVID-19, industry representatives recommend additional participation from experts on standing calls. Utilities repeatedly emphasized that hearing from DOE, DHS, CDC, and other U.S. government representatives directly, and more quickly, on testing, PPE, and related issues helps organizations manage their response to the pandemic. The ESCC would need to establish a proper cadence for participation and a clear purpose for federal partner involvement and would need to identify appropriate participants for future Tiger Teams.

The ESCC also should consider establishing standing Tiger Teams focused on different areas of a response operation. For instance, as noted, a standing supply chain team of industry and government experts could build “blue sky” relationships with key suppliers and vendors that would benefit the entire subsector during a major incident.

Additional International Engagement Should Be Considered

In the early stages of the pandemic, the Electric Power Research Institute provided helpful insights on how other countries were approaching this health emergency. Given the global implications of a fast-moving pandemic, the ESCC should consider additional outreach and collaboration with international partners. This engagement will facilitate the sharing of leading practices that could inform and improve how we prepare for and respond to future health emergencies.

V. ESCC COVID-19 RESOURCE GUIDE

The ESCC Resource Guide developed by the Tiger Team and subgroups offered a core set of planning considerations to inform the electric power industry's COVID-19 response. With regular updates and additions, the Resource Guide has become a widely used source of information across industries in the United States and around the world. Industry representatives speak highly of the Resource Guide, noting the document's accessibility, detailed sections, and ease of implementation. These same representatives consider the Resource Guide to be a central component of the ESCC's response to COVID-19, and they recommend that it remain a core component, with some additions and updates, of the pandemic response moving forward.

Resource Guide – Accomplishments and Strengths

The Resource Guide Is Comprehensive and Broadly Applicable to the Electric Power Industry's Pandemic Response

The ESCC Resource Guide has been a well-received and widely used tool across the electric power industry and beyond during the COVID-19 pandemic. Organizations note that the Guide stands out among documents provided by trade associations or sector coordinating councils in other industries. It is used by other critical infrastructure sectors in the United States, as well as internationally, to help organizations guide their COVID-19 responses.

Industry representatives appreciate that updates to the Guide reflect new and expanding guidance from U.S. government and health authorities, and they feel that the updates come in a proper cadence, with appropriate markings to reflect these updates. They also note that template documents included in the Guide are helpful and can be incorporated easily into an organization's internal planning materials. The sections on mutual assistance and control center sequestration, in particular, are helpful.

Overall, the Resource Guide demonstrates true industry leadership in thought, clarity of mission, and actions, and it was produced at a speed that enabled it to be used by organizations while they planned and managed their initial responses to the pandemic.

Resource Guide – Opportunities for Improvement

The Guide Could Benefit from Enhanced Marketing and Distribution

Although the Resource Guide is valued by organizations that have learned of its availability, the ESCC could expand its marketing and distribution of the document beyond traditional recipients. As discussed, some utilities are not members of the ESCC or do not participate routinely in trade associations. Many of these utilities were not on the initial distribution list for the Resource Guide.

ESCC participating organizations report that organizations that received the Resource Guide via formal or informal information-sharing between organizations greatly appreciate the information from the ESCC. The Resource Guide has extensive applicability to critical infrastructure in adjacent industries like natural gas. The ESCC is well-served by helping a broader set of asset owners, not just immediate members, respond to the COVID-19 pandemic, as it reinforces the ESCC's role as a leader within the electric power industry and as a trusted partner for emergency response. Exploring other platforms, such as FEMA's NBOEC online portal, would help distribute the document to a broader audience.

Additional Templates and Checklists Could Help Organizations Operationalize the Resource Guide

The checklists/templates included in the Resource Guide are helpful to utilities in implementing the tools and resources contained in the document. A checklist or tear-sheet for each section of the Resource Guide distilling the main points would be useful to many utilities. Hyperlinks within the document also would make it much easier to navigate. Other industry representatives have suggested the use of an online wiki-tool to ensure consistency throughout the document.

Continued Updates to the Resource Guide Should Reflect the Evolving Pandemic and Response Activities

The ESCC Resource Guide is a living document and should serve as the basis for continued updates as the United States continues to respond to the pandemic. Several industry representatives cited the Resource Guide as a jumping off point for additional materials to guide utilities through a resurgence of the virus across the United States. For example, information on the types of external and internal triggers for reentry planning were cited as a welcome addition to the document. The Resource Guide was helpful to utilities during the first wave of the virus. Additional information would help utilities during the ongoing first wave and during any secondary waves of COVID-19, or any future pandemics.

VI. CONCLUSION

The ESCC response to the COVID-19 pandemic is ongoing, as the virus continues to spread around the world and across the United States. As the industry sustains a coordinated response alongside partner organizations and the U.S. government, the ESCC will continue to organize collective efforts, to solicit feedback on ongoing initiatives, and to provide tools and resources through the Resource Guide and other materials. This report serves as an interim review of the current state of the ESCC response to COVID-19 and will help inform ongoing efforts during this pandemic or during a resurgence of the virus or a similar health emergency in the future. Additionally, the report will aid ESCC efforts to maintain situational awareness and response capabilities for all-hazards, whether natural or man-made, which continue to threaten utilities across the country even amid the pandemic.

APPENDIX A: ACTION ITEMS

Based on the feedback provided in this report, the ESCC should consider the following action items to enhance its response to the current pandemic and to future incidents that impact the energy grid:

1. **Develop a Process for Accessing Government PPE Stockpiles:** Coordinate with federal government partners to develop a clearly defined process and timeline for securing and distributing PPE from federal, state, and local stockpiles.
2. **Anticipate and Prioritize Testing:** Coordinate with federal government partners to anticipate and to prioritize pandemic testing for the energy sector.
3. **Facilitate “Blue Sky” Outreach to State and Local Governments on “Mission-Essential Workers”:** Develop materials for the subsector to use during “blue sky” days to engage with state and local officials and discuss how the work performed by mission-essential workers in the electric power industry is critical.
4. **Explore Options for Streamlining Federal RFIs for Industry:** Work with federal government partners to discuss the RFIs submitted to the industry by DOE, DHS, and other federal agencies, and explore ways to combine or streamline those requests.
5. **Expand Cross-Sector and Government Participation in the Tiger Team and Subgroups:** Expand participation of government staff and trade organizations and sector coordinating councils for other partner industries on the Tiger Team and subgroups.
6. **Include Additional Government Experts on Standing ESCC Calls:** Include additional government experts on standing ESCC calls, with the understanding that U.S. government personnel resources are strained during the COVID-19 health emergency.
7. **Expand Communications to Electric Industry and External Stakeholders:** Develop a new procedure for distributing ESCC-branded communication to executives and staff within the electric power industry and to external stakeholders. These communications efforts should include a focus on industry staff who may not be familiar with the ESCC and should provide clear guidance on how to disseminate ESCC-related information within an organization. In addition, the ESCC also should consider other information channels, such as FEMA’s National Business Operations Center online portal and the U.S. Chamber of Commerce and its state affiliates, for broadly distributing ESCC messaging and materials.
8. **Encourage Additional Communication Within the Tiger Team:** Encourage additional communications among subgroups, such as the sharing of meeting minutes across groups, to improve Tiger Team coordination.
9. **Develop Procedure to Form Ad Hoc ESCC Groups:** Use the pandemic response as a model for future ESCC initiatives and develop a procedure to form ad hoc groups within the ESCC to focus on specific issues and deliverables.

- 10. Establish a Standing Industry Supply Chain Team:** Establish a standing supply chain team of industry and government experts to build “blue sky” relationships with key suppliers and vendors that would benefit the entire subsector during a major incident.
- 11. Create a Health- and Safety-Focused Subgroup:** Create an additional subgroup to track and amplify health and safety information and guidance.
- 12. Expand International Collaboration with International Partners:** Expand outreach and collaboration with international partners, given the global implications of a fast-moving pandemic.
- 13. Include Additional Checklists and Templates in the Resource Guide:** Where appropriate, include a checklist and/or tear-sheet for each section of the Resource Guide that summarizes the main planning considerations.

APPENDIX B: TIGER TEAM SUBGROUP LEADERSHIP

Tiger Team Executive Sponsor

Stan Connally
Executive Vice President for Operations
Southern Company Services, Inc.

Control Center Continuity

- **Leads:** Tom O’Brien (PJM); Kevin Howard (WAPA)
- **Secretariat Leads and Support Staff:** Sam Rozenberg (APPA); Hailey Siple (EEI); Nathan Mitchell (APPA)
- **Federal Government Representatives:** Pat Hoffman (DOE); David Howard (DOE); Mike Wech (SWPA); Danny Johnson (SWPA); Lloyd Linke (WAPA); Jonathan Aust (WAPA)

Accessing Quarantined and Restricted Environments

- **Leads:** Kimberly Denbow (AGA); Adrienne Lotto (NYPA)
- **Secretariat Leads and Support Staff:** Pat Hart (EEI); Nathan Mitchell (APPA)
- **Federal Government Representatives:** Sean Plankey (DOE); Stephen Curren (DHS)

Supply Chain Challenges

- **Leads:** Johnny Howze (Southern Co.); Michele Guido (Southern Co.)
- **Secretariat Leads and Support Staff:** Jack Cashin (APPA); Sam Chanoski (E-ISAC)
- **Federal Government Representatives:** Sean Plankey (DOE); Shana Kuhn (BPA); Virgil Hobbs (SEPA)

Mutual Assistance Preparation

- **Leads:** Louis Dabdoub (Entergy); Michael Willetts (Minnesota Municipal Utilities Association); Kenny Roberts (ElectricCities of North Carolina)
- **Secretariat Leads and Support Staff:** Wally Mealiea (EEI); Chris Eisenbrey (EEI); Sam Rozenberg (APPA); Martha Duggan (NRECA)

TLP: GREEN

- **Federal Government Representatives:** Kate Marks (DOE); Ashton Raffety (DOE); Mike Miller (BPA)

Generation Operational Continuity

- **Lead:** Jim Heilbron (Southern Co.)
- **Secretariat Leads and Support Staff:** Sam Rozenberg (APPA); Matt Duncan (E-ISAC)
- **Federal Government Representative:** Danny Johnson (SWPA)

IT and Telecommunications Issues

- **Lead:** Sharla Artz (UTC)
- **Secretariat Leads and Support Staff:** Laura Schepis (EEI); Corry Marshall (APPA); Sam Rozenberg (APPA)
- **Federal Government Representatives:** Chris Alexander (DHS)

Responsible Reentry and Return to the Workplace

- **Leads:** Adrienne Lotto (NYPA); Dave Megna (WEC Energy Group)
- **Secretariat Leads and Support Staff:** Pat Hart (EEI); Sam Rozenberg (APPA); Martha Duggan (NRECA); Matt Duncan (E-ISAC); Hailey Siple (EEI)
- **Federal Government Representatives:** Pat Hoffman (DOE); Megan Tsuyi (DHS); Emily Burdick (DOE); Charles Rousseaux (DOE)

Internal and External Communications

- **Leads and Secretariat Support Staff:** Stephanie Voyda (EEI); Brian Reil (EEI); Tobias Sellier (APPA); Scott Peterson (NRECA); Stephen Bell (NRECA); Sarah Robinson (CEA); Susan Buehler (PJM); Jon Wentzel (NEI); Kimberly Mielcarek (NERC); Christina Nyquist (EPSA)

Power Line-Caused Wildfire Mitigation Annex

Mitigation

After the devastating fires of 2011 and 2012, Texas A&M Engineering Experiment Station (TEES) developed a powerline-monitoring technologies to detect downed powerlines, failing line apparatus, and arcing equipment that can cause fires. Preliminary work has shown that this technology, in concert with Texas A&M Forest Service fire risk predictive models, can prevent many wildfires and provide more timely awareness of fires as they occur, facilitating rapid response. These two Texas owned and developed technologies have the potential to improve public safety, save lives, and significantly reduce wildfire-related property losses.

The Texas legislature has authorized and funded a two-year TEES project to demonstrate the effectiveness of its technology in selected high-risk fire areas. The success of the project will depend upon cooperation from many stakeholders: utility companies, local fire-response teams, and state agencies, including Emergency Management and the Public Utility Commission.

United was invited to participate in this study along with other cooperatives and investor-owned utilities. United board has given the approval to be active in this project which will include acquiring and installing substation hardware for four substation feeders, act as a participating member of the Wildfire Project Advisory Council and work cooperatively with TEES to respond to failure events and evaluate the performance of the equipment that is being tested.

United will use lessons learned from this project along with the associated power line equipment to mitigate the damaging effects of wildfires going forward.

Wildfire Emergency Response

As with weather related emergencies, United's employees should refer to the Disaster Planning Guide for weather related emergencies. Additionally, the System Operators and other key personnel are expected to follow the ERP Considerations Chart and the Definition of Emergency Levels Chart when handling any outage effecting United's Members. These Charts and Definitions are found in the Weather Emergency Annex.

UNITED COOPERATIVE SERVICES
EMERGENCY RESPONSE PLAN/EMERGENCY OPERATIONS PLAN
Version 1.2023

Pages 334 through 355 redacted due to confidentiality

UCS Security Guidelines

Table of Contents

Confidentiality Notice.....	1
Table of Contents.....	2
Purpose.....	3
Roles and Responsibilities	3
Physical Security.....	4
Cyber Security	7
Incidents/Response	20
Training/Personnel Issues	21
Security Incident Form	22

Purpose

UCS needs established guidelines for security to detail procedures, requirements, etc. These guidelines shall include roles and responsibilities, physical security, cyber security, responses to incidents, and training requirements. It is feasible that new threats will be developed after the initial release of these guidelines; therefore, they must continually be updated at least on an annual basis. It is also the intent of these guidelines to conform to the industry requirements including NERC, RUS, and PCI requirements as they apply to electric cooperative distribution systems. These guidelines are established for the purposes of meeting the requirements of UCS Policy 3475.

Roles and Responsibilities

UCS Security Committee: This committee is established to review and/or recommend new or changes to any guidelines as well as implement such for UCS security. Further, this committee shall work together in evaluation of any security incidents that occur. The committee shall include:

- Robert Bernhoft – Chairman – VP of IS&T
- Cameron Smallwood – CEO
- Marty Haught – Assistant General Manager/COO
- Russell Young – VP of Accounting and Finance
- Jared Wennermark – VP of Planning and Procurement
- Landy Bennett – Senior VP of Member Services and Marketing
- Mike Huston – Facilities/Print Shop Director
- Kevin Keesee – Director of Human Resources
- David Stone - JTS/Loss Control Director
- Mark Dixon - Field Safety Coordinator
- Eric Cagle – IS&T Administrator
- Brad Mead – IS&T Administrator
- John Huffman – IS&T Administrator
- Yuri Lavadour – IS&T Administrator
- Robert Sherman - Senior Manager of Procurement/Facilities

The VP of IS&T shall lead the UCS Security Committee, in coordination with the CEO and the Assistant General Manager/COO, to implement all the guidelines contained in this document. In the event that the VP of IS&T is not able to perform such duties for whatever reason, the Assistant General Manager/COO shall either perform the duties or appoint another individual from the committee to do so.

It is the responsibility of each employee at UCS to follow all security guidelines as presented.

Physical Security

The physical security portion of these guidelines includes access control procedures, key and access code procedures, general office facility security, physical media security, monetary access, vehicles and uniforms.

Access Control Procedures

All UCS building exterior doors shall be locked when not in use. All exterior doors shall be locked outside of business hours. Any lost keys should be reported to HR as soon as possible. Any lost key fobs should be reported to IS&T as soon as possible. In the event of the Community Rooms at any office being utilized, the interior door(s) with access to the other parts of the building shall be locked anytime possible in order to limit traffic between the Community Room and the office environment.

Computer, power, and telecom equipment rooms shall be keyed with a special limited access key. A key log shall be maintained by Human Resources. Any lost keys should be reported to HR as soon as possible. Limited access means not only that select UCS employees have keys to these rooms but also that those who have access are to be responsible in limiting access by others. The limited access area doors should be closed and locked when leaving the area--even if for only a moment. If any employee sees a limited access door standing open and no one is visibly working in that room they should close the door and report it through a security incident report. Limited access rooms are not only limited for security reasons but also for safety and liability concerns. These rooms all have trip hazards, high voltage switch panels and high voltage equipment in them.

Outside of the office, any UCS facilities that have control ability of the distribution line shall be locked with the standard UCS brass-style lock. The Senior Manager Procurement/Facilities shall assign keys based on Key Authorization Guidelines. Any lost keys should be reported to the Senior Manager Procurement/Facilities as soon as possible. UCS employees shall not lend keys out to any unauthorized individuals without prior authorization of the Senior Manager Procurement/Facilities. Employees that work with Contractors and have keys issued for Contractor's ability to perform work are responsible to collect issued keys at the completion of the work.

A separate lock shall be used on gates for UCS access where gates are not electronically/mechanically secured. The Senior Manager Procurement/Facilities shall assign keys based on Key Authorization Guidelines. Any lost keys should be reported to the Senior Manager Procurement/Facilities as soon as possible.

When visitors come to the cooperative for a meeting (not including membership for customer service purposes), it is best practice for the employee that accepts the visitor to go to the lobby area and escort the visitor to the location of the meeting. After the meeting is complete, the employee should escort their visitor back to the lobby.

When no employees are staffing an equipment/material yard, gates should be closed and locked.

Key and Access Code Procedures

As a general rule, an employee should only have access to facilities which are deemed as “Necessary work areas” for that particular employee. This general rule will help in limiting the access to the facility to only employees who directly need the access. Necessary work areas are further defined below.

Keys, key fobs and access codes for the security system should be restricted to the following personnel as it pertains to the following:

Office Buildings – All office personnel should have a key fob and security code to their designated office building. Offices are also considered necessary work areas as it pertains to warehousemen and line foremen if their office is attached to their office complex. Facilities, IS&T and technical services personnel should have access to all offices that they are required to work in. Other line personnel should be considered on a case by case basis depending on their job duties.

Yards – All warehousemen, facilities, and line personnel should have a key, electronic code, or remote opener in a co-op vehicle to open the yard gate. All gates should be keyed alike so that gates can be opened by any of the above personnel in case of outages or emergencies. Gate keys should be attached to pool car key rings to allow for before or after hours vehicle pick up. All staff should have keys to gates.

Warehouse buildings – All warehouse and line personnel should have keys to designated warehouse facilities. All staff should have a warehouse building key.

Communications/Power Supply/Computer Area – Technical service, IS&T and facilities personnel should be the only employees to have key access to these areas because of their critical nature. Any request for keys to these areas should be made to the VP of IS&T.

A key log should be maintained for each office, warehouse and yard by facilities/warehouse personnel. A key fob log will be maintained in the software that controls key fob system. A security code log should also be maintained for each office.

General Office Facility Security

All offices shall have locking exterior doors that shall remain locked from the exterior during non-business hours. This shall be the same for all yard gates.

Any office not manned 24 hours a day should have a security system that is remotely monitored when armed. The system shall become active and armed outside of business hours. Only an approved listing of employees shall be allowed access to arm/disarm the system. In the case that an event occurs, JT&S/Loss control personnel should respond if contacted and report such event

to the UCS Security Committee using the appropriate form found at the end of this document labeled "Security Incident Report."

When an employee is terminated or resigns, HR and the Senior Manager Procurement/Facilities shall ensure that all keys and key fobs that were assigned to that employee are collected. Further, if applicable, their passcode on any office security system shall be disabled and programmable door lock/gate codes shall be changed.

Remote door locks, key/FOB systems and video monitoring may be implemented in offices or on UCS property on a case-by-case basis to improve security.

Physical Media Security

UCS has items of proprietary and confidential nature that are stored in paper form and on computer media such as removable disks, USB memory devices, hard drives, backup tapes, etc. All media with such data should be secured on encrypted drives when possible.

Encryption software shall be utilized on all laptops and desktops with potentially sensitive data.

UCS mobile devices guidelines should be signed by all employees with such a device.

Backup tapes, program media, etc. should be kept in the fire proof safe in the appropriate office and all IS&T backup procedures/guidelines shall be followed.

When computers are no longer needed by UCS, the hard drives shall be fully and completely destroyed either physically or with software applications.

When backup media is no longer needed, it shall be destroyed, not simply thrown in the trash.

Monetary Access

UCS has cash drawers for taking cash payments and petty cash drawers for minor reimbursements among other things. Payment cash drawers shall be stored in locked and secured areas when not in use. During office hours, the cash drawer shall stay closed when not in use. All procedures/guidelines for handling the cash drawer established by accounting/member services shall be followed. Petty cash drawers shall have limited access and shall be locked and secured at all times when not in use.

Vehicles

Company vehicles shall be locked when not in use. Keys for vehicles or other company assets should not be kept inside the company vehicle. Tool bins, material bins, etc. on all vehicles shall be locked when the vehicle is not occupied where applicable. Items of worth should not be left in the bed of the truck or stored inside the vehicle when possible, but when such is required, these items should be removed from easy viewing from the outside.

When UCS vehicles are parked at cooperative offices outside of business hours, they should be parked in the gated/secured area.

Cooperative Uniforms

UCS provides certain employees with logo uniforms. When these are replaced, all old uniforms should be returned to HR for proper disposal. UCS Uniform Policy 3230 shall be followed.

Cooperative Records

UCS collects certain information for membership and employment purposes. Membership information collection and storage of such records are governed by UCS Policy 4120, Privacy and Confidentiality of Member Personal Information. As far as employment related records, similar care should be taken to protect the confidentiality of personal and Protected Health Information. Written/printed personnel and health records shall be locked in a location accessible only to Human Resources and other authorized employees. Employee personnel files are stored electronically and can only be accessed by Human Resources based on their iXp login credentials.

Handling of Credit Card Information

Due to credit card security requirements, the following recommendations shall be followed by all employees handling member credit card information:

1. Credit Card #s must **not** be emailed. (Email is not a secured method of sending this information).
2. Anytime an employee writes down a credit card # (for any reason), that paper must be shredded before thrown away.
3. Any written document that contains full credit card information must **not** be saved to the employee's computer (unless full disk encryption has been installed on the computer). If the document is faxed to a bank, the original must be shredded after it is faxed.
4. Credit card receipts from the swipe machines that contain the full credit card number must be stored in a safe area (preferably the vault) and need to be shredded in accordance with record retention policy.

Cyber Security

The cyber security portion of these guidelines includes password guidelines, levels of security evaluating risks/threats versus response, network setup, anti-virus, anti-spam, anti-spyware and IPS signature requirements, PC security, and application development and deployment.

Each user of network resources at UCS should have their own unique username. In other words, there should be no group, shared, or generic accounts in use by more than one employee.

Policy 3470

Employees should follow UCS Policy 3470 located in UCS Employee Policy Manual.

Password Guidelines

The following is a listing of the password rules for the UCS network:

1. Passwords will be synchronized between PCs, servers, AS400, iXp, and MyAccount.
2. All passwords are required to be changed every 3 months on all systems and users will be forced to do this.
3. All passwords may be required to be changed at other times depending on risk level.
4. Passwords should not be shared with others (except for IS&T employees).
5. Passwords cannot be the same as the user name.
6. All passwords have to be at least 8 digits/characters/special characters long and no longer than 10.
7. All passwords must start with a letter.
8. All passwords must have at least one numeric character/digit.
9. No written notes detailing password can be located in computer space visible from the general work area.
10. Vendors that need access will have accounts and passwords that must follow the rules above with restrictive profiles and access. Further, these accounts shall be disabled when not in use.
11. Employees that are terminated or terminate employment will have all access disabled on their last day of employment.
12. Specialized user names and passwords for network, server administration, etc. should be kept in a special restricted location allowing IS&T personnel access to those user names and passwords for support reasons.
13. Default passwords for systems should be changed prior to being placed into production.

If you suspect an account or password has been compromised, change the password immediately and then report the incident to your supervisor and/or IS&T staff.

It may become necessary for the IS&T Department at UCS to change passwords in the network due to an outside threat.

Some of these threats are as follows:

1. An employee with knowledge of our network resigns or is terminated
2. A known threat is imminent
3. It has been discovered that the network has already been compromised

Employees of the IS&T department are the only employees that should be able to change security related items on the network. The following is a list of passwords that need to be changed if one of the above threats should appear.

1. Network Domain Administrator password
2. Passwords for all routers, switches, and firewalls

The IS&T Administrators will determine what the new passwords will be. Once the new passwords are determined, they will be handed out to all of the IS&T department employees. A document with all of the network and router passwords will be kept by all employees of the IS&T department. This document will be kept secure while in each of the employee's possession. The passwords will be kept as a document only and will not reside on any user's PC or on any server. This will decrease the chance of someone hacking into a PC or server and obtaining all of the passwords.

Levels of Security

Different threats and risks exist relating to security of cyber systems in the categories as defined. Further, industry and national threats may exist that affect our threat/risk level locally, such as possible terrorist activity. Some members may pose a threat/risk level increase when they enter into our offices. Unhappy employees can increase the threat/risk level. Due to many implications, it is necessary to define threat/risk levels and the action that should be taken depending on the risk/threat level. Assessing and thus changing the threat level can be done by the VP of IS&T in coordination with the Executive staff after review of data provided by the Security Committee or other employee resources. Possible threat/risk levels are below.

1. Routine Risk – defined by normal operations with no known or probable threat to security
 - Normal physical access procedures in place
 - Standard firewall in place with standard intrusion detection
 - Normal virus updating
 - Normal password procedures
 - Normal PC/Network/Internet use available to employees
2. Elevated Risk – defined by termination of employee or completion of network usage by associate outside of Co-op
 - Normal physical access procedures in place
 - Standard firewall in place with standard intrusion detection
 - Normal virus updating
 - Change of select passwords
 - Disabling/deletion of select network accounts
 - Normal PC/Network/Internet use available to employees
3. Probable Risk – defined by disgruntled employee or member or detection of probable attacks to internal servers or network
 - Key areas in United offices will be locked/secured
 - Firewall intrusion detection will be analyzed and unnecessary connections to the internet will be terminated
 - Manual virus updates will be performed to ensure current definitions

- Change of select passwords
 - Disabling/deletion of select network accounts
 - Limited use of PC/Network/Internet by employees
4. Extreme Risk – defined by severe circumstances with employee or key personnel, a terrorist action, or confirmed detection of intrusion to servers or network
- Key areas in United offices will be locked/secured
 - Access to internet will be denied
 - Network resources will be disabled to isolate risk(s)
 - All users will change passwords per password policy
 - Disabling/deletion of select network accounts
 - Limited use of PC/Server by employees

Network Setup

All network links shall be physically secure and shall be password protected via the password guidelines. Backups of configurations of all routers should be kept in a secure location accessible only to employees with such responsibilities.

All documents stored and available on network resources shall have user limitations. Shares should only be used when necessary and when implemented, should only include an approved list of users depending on the share that is set up. No shares should be setup with the ‘everyone’ group with access.

The network setup shall include an IPS external sensor, firewall, DMZ zone, and IPS internal sensor. Fully trusted components can exist directly on the network while partially trusted components or components regularly visited from the internet (i.e. web services) shall be located on the DMZ zone off the firewall. Logs shall be kept for all IPS events, firewall events and configuration changes. Firewall and switch rule sets should be reviewed at least every six months. Switches shall be used anytime network components require multiple connection points (no hubs allowed on core network). A network diagram is shown below.

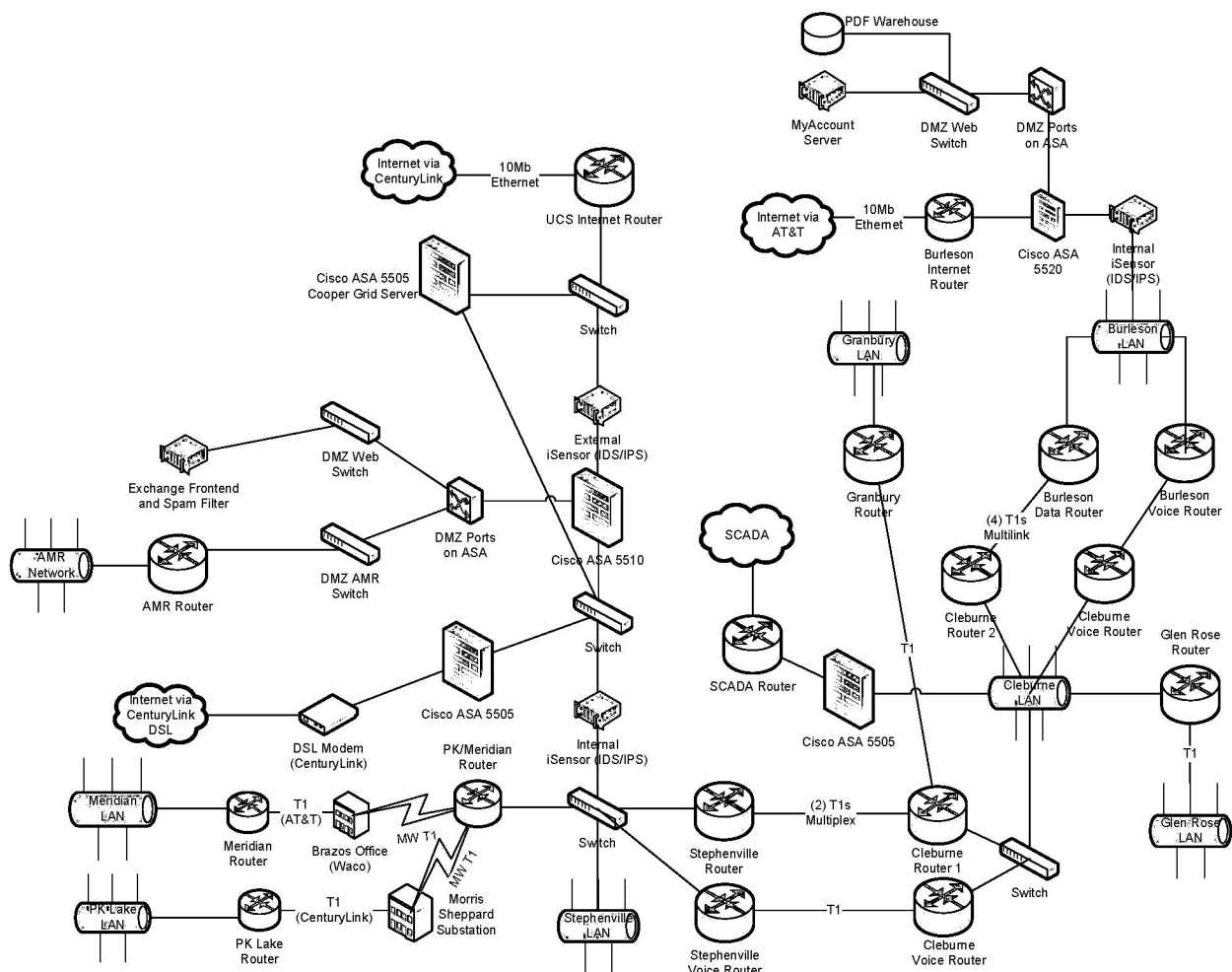
Ingress and egress filtering should be installed on all border routers or Internet Security Gateways. There shall be no public IP addresses located inside the secured portion of the UCS network. NAT (network address translation) shall be utilized when there is a requirement for such a connection.

Minor variations in network setup will be required as new systems are developed, purchased, and integrated. It is a requirement for IS&T personnel to get network improvements and changes pre-approved by the VP of IS&T using the Change Request Form located on the Intranet under the IS&T Menu. These changes to the network should be reflected in a network diagram that is updated and reviewed as changes are made.

Any remote connection to the core network, including connections from cooperative issued devices, must occur via secure and encrypted VPN. All VPN connections will require a 2-factor

form of authentication in order to establish the connection. For security reasons, dial-up connections to the core network will not be allowed.

VPN connections via the internet from employees working outside of the office LAN are allowed but must be secured via encrypted VPN and 2-factor authentication. Employees requiring VPN capabilities will be approved and configured by the IS&T staff.



Anti-Virus, Anti-Spam, Anti-Spyware, Anti-Malware and Intrusion Prevention

An anti-virus system shall be in place and receive regular signature updates. The program shall be loaded on all company-owned computers and shall be set to perform file and email scanning.

All employees should observe the following to help prevent viruses on the network:

- Never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.

- Delete spam, chain, and other junk email without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is a business requirement to do so.
- Always scan a CD, DVD or flash drive from an unknown source for viruses before using it.
- Employees are forbidden from using a computer that does not have updated anti-virus software installed.
- Employees are forbidden from disabling anti-virus software in any way.

An anti-spam system shall be in place and receive regular signature updates. The program shall integrate with the company's mail services and should limit SPAM entry into the service.

An anti-spyware/anti-Malware systems shall be in place and receive regular updates. The programs shall keep spyware and other mal-ware programs from loading from visits to the internet or emails with attachments.

An intrusion detection and prevention system (IDS/IPS) shall be installed at each cooperative location with direct internet access. The IDS/IPS system will receive regular updates and be monitored 24 hours per day with alerts to be sent to designated IS&T staff. The systems shall filter questionable traffic out of the network and monitor internet connections thereby further enhancing system security.

A firewall shall be installed and configured to restrict traffic at each network location that connects to an untrusted network, such as SCADA, AMR, ISP network, public internet, etc. The firewall will be maintained and any changes approved/performed by IS&T staff. For locations that utilize the firewall as a VPN gateway, an IDS/IPS device will reside on both sides of the firewall.

Wireless Network

For all wireless hardware and software, the password shall be changed from the original vendor default password to a strong password in accordance with the company's requirements for administrative passwords.

Wireless routers/access points shall use WPA2 level encryption or higher.

The office wireless network name (SSID) shall not be broadcast.

Guest wireless network traffic shall be limited to internet access which includes the ability to send and receive emails from the UCS email server.

Wireless routers and access points must be secured so that they are accessible only to authorized individuals.

Simple Network Management Protocol (SNMP) community strings shall be changed on all wireless devices.

A wireless network scan shall be routinely performed to detect unauthorized wireless devices.

Acceptable Use of Network and Attached Devices/Software

Improper use of the Internet and our computers can expose the UCS to unwanted traffic and attacks.

All employees and third party users are expected to exercise good judgment to protect themselves and the company from undesirable activity.

- Only authorized employees may use credit card processing software or systems.
- The following cardholder information related activities are strictly prohibited, with no exceptions:
 - Storage of credit card account numbers (PAN's) on local computers under ANY circumstances.
 - Credit card terminals are to be used for processing sales and credits for cooperative business only.
 - Never process a transaction for another business for any reason.
 - You must be authorized by management to use the terminals and settle transactions.
 - Copying/Pasting cardholder data in Windows via the Windows Clipboard.
 - Sending unencrypted cardholder data in email or other forms of communication such as instant messaging.
- Never reveal the password for a workstation, server, or network device to others.
- Never attempt to circumvent user authentication for security of any host, network or account.
- Never provide detailed information about the network or workstations to an outside party.

Change Management

The UCS Security Committee will act as the Change Management Committee (CMC) when required. The CMC shall review system configurations at least annually to assess data risk.

The CMC shall review configurations:

- Prior to deployment of hardware, operating systems, services and applications that could impact business functions.
- Prior to deployment of new computer code.
- Of back-out plans in the event of implementation failure.
- To ensure system configurations conform to all policy requirements.

The VP of IS&T will be responsible for overseeing and approving changes to router and firewall configurations prior to these changes being made. Changes shall be tested prior to deployment whenever possible. There should always be a plan to roll back changes in the event the changes are not completely successful. A full Change Management Process can be found filed with the Processes filed with the Process Committee.

Groups, Roles and Responsibilities

Members of the IS&T department will have administrative rights to network resources. All other users will be assigned standard user privileges with exceptions reviewed on a case-by-case basis and monitored by IS&T personnel.

Vendors and Contracts

Systems and equipment deployed by a third party must be PCI compliant. This should be documented in any contracts with the third party. Departments or persons that engage contractors are responsible for third party compliance with this policy. External vendors shall be required to comply with the portions of the PCI DSS that apply to them. Contracts shall allow the United to verify that the vendor is compliant with the PCI DSS.

PC/Server Requirements

When not in use, PC's and servers should be locked so unauthorized users cannot gain access to files on the computer. Further, the screen-saver password should be set to lock the computer after a minimum of 10 minutes of non-use. If support or use reasons require this feature to be disabled, it should be re-enabled when the function has completed.

Depending on nature of data stored at the PC level, the PC and any components that store sensitive data may be required to be encrypted and password protected. This will be reviewed on a case by case basis as necessary.

Unnecessary services shall not be running on any PC or Server.

Secure and encrypted communications shall be required for any remote administration of PC's or servers on the UCS network.

Users shall be careful not to download non-approved programs from other sources due to the fact many are malicious and could threaten the security of the network.

A network time server shall update and synchronize all time clocks on network devices such as servers, PC's and routers.

Computers that store credit card data must be kept in a locked room or cabinet.

Visitor access, including contractors, must be controlled when working in the area of computers that store or process cardholder data.

- Visitor access shall be assigned by authorized personnel.
- Visitors will be required to display badges.
- Visitor access should be logged.
- Any network access will be revoked for the visitor upon completion of the project.

Computers shall be inventoried, and in some cases labeled.

It is required that all servers have installed the latest recommended security patches and updates within one month of release by the vendor. There should be a process in place to stay current on patches and hot fixes, such as auto update.

Remote administration of workstations and servers must be performed over secure channels.

Software

New software shall be tested for security vulnerabilities prior to deployment.

No software shall be deployed without approval by management or IS&T.

There shall be only one primary function per server. If virtualization is used there shall be only one primary function per system.

Only necessary services, protocols, daemons, etc. directly necessary for the function of the system may be enabled. All unnecessary services, protocols, daemons, etc. shall be disabled.

Insecure services, protocols, daemons, etc. shall be justified and documented security features shall be implemented (SSH, SSL, IpSec VPN, etc.).

Common system security parameter settings shall be set appropriately.

All unnecessary functions – such as scripts, drivers, features, subsystems, file systems and unnecessary web servers shall be removed.

Access Controls and Logs

Access to system components and cardholder data shall be limited to only those individuals whose jobs require such access.

Access rights for privileged user IDs shall be restricted to least privileges necessary to perform job responsibilities.

Privileges assigned to individuals shall be based on job classification and function (also called “role-based access control” or RBAC). Access levels for each system are defined and limited for individual job codes. These are reviewed annually by the VP of IS&T and VP of Accounting and Finance. Any deviations from the predefined access levels must be requested in writing or email to the VP of IS&T from the supervisor of the employee.

Access to shared network folders must be requested in writing or email by the employee’s supervisor. The requesting supervisor must have access authority to the shared network folder in order to request access for their employee.

An access control system shall be in place for systems with multiple users to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed.

A process shall be in place to link all access to system components (especially access done with administrative privileges) to each individual user.

Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) shall be offloaded or copied onto a secure, centralized log server or media on the internal LAN.

Application Development and Deployment

Any application introduced into the network should be reviewed by technical staff to ensure no security enhancements are required in the implementation of the new application. When possible, vendors should be held responsible for application security and the impacts to the company by contract.

In-house applications shall be developed with security measures in mind.

Web-Access by Members

Web access for review of billing data and payment processing must be done via SSL technology. All members with web access to data are required to have a unique user id and password in order to access data.

Vulnerability Scanning

Scanning shall be performed on a timely basis, as indicated in this section, and after any significant system change, including operating system upgrades, infrastructure, software architecture (e.g. adding a sub-net), web server additions, firewall changes, router changes, etc.

A PCI (payment card industry) certified scanning company should be hired to perform a certified vulnerability scan quarterly to verify no vulnerabilities exist within the network setup from the internet that could be exploited by individuals outside of the network.

Internal penetration and vulnerability testing shall be performed quarterly by a qualified individual or vendor.

External penetration and vulnerability testing shall be performed annually by a qualified individual or vendor.

For both types of scans, vulnerabilities scoring 4.0 or above on the Common Vulnerability Scoring system (CVSS), found at <http://nvd.nist.gov/cvss> shall be resolved. Rescans shall be performed until a report can be generated documenting the successful results of the scan.

Reports of network scans should be retained as evidence of meeting these requirements.

System Backups

Server backups and desktop-laptop backups are performed on a regular basis. Server backups are performed according to a schedule and desktop-laptop backups are performed as files change locally and to the server for redundancy. In four major offices, Burleson, Cleburne, Stephenville, and Granbury, we use designated servers for server backups and desktop-laptop backups. Offsite backups are to be performed according to the schedule and locations requirements. For specific configurations and other information, please refer to the UCS - Symantec Backup Exec 2012 Informative Guide document.

Only authorized personnel should move or transport media that contains cardholder data from a secured location. Logs should be kept of any movement.

Credit Card Data Security

Security Codes

- Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be stored – EVEN IF ENCRYPTED. This number is found printed on the signature block of the card on MasterCard, Visa and Discover or printed on the front of American Express cards.
- Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered into a terminal or computer where it is erased after authorization.

Cardholder Information

- Cardholder information data shall be stored on network file servers only in accordance with the Encryption Policy. No storage on workstations, laptops or personal computers is permitted, even for brief periods of time.
- Under no circumstances are the full contents of the magnetic stripe to be recorded or stored.
- The cardholder information that may be obtained from the magnetic stripe is limited to card number, expiration date and card holder name and this data shall be encrypted when stored.
- Cardholder information is to be encrypted or truncated to the last four digits at all times when stored.
- When data is displayed in reports or on user screens the cardholder numbers shall be masked so that a maximum of the last four (4) digits of the number are printed of displayed.
- When credit card data is sent over public networks, such as the Internet, it must be encrypted.
- Access control to cardholder information data shall be on a strict need-to-know basis only. All other traffic is to be denied unless specifically authorized.

Data Backup

- Any backup media shall be securely stored and transported.
- Back up media may be reused by overwriting the prior back up.

- When no longer needed back up data shall be destroyed by degaussing or the media itself shall be shredded.

Paper Record Storage

- Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be written down or collected on paper. This number is found printed on the signature block of the card on MasterCard, Visa and Discover or printed on the front of American Express cards. Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered into a terminal or computer where it is erased after authorization.
- Paper records of credit card account numbers (cardholder information) shall be stored in locked files when not in use.
- Cardholder information data shall not be left unattended when in use. Employees who must leave the work area while cardholder information records are outside of the locked file shall secure them in a drawer, a locked room or return them to the file.
- If Cardholder information is part of a data entry or order form they may be destroyed by shredding after data entry and verification.
- Cardholder information received by fax shall be subject to the following:
 - The fax machine shall be secured or attended while receiving cardholder information.
 - Faxes shall be treated the same as paper records.
- Destruction of paper records shall be performed securely by either an employee or a secure destruction service.
- Destruction must be through shredding, incinerating or pulping.

Employees

- Each employee who handles or uses credit card information or cardholder information data shall be screened appropriately (background check) before being granted access to this data.

Encryption

- Cardholder information data is to be encrypted at all times when stored. When data is displayed in reports or on user screens the card number shall be masked so that only the last four (4) digits of the number are printed or displayed.
- Proven, standard algorithms should be used as the basis for encryption technologies of credit card data.
- Symmetric cryptosystem key lengths must be at least 128 bits.

Access to Cardholder Data

- Access to databases and/or files containing cardholder data, including access by applications, administrators and users shall be authenticated.
- User access, queries, and actions such as add, delete, move, etc. shall be done via stored procedures or other programmatic methods. Therefore, no direct user access to databases.
- Direct access shall be limited to administrators only.

- Application IDs with database access shall only be used by applications and not individual users.

Incidents and Response

The UCS Security Committee shall evaluate any security breach that occurs. A Security Incident Form shall be filled out by appropriate personnel and submitted to the Director of Human Resources which will disseminate the incident information to the rest of the Security Committee. The Director of Human Resources shall also keep a Security Incident File with all occurrences. The file shall be accessible by members of the UCS Security Committee as necessary.

It is the Security Committee's responsibility to work together to evaluate each incident and discuss how the incident could have been prevented. Further, procedures/guidelines should be created or where existing modified to lessen the risk of the same event occurring again. The Security Incident Form shall be available to all employees via the company intranet site for submission to the Security Committee.

In the case where an employee is involved in the security breach, the VP and/or supervisor of that employee's department may be included in the Security Committee for the duration of discussion of the breach.

In the event of a server or workstation related breach, take immediate action as follows:

- Remove the affected computer from the network by disconnecting its cable.
- Do not turn the machine off, log on to it or modify it in any way.
- Notify the Incident Response Team.
- Identify the path of the breach and block it, if possible.
- Preserve all logs and data.

In the case where a security breach occurs, the affected parties should be notified within a reasonable timeframe.

Incident Response Team actions:

- Determine the extent of the breach.
- Notify executive management.
- Make required notifications according to local, state and federal laws and your merchant services contract.
- Determine if severity justifies notifying the merchant bank; and, if so, merchant bank must be notified within 24 hours.
- Follow all instructions received from merchant bank without delay.

A review of incidents and tests is to be conducted to identify any possible improvement opportunities to this plan.

The Security Incident Form is attached at the end of this document.

Training/Personnel Issues

All company employees shall be trained on UCS Security Guidelines each year. At the end of such training, they shall sign that they have attended and understand the guidelines as presented. This can be accomplished via a class sign-up sheet for all attendees. It is the responsibility of each employee to follow the security guidelines as presented each year. Further, it is the responsibility of each employee to ask any questions on situations not covered in these guidelines.

Certain employees fall under requirements to have criminal background checks performed/verified annually. These employees will be required to sign a release to allow the background check to be performed. The Director of Human Resources shall run this check annually and should report to the Executive Management any information that shows the company might be at risk by employing a certain individual. The Executive Management will make an employment decision based on factual information after reviewing the data from HR and speaking with the employee about the questionable history.

A security awareness program including information on handling credit cards and credit card information must be conducted annually for all employees and third party system users.

United Cooperative Services

Security Incident Form

Current Date: _____

Name of Employee Reporting Incident: _____

Office Location: _____

Date(s) of Incident: _____ Time(s): _____

Circle Type of Incident: Physical or Cyber

Description of Incident:

Recommendation to Security Committee (if any):

Signature: _____

Please turn this completed form in to the Director of Human Resources and the incident information will be promptly forwarded to the UCS Security Committee for review and remediation if necessary.

Emergency Response Plan Active Shooter Training

In 2018, United's employee group was provided with Active Shooter Awareness training. As a part of the training, information from the State of Texas and The U.S. Department of Homeland Security was shared with the employees. Information from the training, as well as other pertinent information can be located at:

- <https://www.youtube.com/watch?reload=9&v=pY-CSX4NPtg>
- <https://www.youtube.com/watch?v=j0lt68YxLQQ>
- <https://www.dhs.gov/active-shooter-workshop-participant>
 - <https://www.dhs.gov/sites/default/files/publications/active-shooter-how-to-respond-2017-508.pdf>
 - <https://www.dhs.gov/sites/default/files/publications/active-shooter-pamphlet-2017-508.pdf>
- <https://www.youtube.com/watch?v=tLbhurhAYzs>

Emergency response plan considerations

These guidelines have been developed to grade the outage severity level to determine staffing, outage time expectations, internal communications and member communications.

These guidelines do not take into account all variables, circumstances, and emergencies which may dictate other actions.

Note: outages involve many dynamics that must be working in tandem for outages to be handled perfectly including:

- | | | | |
|-----------------------|----------------------------------|-----------------------------|---------------------|
| (1) SCADA | (5) Inbound Communication Volume | (9) Member Communication | (13) AML system |
| (2) Telephone Systems | (6) Outage Management System | (10) G&T Communication | (14) AVL/Crew Mgmt. |
| (3) IVR system | (7) Crew/Staffing availability | (11) Substation status | |
| (4) Radio System | (8) Radio Communication | (12) Equipment availability | |

Conditions	Level 1 Outage	Level 2 Outage	Level 3 Outage	Level 4 Outage	Level 5 Outage
Main cause of outage?	Various reasons for outage	Various reasons for outage	Storms	Major Storms / Accidents	Major Storms / Accidents
Expected frequency of occurrence?	Daily possibility	Sporadic	15 times per year	Several years apart	Several years apart
How many crews are out on site calls?	3 crews or less	Enough crews for timely work	More site calls than crews	More site calls than crews	More site calls than crews
How many site calls?	Enough crews for timely work	< 10 outages per office/< 20 for multiple offices	> 10 outages per office/< 20 for multiple offices	> 10 outages per office/> 20 for multiple offices	> 30 outages per office
Possible outage time with sectionalizing capability?	2 hours	4 hours	> 4 hours	> 12 hours	Multiple days
Actions	Level 1 Outage	Level 2 Outage	Level 3 Outage	Level 4 Outage	Level 5 Outage
Are additional Sys Operators needed?	No additional Sys Operators	More than 3 crews = additional	Yes	Yes	Yes
Notify Engineering Services for support?	No unless there are software issues	No unless there are software issues	Yes	Yes	Yes
Request MSRs to handle unresolved calls?	No, unless extreme call volume	No, unless extreme call volume	Yes	Yes	Yes
Does the staff need to be notified?	No, unless unusual circumstances	No, unless unusual circumstances	Yes	Yes-Emergency action plan?	Yes-Emergency action plan enacted
Notify Communications Dept. for press release?	Not normally	Possibility, dependent upon # of Priority accts affected	Yes	Yes	Yes
Priority accounts contacted by phone?	Yes	Yes	Yes	Yes	Yes
Priority accounts which cannot be contacted by phone?	Sys Ops first available crew to priority account	Sys Ops first available crew to priority account	Sys Ops first available crew to priority account	Sys Ops first available crew to priority account	Sys Ops first available crew to priority account
Use the High Call or Low Call Volume IVR Script?	Low	Low	High	High	High
ETOR applied?	Yes	Yes	No	No	No
Other	Planned may be postponed	Postpone planned outages	Postpone planned outages	Postpone planned outages	Postpone planned outages
Damage assessment				Yes?	Yes - Damage assessment enacted
Staff and Leadership Team - TEAMS Meeting Initiated?				Yes - Initial Meeting with possible bi-hourly updates	Yes - Initial Meeting with probable bi-hourly updates
Need for Mutual Aid Evaluated?				Yes?	Yes

***Communication - Expectations**

Notification of Engineering Services will be the responsibility of System Operations

Notification of Member Services Department will be the responsibility of Engineering Services

Notification of Staff, Communications and MSRs will be the responsibility of System Operations

Business Continuity

The Business Continuity addendum must address the basics of what shall receive priority attention by the personnel of the cooperative during any emergency situation. The Executive Staff and Leadership team shall review each of these items immediately prior to or immediately following an emergency situation.

Employees

UCS must have employee resources in order to serve the membership during the emergency situation. Without employees, the cooperative will not be able to meet the needs of the membership.

Availability of the employees must be addressed. Executive management, or the Leadership Team in their absence, should perform a thorough availability analysis of all personnel in the first emergency meeting. Any deficiencies should be discussed at that time, and solutions developed during that time where shortfalls exist. Employees within the cooperative may be asked to perform duties outside of their normal job description to fill the most pressing needs of the emergency situation. Further, mutual aid agreements should be acted upon through Texas Electric Cooperatives employee Martin Bevins **(Vice President, Communications and Member Services) (Contact Info - Phone: 512-486-6249 e-mail: mbevins@texas-ec.org)**. Contractor use should also be considered as an option for pressing needs.

Accounting shall ensure salaries are continually paid throughout the emergency situation to maintain income stability for employees and their families during the emergency timeframe. In the event that the Daffron iXp and MyAccount servers fail or are destroyed, United will utilize Daffron's Disaster Recovery services as detailed in the IS&T Addendum. This will ensure that Payroll functions will continue with very little interruption.

Human Resources shall work with the Executive Management/Leadership team to ensure the employees are available to serve the membership. HR shall be ready to review housing options for employees and their families that might have been displaced by the situation at hand. If an employee's family's needs are not being met, the employee will most likely not be available to work, therefore this is a key consideration.

Revenue

Membership billing shall continue during the emergency situation where and how reasonably possible. In the case that the meter reading function is not available for some reason, bills shall be estimated at their normal cycle billing dates to ensure continued cash flow. Engineering services will work with IS&T

to upload the list to the Daffron system and move the affected accounts to a special cycle and rate. These accounts will be on "hold" until readings are reported again. The special cycle will be monitored by the billing department to bill any accounts that have readings for more than a 20 day billing. No accounts will be billed a minimum estimated bill during the transition time. As the AMI readings post daily, the program will change any of those accounts that had a reading reported back to the rate and cycle they were in prior to the move.

In the event that the Command Center and Daffron iXp servers at the Burleson office fail or are destroyed, the billing process will be disabled. IS&T personnel will be responsible for loading Command Center on a backup server in Cleburne to allow meter readings to be gathered for billing. United will utilize Daffron's Disaster Recovery services as described within the ERP. With these procedures completed, the billing process would be restored with very little interruption.

Collections can be worked during this time, but the Executive Management/Leadership team shall agree to what level this will occur.

Cash/Credit Availability

UCS shall be prepared to make short term advances from lines-of-credit from financial institutions and be prepared to set up credit accounts with local businesses as necessary to support the emergency restoration effort. Where applicable, company credit cards should be used in lieu of credit accounts with local businesses. In the event that credit card information has been compromised, new credit cards should be ordered and the old ones canceled.

Offices

UCS shall maintain its three key facilities at a minimum (Burleson, Cleburne and Stephenville) in the case of an emergency situation. In the case where smaller offices need to be closed, personnel will be moved to other offices as necessary.

Communications and IS&T

UCS relies heavily on communications and IS&T functions. A backup and security plan must be in place to account for different types of failures with solutions already detailed. This plan along with several guidelines for backup purposes are listed within the ERP.

Transportation and Fuel

The Executive Management/Leadership team shall review the availability from the various departments prior to and immediately following the emergency situation. Mutual aid agreements/contractors shall be used in the event that the UCS transportation assets are severely impacted. Rental vehicles from vendors shall be considered if necessary. Fuel arrangements for each local area shall be made prior to the situation or immediately following the emergency.

Materials and Supplies

The purchasing/warehouse disaster plan shall be followed to ensure continued availability of warehousing duties and material availability. Other neighboring utilities stock may be used if necessary. Material review shall be done where possible if the situation requires UCS to move away from currently approved materials. Other supplies shall be made available to employees and visiting employees and contractors as necessary and possible. TEC may provide statewide support, where local organizations such as the Red Cross, United Way, Operation Blessing, will be used to support needs as possible. Further, the Wal-Mart Distribution Center may be an outlet for further support. Local community organizations and churches may be contacted for assistance for meal preparation until formally organized operations can begin. Credit accounts shall be established by the cooperative where necessary to support needs of employees and visiting workers. Preference should again be given to the use of company credit cards instead of establishing credit accounts with local businesses.

Member/Asset Information

Prior to the event or immediately after the event, member information must be available to all employees, visiting workers and contractors as necessary to perform their assigned function. The Emergency Coordinator shall ensure all information is available to workers as necessary and kept secure. There shall be a process set initially to track all system changes as they occur to keep up with accounting and engineering information. System engineering employees shall work to ensure work orders are created as necessary. Further, information shall be kept in methods where FEMA support can be requested if necessary.

ERP – Live Data Pulls

Several of the documents in the ERP are outdated by the time a printed copy is available. These documents are in the ERP; however, there are ways to pull “Live” data included in each TAB of the electronic version of the ERP that will allow access to the most current data available. These items are marked with “Live Data Pull” in the table of contents for each tab.

Guidelines for providing lodging and meals to UCS employees as well as outside resources as deemed necessary. These guidelines are intended to be used where feasible; however, they may be modified as needed to better accommodate the needs of UCS' employees and outside resources.

- Logistics Team (Landy Bennett, Russell Young, Blake Beavers, and Kade Kincannon) shall assess the severity of the event to effectively address lodging and meal needs for both UCS employees as well as outside resources.
 - Identify locations affected
 - Communicate/coordinate with appropriate UCS personnel to determine number of UCS employees that will need temporary lodging and the location(s) in which these resources are to be assigned
 - Communicate/coordinate with appropriate UCS personnel to determine the number of outside resources needed and the location(s) in which these resources are to be assigned
- Accounting Department to request temporary limit increases to company-issued credit cards for appropriate UCS personnel.
 - Instruct UCS personnel to obtain receipts of all purchased goods during and for the event
- Accounting Department to contact mutual aid organizations, if applicable, with record keeping and invoicing instructions, keeping in mind the possibility of FEMA requirements for such records.
- For the duration of the event, Logistics Team to obtain list of resources (both internal and external) each morning from appropriate UCS personnel that require temporary lodging that night and the location each resource has been assigned. Such list may be submitted to Logistics Team via e-mail at ERPLogisticsTeam@united-cs.com.
- Contact surrounding hotels to book appropriate number of rooms for the number of resources assigned to each specific location that will require temporary lodging.
 - Two (2) individuals per room
 - Book all rooms/reservations under the name 'United Cooperative Services'
 - Request from each hotel to apply all lodging expenses to one of the Logistics Team member's company-issued credit cards
 - Obtain/validate hotel invoices/room confirmations each day—direct hotel(s) to send all room confirmations electronically to the ERPLogisticsTeam@united-cs.com e-mail address
 - Use Mutual Aid Hotel Flyer, located in the ERP, to provide lodging information to internal and external resources (include hotel room confirmations, if available)
- Depending on how widespread the event is, coordinate meals (breakfast, lunch, dinner) for both UCS employees as well as outside resources.
 - When feasible, all breakfasts and dinners will be served in a communal fashion.
 - Lunches are to be served as a 'sack lunch' and available for pickup during breakfast each morning.
 - Coordinate meals with local restaurants the day before they will need to have food prepared
 - Where possible, all meal costs are to be applied to one of the Logistics Team member's company-issued credit cards
 - Verify if food will be delivered, served or require pick-up; pick-up food when necessary
 - When needed, assist in the setup and breakdown of "chow hall" for communal meals

Damage Assessment Process

Damage Assessment (DA) process will be initiated once a significant number of outages have been reached and crews dispatched are unable to restore outages without considerable construction efforts. When this occurs, management personnel should be prepared to call crews in and begin the DA process.

Once United has entered DA, all efforts to restore power have essentially been halted. All personnel and resources will be directed towards the DA process. There might be a need for operations personnel to help public safety officials in affected areas.

Field Engineering Manager will be the responsible person for directing the DA in each of the respective areas. Specifically, Senior Field Engineers – Gary Sowders (Granbury/Meridian), Denny Adams (Stephenville/PK) and Wes Burton (Burleson/ Cleburne) will coordinate DA operations in each of their respective areas.

Field Engineering Manager and Sr. Field Engineering Personnel will:

- Determine area to be assessed using:
 - OMS and SCADA information
 - Information from the field
 - News reports
- Determine DA crews
 - DA crew will need to consist of at least 2 persons
 - Ideally would consist of an engineering and operations person.
- Create and assign DA areas
 - Laptop with Partner's damage assessment module loaded.
 - Maps and/or other beneficial documents
 - Digital Camera associated to the DA (association will be a picture of the damage assessment log sheet (snap a picture of the laptop screen with the log sheet filled out) clearly visible at the beginning of the picture set. note: ensure date/time stamp is correct in camera and the function is on in the camera
 - Damage Assessors will:
 - Visit site assigned.
 - Fill out Damage Assessment Log
 - Take pre-cleanup/pre-restoration pictures of site assigned. to tie to FEMA form/staking sheet. note: ensure date/time stamp is correct in camera and the function is on in the camera
 - Synch DA package back to the Partner Hub upon return to the office.


Engineering Services will:

- Compile data from DA entries within the Partner module and make available to all departments to use in restoration processes. This will be done in Excel spreadsheet format and accessible through the network. The data will also be available through Partner's DA module and Filter Table.

Things to consider:

- It should be understood that when the DA process is put into place, FEMA reimbursement occurs with the outage restoration. Therefore, it is important where possible to return the line back to normal construction spec when restoring power, rather than utilizing the band-aid approach to get power restored.
- One DA = One log sheet = One Work Order. This will be the thought in the beginning. Findings from the field might dictate otherwise. For example, One DA might be broken into multiple Work Orders if significant damage is found.
- Cameras should be used from the inventory, but more can be purchased if necessary during the time of gearing up to begin the official damage assessment (see attached Digital Camera Inventory list). A digital camera with preview screen (non-lithium type battery) and a 1 gig SD card will be sufficient for the DA process - @ \$60 class camera.



Your Touchstone Energy® Cooperative 

Disaster Planning Quick Reference Guide for Employees

Last Updated: December 2022

Introduction and Purpose

As established by the United States Department of Homeland Security, United's facilities are considered critical infrastructure. Consequently, United is required to prepare and practice for emergencies in case they do occur so there is minimal impact on critical infrastructure and ultimately the public.

This Disaster Planning Quick Reference Guide for Employees of United is meant to serve as a general guide for employees when dealing with emergencies. The intent of this guide is to ensure that employees are prepared for various types of emergencies, but is not possible to cover every possible emergency scenario.

This Guide is broken up into sections that can help employees understand their roles in an emergency. Primarily, United must maintain an Emergency Response Plan (ERP) that will guide the organization in the event of an emergency. An "emergency" is defined as **"an unusual event that involves risk to people, property, or the environment."** Some potential threats that can lead to an emergency are listed below:

Fire	Employees	Pandemic
Chemical Spill	Terrorism	Gas Leak
Power Failure	Contract Labor	Domestic Violence
Weather	Aircraft	Explosion
Customers	Vehicles	Biohazard
Flood	Bomb Threat	Loss of Communications

Each employee should take time to consider how they would respond within these guidelines to the threats above, and possibly others. The remaining sections following the overview of United's ERP provide general information that will allow each employee to evaluate their response readiness.

Any questions or concerns regarding this Guide should be brought to the attention of the employee's direct supervisor or United's Emergency Coordinator.

United Emergency Response Plan Overview

The process of creating United's ERP began with creating a departmental vulnerability and risk assessment (VRA). With the VRA complete and after reviewing a myriad of available materials, United decided to use Texas Electric Cooperative's (TEC) emergency response plan template as its starting point. United has adopted this document as the foundation of its ERP to maintain consistency with other cooperative's in the State of Texas. United has not edited content, other than the addendums described below, and understands that the typical organizational structure described in the document does not exactly coincide with United's organization. It is imperative that United's emergency response team review this document prior to or within 24 hours following the emergency situation to ensure guidelines are agreed to and followed.

The addendums to the ERP provide details and supplemental documentation specifically applicable to United. The addendums to the ERP follow the below numbered tab format:

1. Emergency Response Plan Structure and Guides
 - a. Disaster Specific Information
2. Contacts, and Key Accounts Lists
3. Processes, Guidelines, and Procedures
4. Regulatory Agencies
 - a. RUS
 - b. FEMA
 - c. PUC
 - d. ERCOT
 - e. Other
5. Miscellaneous

This document has been accepted and approved by the Executive Staff, CEO, and Board of Directors as United's Emergency Response Plan as required by CFR 1730.28.

This document should be reviewed and tested by United's emergency response team annually as required by CFR 1730.28.

An excerpt from the ERP concerning responsibility of employees follows:

The organizational chart shall govern the operations of United in the case of an emergency event. In the event that United has information of a potentially severe emergency, the Executive Staff shall meet prior to the potentially severe emergency and review the elements of this plan. In the event that the emergency has already or is occurring, the Executive Staff, or the Supervisor Task Force in their absence, shall meet as quickly as feasibly possible immediately following the start of the emergency situation in order to prepare for handling such using this plan.

The Emergency Coordinator (Senior Vice President of System Engineering) [or secondary Emergency Coordinator (Senior Vice President of Cooperative Planning and Procurement) in the absence of the Emergency Coordinator] shall work with the rest of the Executive Staff to coordinate all emergency response. In the absence of both the Emergency Coordinator and secondary Emergency Coordinator, the CEO shall appoint some other employee to be the Emergency Coordinator. In the absence of the CEO and Executive Staff, the President of the Board of Directors will be contacted to call an

emergency Board meeting to name an interim CEO. For immediate disaster response, the Manager of Operations will assume the role of interim Emergency Coordinator, the Vice President of Information Systems and Technology will assume the role of interim Secondary Emergency Coordinator, and the Leadership Team will provide leadership as well. It is the responsibility of the Emergency Coordinator to ensure the plan is followed for its purposes. In the absence of the CEO, the Emergency Coordinator shall work with the COO and CAO along with the rest of the Executive Staff or Leadership Team in their absence.

Other duties of the Emergency Coordinator are as follows:

- *Keep this plan and all information contained herein consistent with the TEC statewide disaster plan(s) where applicable,*
- *Keep up/be involved with Local, State, and Federal training exercises where possible/applicable,*
- *Keep the information contained herein up-to-date and accurate with a minimum of an annual review and update process, and*
- *Annually 'test' the plan and coordinate information transfer with RDUP concerning UCS' compliance with ERP requirements.*

Duties of UCS employees may not follow general job descriptions following an emergency. Employees will be utilized where and how necessary to best deal with the emergency at hand.

Employees with responsible charge to act within the ERP for United as designated by United's Emergency Coordinator/Secondary Emergency Coordinator or the Assistant Manager, or CEO in his absence should have a copy and should annually review the Plan.

Office Evacuation in Emergency

Office evacuation may be necessary in the event of an emergency. United has employees working in seven different offices across its service territory, all of which have different layouts, tools, and resources that each employee should be familiar with in an emergency situation. Evacuation plans for each office are located on the Circuit under the Safety Documents in the Human Resources and Safety Section. Following the contacts sections in this Guide is an 'Employee Checklist' that each employee should fill out during or immediately following the annual emergency training session.

The Total Evacuation method should be utilized in the case of an emergency. Total Evacuation requires all employees in the affected building to orderly evacuate to the nearest safe, accessible exit. In the event that all accessible exits are blocked by the emergency, employees should exit through windows of the first floor.

Employees should consider when evacuation might be necessary if any of the threats listed below should occur. There may be different correct answers across United's offices and work areas.

Threat	Some Points to Consider about Preparedness
Fire	Is the fire within portable control? Do you know where the fire extinguisher is located? Are there other fire extinguishing methods that could be used? Have you contacted 911? Have you notified personnel necessary to begin an evacuation?
Chemical Spill	Do you know where the MSDS sheets are located to determine what steps you may need to take in the event of a spill? Do you know who to contact if a spill occurs? What should you do if you encounter a substance that is unknown?
Power Failure	Is your equipment on a UPS? Should it be? What should we do to restore power?
Weather	How does weather impact your job? What would you do if there is a tornado that creates building damage? Where would you go in the building for safety? Is it safe to drive in ice conditions?
Customers	How do you handle an impatient/uncontrollable customer? Should you challenge them? What if they are armed?
Flood	What if a building floods due to water pipe break or massive rains? How will it impact your job? Are computers or other electrical equipment directly on the floor?
Employees	What would you do if an employee or ex-employee became belligerent?
Terrorism	What areas at work are vulnerable to a terrorist act? How would you respond?
Contract Labor	How do we maintain total security with contract labor? Do we perform background checks? How is insurance handled?
Aircraft	Two of United's offices are near landing strips. What would happen if we had an accidental crash into our facility? How would you react?
Vehicles	What would occur if a vehicle was used to damage United office facilities? What would you do if an employee was injured?
Bomb Threat	What should you do if you receive a bomb threat? Does your telephone show caller ID?
Pandemic	How should you conduct your job in the case of a severe pandemic? What actions would UCS need to take to separate employees from infectious materials/areas?
Gas Leak	What if we have a natural gas leak? How will we know? Who do you call?
Domestic Violence	What do you do if an unhappy family member of an employee shows up to the office to discuss family business? What if the situation gets out of hand?
Explosion	If there is an explosion, should you evacuate immediately? What about if employees are left in the building that are injured?
Biohazard	What if a biohazard presents itself, say in a bathroom, or in other areas in the office? Who are you going to contact?
Loss of Communications	What plans are in place for loss of communications? Who is responsible for implementing backup plans? Are there complete backup plans for likely modes of failure?

Reporting to Offices in an Emergency

There are several emergencies that could keep employees from reporting to an office. The likely possibilities are 1) weather complications that prohibit the travel of employees to the office; or 2) an office has been damaged to the point that it cannot be occupied.

If there is an emergency and you cannot report to the office, you should do the following:

1. Contact the HR employee lines at 817-556-4099 or 254-918-6199 to find out if there have been messages left as to the status of offices.
2. Contact your supervisor by any means possible and let them know that you cannot report to the office. At this point, the supervisor will have to decide whether or not he will work out other modes of transportation.
3. If your supervisor cannot be directly reached, leave a message and attempt to contact the next level supervisor. Leave a message if there is no answer.

If you report to an office and it is not accessible, you should report this to the Emergency Coordinator and Safety On-Call Employee as soon as possible if no employee is already on site. If there are no other instructions, employees should report to the following offices under these circumstances:

- Cleburne Office Damaged: All employees report to Burleson.
- Stephenville Office Damaged: Stephenville Administration employees and Cooperative Planning employees report to Cleburne. Customer service, system engineering, and line crew employees report to Granbury.
- Granbury Office Damaged: All employees report to Stephenville.
- Burleson Office Damaged: All employees report to Cleburne.
- Meridian or PK Lake Office Damaged: All employees report to Stephenville.
- Joshua Office Damaged: All employees report to Cleburne

Contact with Media

Media personnel will generally be involved in emergency situations. If a member of the Media contacts you, please direct them to the Chief Operating Officer/Assistant General Manager. If this person is not available, then the CEO shall be the next employee to be contacted. If this does not work, contact the Emergency Coordinator. It is important to remember that all media contact should be directed through a single point of contact to enable consistency of the message. Further, kindly avoid responding to media citing lack of information and pass the request to the appropriate employee as mentioned above.

Personal Preparation

In the event of impending disaster prepare by doing the following:

- Store a two-week supply of water, non-perishable food, and prescription medications. During an emergency, if you cannot get to the store or the store is out of supplies, it will be important for you to have extra supplies on hand.
- Have other needed items such as batteries, flashlights, manual tools/appliances, garbage bags, toilet paper, soap, etc.
- If possible, maintain an extra supply of your regular prescription items to ensure continuous supply is available to see you through an emergency situation that may continue for several days.
- Have any non-prescription drugs and other health supplies on hand, including pain reliever, stomach remedies, cough and cold medicines, fluids with electrolytes (Gatorade), and necessary vitamins.
- Talk with family members and loved ones about how they would be cared for if you were not available to take care of them.

To Limit the Spread of Germs:

- Follow CDC guidelines for personal hygiene.
- Wash your hands frequently with soap and water; model the correct behavior for peers and children.
- Always cover when coughing or sneezing.
- Stay away from others as much as possible if they are sick or if you are sick. Stay home if you are experiencing any common symptoms of the pandemic.

Employee Checklist

There are some key things employees should know about their work area to properly respond in an emergency. Below is a checklist that should be reviewed during or immediately following the annual emergency training. Place a check mark on each item as you have evaluated the appropriate answer for your office. Notes should be written next to each question to assist you in remembering your environment.

- ☐ Do you know how to use the telephone system at the office in which you work? How do you dial 911 from your office?
- ☐ How would you describe the location/address of your office to law enforcement personnel in a 911 call?
- ☐ Where is the closest fire extinguisher to your work area? Do you know how to operate the extinguisher if necessary?
- ☐ If it were necessary and available, do you know how to access the overhead paging system for your office to notify other employees in the building that there is an emergency?
- ☐ Do you know where all exits are for your office? What is the closest exit to your actual work area? What is the next closest exit to your actual work area if the closest exit is not accessible?
- ☐ If a Total Evacuation is required, do you know where you should meet with other employees? Should someone attempt to make a count of each employee after an evacuation has occurred?
- ☐ If a Total Evacuation is required, what timeline applies to be totally complete with the evacuation?
- ☐ Where is the closest first aid kit to your work area?
- ☐ Who is United's Emergency Coordinator? Who is the Backup Emergency Coordinator?
- ☐ Where can you find a copy of the EEC (Employee Evacuation Plan)?
- ☐ Where are you going to keep this Guide so that you have access?
- ☐ Where can you find United's Emergency Response Plan?

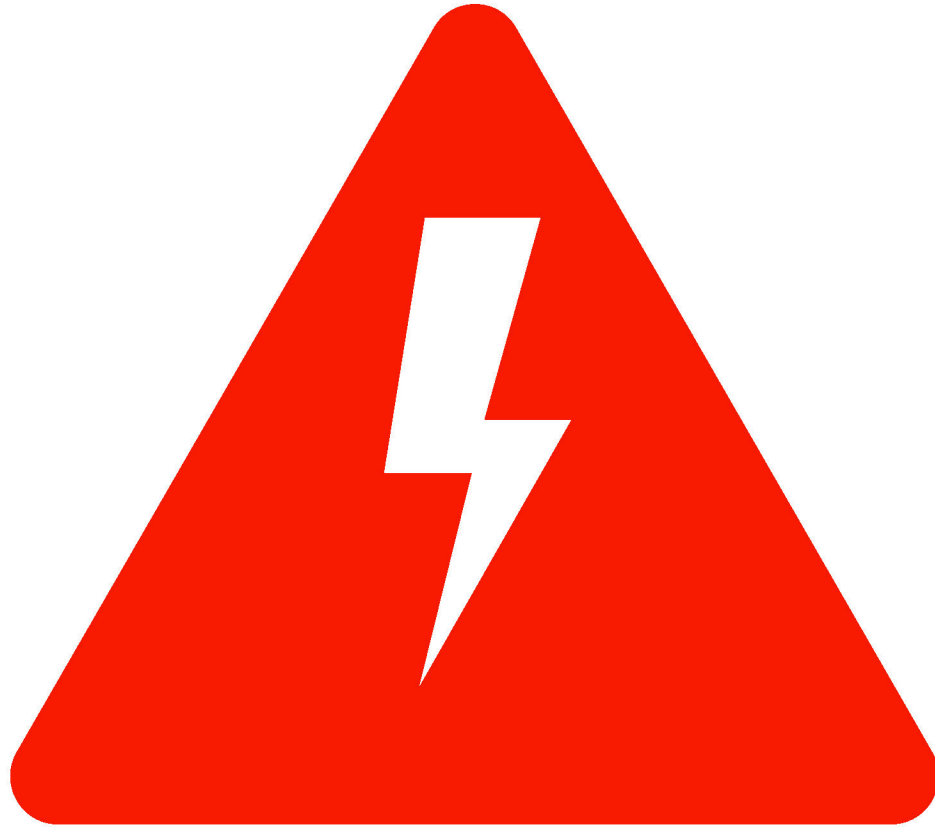


Disaster Planning for Employees

JANUARY 2023

WHY ARE WE GOING OVER THIS?

- The Department of Homeland Security defines United as Critical Infrastructure
- Rural Utilities Service – Requirements to continue to receive loan funds
- Over the past 15 years, United has had the “opportunity” to use the contents of the ERP every other year on average.
- **Most importantly - Being Prepared = The Safest Work Environment**



Emergency Response Plan

- **Emergency Coordinator:**
Quentin Howard
- **Secondary Emergency Coordinator:** **Bruce Goss**
- **ERP Must Be Tested And Updated Once a year**

Emergency Response Plan (ERP) Overview



Follows TEC's Emergency Plan template for Texas Co-ops.

Tabs 1 through 5 give specific information related to the type of emergency event that occurs.

The current Emergency Response Plan can be found on The Circuit under Important Documents/Disaster Plan

2022 Tabletop Exercise - Disaster Scenario

- In early July 2022, United's territory was hit by a late season thunderstorm.
- At the same time the rest of Texas was experiencing record heat and the potential for rolling outages across the State.
- The storm caused over 100 outages across UCS's system which left approximately 5,000 meters without power
- Several of United's employees were on vacation following the July Fourth Holiday, and a number of the Cooperative's IS&T, Billing, and Member Service supervisors were out of town for the annual Milsoft Users Conference.

2022 Tabletop Exercise – Disaster Scenario

- Phishing emails were being sent to utilities (including United) posing as ERCOT requesting emergency load shed to stabilize the grid.
- An employee that was busy working the outages accidentally clicked on the link in the email which loaded a Zero-Day ransomware on the network.
- During the storm the Burleson POP building was and there were approximately 12,000 Internet Customers who lost internet access across United's territory including the cooperative's offices.
- Finally, the cooperative's Cloud based VOIP Phone system was also rendered unusable because of the damage to the Burleson POP.

Quick Reference Guide Layout

Introduction and Purpose

Emergency Response Plan Overview

Office Evacuation in Emergency

Reporting to Office in Emergency

Contact with Media

Personal Preparation

Employee Checklist

The Quick Reference Guide is located on The Circuit under Important Documents/Disaster Plan

- List of Threats: How would you respond to an emergency as listed?
- Read through this list, if you can't answer a question, please get with your supervisor.
- If a total evacuation is required, do you know where you should meet with other employees? Should someone attempt to make a count of each employee after an evacuation has occurred?

Office Evacuation in an Emergency

Reporting to the Office in an Emergency

If you cannot report to your normal office location due to a widespread emergency, what should you do?

Contact HR employee lines for employer instructions:

Cleburne 817-556-4099

Stephenville 254-918-6199

Contact your supervisor for further instructions as soon as practical; leave a message.

Understand which office you are to report to if an office is damaged.

Contact with Media



- Please don't try to be a media spokesman for United.
- It is very important to provide the media with a single point of contact during emergency events to ensure timely and accurate information is always provided.
- Direct all media requests to United's Chief Operating Officer/Assistant General Manager Marty Haught

Personal Preparation

- Be prepared for an emergency. Your understanding of emergency procedures will save valuable time in United's response.
- Review the information provided in the Quick Reference Guide.
- Red Cross, CDC, and FEMA also provide helpful information on personal disaster preparedness.



Are you
prepared?

Understand how you should react
to different threats

Understand and answer the
check-list

***Questions should go to your
supervisor***

ERP – Distribution List

Distribution List for United Cooperative Services Emergency Response Plan – Version 1.2023

Emergency Coordinator: Quentin Howard

Secondary Emergency Coordinator: Bruce Goss

Emergency Team Copies:

Quentin Howard – Electronic copy for business computer; Iron Key copy for home

Bruce Goss – Electronic copy for business computer; Iron Key copy for home

Official Office Copies: Posted on the Circuit (Cooperative Intranet Site for all employees) –

Microsoft Share Point



Date: _____

RE: United Cooperative Services requests your assistance.

United Cooperative Services has sustained significant damage to our electric distribution facilities as a result of the recent _____, and United is requesting your Cooperative's help. In accordance with the Cooperative Mutual Aid Agreement, United is sending you this letter to officially request your assistance. If you have personnel and equipment available and are willing to render aid to our Cooperative, United is specifically in need of the following personnel and equipment to assist us in restoring power to our Members as quickly and safely as possible:

I would like to personally thank you in advance for your help! In addition, I would like to point out that any and all aid will be reimbursed in accordance with the Cooperative's Mutual Aid Agreement.

Should you have any questions or concerns you can contact United's Emergency Coordinator, Quentin Howard at (254-918-6127) or Quentin@united-cs.com; or our secondary Emergency Coordinator, Jared Wennermark at (817-782-8358) or Jared@united-cs.com.

Yours truly,

Cameron Smallwood
Chief Executive Officer
United Cooperative Services

United Cooperative Services 2/16/2021

Considerations for the Operations Department during a Disaster

Set up:

- 1) Locate an area large enough to be utilized for warehouse, control center, on-site fueling, and scrap material. Location needs to be as close to damaged area as possible. Additional locations for pole distribution and ease of delivery required.
- 2) Location will require scrap material trailers and large dumpster to accommodate large volume of trash.
- 3) Restroom facilities
- 4) If this event may last for days, security fence or 24-hour security may be required
- 5) If operations from the selected area will continue during non-daylight hours, portable lighting systems may be necessary.

Daily Crew Work:

- 1) Have all contact info-Company names /foreman /cell phones readily available
- 2) Spec book-to each crew, crews will utilize since they will be given a W/O with units
- 3) Keep track of crew W/O's for coordination with warehouse to allow for progression times of completion of each W/O
- 4) Crew Foreman turn in W/O after each is completed and check for as-builts
- 5) Coordinate with engineers on next area needed for progression

Safety:

- 1) Safety meeting at the start of each day
- 2) Ensure that all PPE is expected to be utilized
- 3) Review Personal Grounds
- 4) Have United employees assist crews to work site
- 5) Brief each crew on W/O's
- 6) All line to be energized will only be done so thru coordination with Dispatch and Operations Field Coordinator
- 7) Have name and contact of Fire Marshall and other emergency officials

Equipment:

- 1) Have phone numbers for onsite repairs, tires, and welding vendors (internal and external)
- 2) Notify fleet mechanic vendors

Determine when to change from construction to disaster management:

Begin to evaluate the transition from construction to disaster management at Outage level 3 to 4, from Outage Management Guidelines in Tab 4 of ERP.

Fuel:

- 1) Operations Manager will notify Senior Fleet Mechanic to start fuel shortage process
- 2) Notify listed suppliers of fuel storage capacity needed to fit districts needs
- 3) Notify listed suppliers of fuel amount and type to be delivered to required district locations

Honstein Oil
370 North Sylvania Ave.
Fort Worth, TX 76137
817-831-0601 office
Shannon Stanley 817-829-4378 mobile

S&S Scott Oil
106 Avenue A
P.O. Box 86
Blum, TX 76627
254-874-5569

Love Oil Company
700 W. Vanderbilt
Stephenville, TX 76401
254-965-3518

Connel Oil Corp.
100 SE 6th Avenue
Suite 280, Bank of America Building
Mineral Wells, TX 76067
940-325-7777

Internet Connectivity 2019

During an emergency it may become necessary to access the internet in an area where internet access is not available. In that case, UCS will utilize (2) Verizon MiFi devices. Up to 5 computers can connect to the internet thru each MiFi device. Tethering to a cooperative issued iPhone is secondary option. The MiFi devices are assigned to the following employees:

1. Cameron Smallwood- Ext. 5222, Cell-817-648-6515
2. Marty Haught- Ext 5223, Cell-817-487-7009

If you need any assistance setting up the MiFi devices or tethering to an iPhone, please contact the following:

1. Brad Mead - Cell-817-648-5906
2. Eric Cagle - Cell-254-396-2705
3. John Huffman - Cell-682-228-8141
4. Yuri Lavadour –Cell-817-456-4382

Identifying Specific Needs 1/13/2023

Evaluate current ERP event to determine cooperative needs regarding internal and external personnel resources, as well as restoration equipment.

To accomplish this, items to be consider are

- Damage Assessment need's
- Type of ERP event
- Ground conditions
- Special equipment
- Type/scope of work
- ERP field managing essentials (command center if needed

Beginning of event ERP Coordinator and Operations Manager will analyze specific requirements that will be communicated to workforce and contractors before restoration begins.

Name	Department	Job Title	Location	Office Phone	Mobile Phone
Aaron Lowe	Field Engineering	Field Engineering Rep I	Cleburne	817-556-4014	817-487-3078
Anthony Mejia	Field Engineering	Field Engineering Rep II	Stephenville	254-918-6143	254-434-3663
Brandon Sadler	Field Engineering	Field Engineering Rep II	Granbury	817-326-1556	817-517-1282
Brian Haydon	Field Engineering	Field Engineering Rep II	Cleburne	817-556-4048	682-459-5223
Brody McPherson	Field Engineering	Field Engineering Rep I	Granbury	817-326-1557	682-228-8668
Brody Weems	Safety	Safety and Loss Control Coordinator	Stephenville	254-918-6140	254-485-5249
Daniel Cornia	Field Engineering	Construction Contract and Veg Mgmnt Coordinator	Burleson	817-556-4058	682-702-8911
Dustin Lumm	Field Engineering	Field Engineering Rep I	Cleburne	817-326-1553	682-459-3080
Gary Sowders	Field Engineering	Senior Field Engineer	Granbury	817-326-1561	254-396-2716
Jason Dillard	Field Engineering	Field Engineering Manager	Cleburne	817-556-4055	817-253-3514
Jason Jean	Field Engineering	Field Engineering Rep I	Burleson		
Jesse Whitt	Field Engineering	Senior Field Engineer	Stephenville	254-435-6752	254-978-0098
Joe LoPalo	Field Engineering	Field Engineering Rep II	Burleson	817-782-8320	817-682-7782
John P. Jones	Field Engineering	Field Engineering Rep II	Stephenville	254-918-6146	254-396-0836
Mark Buckner	Field Engineering	Contract Coordinator	Cleburne	817-556-4066	254-396-1340
Mark Dixon	Safety	Safety and Loss Control Director	Burleson	817-782-8346	817-648-5943
Matt Biery	Field Engineering	Field Service Agent	PK Lake	940-779-7102	940-452-1034
Paul Taylor	Field Engineering	Field Engineering Rep I	Stephenville	254-918-6169	254-431-1383
Phil Silva	Field Engineering	Senior Field Engineer	Cleburne	817-556-4070	254-396-2717
Steven Ferguson	Field Engineering	Construction Contract and Veg Mgmnt Coordinator	Stephenville	254-918-6155	254-485-3588
Wes Burton	Field Engineering	Senior Field Engineer	Burleson	817-782-8316	817-517-9612
Sam Heathington	Operations	Mechanic	Stephenville	254-918-6136	817-408-0640
James Nethaway	Operations	Mechanic	Cleburne	817-556-4000	208-871-1757
Senovio Delagarza	Operations	Mechanic	Cleburne	817-556-4001	254-396-3203
Ronnie Necessary	Operations	Mechanic	Stephenville	254-918-6136	254-485-3505

Credentialing Process

In the event of an ERP event that requires assistance from other Cooperatives, and/or contractors that are not already performing work for United, the following credentialing process will be initiated. The process is as follows:

- Access Permits (see below) will be printed (Landscape – 8 ½ x 11) for each vehicle that will be working on the Cooperative's system.
- Individually assigned and numbered permits will be cataloged through denotation of date, time and participating organization.
- When possible, the permits will be included with the informational packets that are to be given to the Cooperative personnel when they arrive to provide assistance.

ACCESS # PERMIT

PERMIT VOID AFTER:

This unit is assisting United Cooperative Services with mutual aid in response to this emergency restoration event. Please allow these authorized cooperative representatives entrance and access to any unrestricted areas of United's electric distribution system.



**United Cooperative Services
Vulnerability Analysis Chart**

Type of Event	Priority
EMP Attack	18.90
Nuclear Meltdown - Major Loss of Coop. Overhead Assets	18.70
Nuclear Meltdown - Major Loss of Coop. Underground Assets	18.50
Nuclear Meltdown - Materials, Warehouse, and Purchasing	18.30
Ice Storm (Systemwide)	18.10
Tornado (localized) - Facilities	17.60
Nuclear Meltdown - Effect on Staking	17.30
Nuclear Meltdown - Effect on Connects/Disconnects	17.00
Terrorism	16.70
Electrical Contact Fatality - Internal	16.30
Severe Weather - Major Loss of Coop. Overhead Assets	16.20
Ransomware affecting entire network	16.00
Ice Storm (localized)	16.00
OTJ accident causes employee fatality	16.00
OTJ accident causes employee fatality	16.00
Severe Weather - Major Loss of Coop. Underground Assets	15.80
Major Transmission Loss	15.70
Cyber Attack of our network	15.60
Loss of Entire Phone System	15.60
Electrical Contact Fatality - External	15.60
Inadequate Generation	15.60
Fire in the server room damaging servers and network equipment	15.50
Tornado - Warehouse and Purchasing	15.50
Workplace violence, traumatic event	15.20
Flu epidemic, cause serious illness to employees	15.10
OTJ employee accident causes serious injury	15.10
OTJ employee accident causes serious injury	15.10
Fire at Office - Facilities	15.00
Power surge in server room that could take out multiple servers and/or network equipment	14.90
Fire at Office - Materials/Purchasing/Warehouse	14.90
Disgruntled IT employee intentionally bringing down AD or network	14.80
Earthquake - Facilities	14.70
Employees & families displaced due to natural disaster	14.70
Fire at Office - Billing/CIS	14.70
Tornado - Accounting, Payroll, HR	14.70
Solar Flares Event	14.60
MW Tower Loss	14.50
Electrical "Dig In" - External	14.50
Inability to man offices - All offices	14.50
Loss of Internet Connections	14.30
Dispatch Technology Failure	14.30
Severe Weather - Effect on Staking	14.20
Fire at Office - Accounting/Payroll/AP	14.10
Hail Damage - Facilities	14.10
Ransomware affecting one office	14.00
Brazos Network Loop Failure	14.00
Substation Overload Failure	14.00
Electrical "Dig In" - Internal	13.80
Falling Objects (trees, towers) - Facilities	13.70

**United Cooperative Services
Vulnerability Analysis Chart**

Type of Event	Priority
Fleet damage/loss	13.70
Severe Weather - Effect on Connects/Disconnects	13.70
Hail Damage - Vehicles	13.60
Power Contract Obligations - Inability to meet contractual agreements/provide power	13.60
Cell Network - Employee Phones	13.60
PCB/Major Oil Spill	13.60
Theft of wire/materials - distribution system	13.60
Vehicle slamming into the building	13.60
Loss of each offices Computer/Switch room	13.50
Gas "Dig In"	13.50
Power loss of facilities	13.50
Rainwater Damage - Facilities	13.50
Theft of service	13.50
Circuit Overload Failure	13.40
Dispatch - Loss of primary dispatch center	13.40
Material supplier/manufacturer catastrophe	13.30
NRECA Employee benefits (cash/non-cash default)	13.30
Physical Robbery	13.30
Substantial liability suit cause	13.30
Inability to man office	13.20
Earthquake - Roads/Transportation	13.10
Earthquake - Gas Leak/Environmental	13.10
Failure of phone system in individual offices	13.10
D-mark or lines from telco company destroyed into building	13.00
Cell Network - MV90	13.00
Radios - Loss of LMR	13.00
Sudden tariffs on imported goods	13.00
Theft/Vandalism in individual offices	13.00
AS400 Work Order Sys. Malfunction	12.90
UPS problems denying power to server racks	12.90
Earthquake - Distribution System	12.90
AMI System Failure - System Engineering	12.90
AS400 Hardware Loss	12.80
AMI System Failure - Billing/CIS/Pre-Power	12.80
Computer System Failure - Billing/CIS	12.70
Event due to proximity to Highway/Interstate - Distribution Systems	12.70
Employee misconduct/vandalism - Billing/CIS	12.60
Event due to proximity to Highway/Interstate - Facilities	12.60
AS400 Billing System Failure- Effect on Meter Reading	12.50
Loss of both firewalls in Burleson	12.50
Major insurance carrier - bankruptcy	12.50
Earthquake - Materials/Warehouse	12.40
Employee misconduct/vandalism - Accounting, Payroll, & AP	12.40
Geo-Political Events affecting supply chain	12.40
Daffron Billing Software Servers failure	12.40
Employee misconduct/vandalism - Materials/Purchasing/Warehouse	12.30
Key personnel lost/unavailable	12.30
HP Switch Failure	12.20
Cell Network - DA Communications/FCI	12.20

**United Cooperative Services
Vulnerability Analysis Chart**

Type of Event	Priority
Pilferage/Embezzlement	12.20
AS400 Billing System Failure - Effect on Collections	12.10
AS400 Billing System Failure - Effect on Connects/Disc.	12.10
Computer System Failure - Accounting, Payroll, and AP	12.10
Antivirus software failure	12.10
Exchange Server failure/damage/loss	12.00
Protests outside of office(s)	12.00
Key Account Staff loss/inability to contact	11.80
SCADA A and B Down	11.80
UFR Event	11.80
Human Error	11.70
In ability to communicate with media and/or membership	11.70
Recloser/Control Failure	11.70
Supplier Misconduct	11.70
Loss off VMWare Stacks	11.60
Failure of Access Control System	11.40
MV-90 Computer Failure/Loss	11.40
SPCC Event - Facilities	11.30
Capacitor/Control Failure	11.10
Regulator/Control Failure	11.10
Milsoft FE Failure	11.10
Environmental/Historical Impact on Line Construction or Work Plan	10.80
Employee training files lost/mismanaged/compromised	10.30
Driver qualification files lost/mismanaged/compromised	9.80
Test Facility Collections Interruption	8.80