Filing Receipt

Received - 2023-02-20 01:30:13 PM
Control Number - 53385
ItemNumber - 873

EMERGENCY MANAGEMENT PLAN

Note: Printed, hard copy versions may be outdated. Please look for latest version on-line or contact your manager for latest version.

Table of Contents

1. Approval and Implementation

1.1 Introduction

This Emergency Management Plan, (EMP or Plan), has been revised to include all pre-existing safety plans into a single document for Power Resources Inc. ("PRI"). This plan now includes the Emergency Response/Management, Loss Prevention, Crisis Communication, Security Contingency and Business Recovery Plans which are an integral part of the company's overall program for enterprise risk management.

This Plan is designed to provide response guidance, minimize disruption to the critical activities at PRI in the event of a declared major emergency or event affecting plant operations, and enhance the protection of lives and property through effective uses of resources. While this guide does not cover every conceivable situation, it does supply the basic administrative and operational guidelines necessary to cope with most emergencies.

Whenever an emergency affecting PRI's interests reach proportions that cannot be handled by routine measures, the General Manager, or his designee may declare a state of emergency and these contingency guidelines may be implemented, including previsions noted in BHER Business Continuity Plan (management copies only).

"**Emergency**" is defined as an event that disrupts critical business processes and degrades their service levels to a point where the resulting financial and operating impact to our business becomes unacceptable. These business processes include lives, property, environmental processes and equipment.

This Plan documents the team structure and the actions to be taken by plant personnel in the event of disruption to normal business as a result of a major event or emergency, affecting operations of the PRI facility or its employees.

PRI's policies and procedures herein will be followed by all employees whose responsibilities and authority cover the operational procedures found in the manual. PRI's emergency operations will be conducted within the framework of these guidelines. Any exception to these procedures will be conducted by, or with the approval of the General Manager or the Emergency Coordinator. All requests for procedural changes, suggestions, or recommendations will be submitted in writing to the General Manager for review.

The PRI Emergency Management Plan shall be the primary source for guiding employees when confronting emergency situations and supersedes any previously developed and/or implemented policy and procedures, which reference specific emergency situations that had been in effect.

1.2 Revision and Control

Revision No.	Revision Date	By	Changes Made
0	09/28/16	JB	Review all emergency response documents and combined into one single new plan
02	04/26/17	JB	Updated Plant Weatherization Plans and Procedures, contacts
03	11/21/17	JB	Approval Names, Updated Extreme Cold Weather Operations Plan, Contacts, changed Alon to Delek
04	03/21/2018	JB	Updated to reflect organizational changes, critical equipment changes and annual testing per CW audit
05	05/14/2018	JB	Updated management staffing changes and incident types
06	11/20/2018	JB	Cyber security updates, BHER BCP plan key notes Reviewed April 10, 2019 (no changes except updated employee names and phone list)
07	05/28/2019	JB	Updated key management contact information. Included new section on responses to transformer fire/event.
08	11/22/2019	JB	Added additional BCP data, clarified notification duties, security updates and cyber security protection)
09	05/20/2020	JB	Corporate cyber security plan reference, update contacts, water conservations and included additional detail on pandemic events. referenced Corona Virus documents
10	11/19/2020	JB	Included reminder to terminate ex-employee access to non-company sites. Updated employee contact information and winterization checks sheets and forms
11	02/19/2021	JB	Updated key management contact information, corrected spelling issues, minor additions to cold weather plans.
12	07/14/2021	SES	Added petroleum and bulk chemical storage locations, amounts, and containment; updated site maps.
13	11/4/2021	MAG	Updated employee/vendor contact list
14	09/23/2021	MAG	Updated Cold Weather Procedures Updated Cold Weather Procedures
15	04/07/2022	EKW	Updated to incorporate PUCT updates to PUCT Code section 25.53
16	01/31/2023	EKW	Annual Review. Updated to reflect new General Manager

Table 1: Document History

1.3 Approval

The following are authorized to approve issues of this document and are responsible for maintaining and implementing this EOP:

Title	**Name**	**Responsibility**
General Manager	Derek Graves	Maintain and Implement
Operations & Maintenance Manager	Waylon Merket	Maintain and Implement
Compliance Program Manager	Eric White	Change EOP
VP Operations Gas	Eric Bowen	Change/Approve EOP

Table 2: Individual Responsibility Matrix

Revision	Description	Name	Signature	Date
16	Annual Review. Updated to reflect new General Manager	Eric Bowen		01/31/2023

Table 3: Approval

As of January 31, 2023, Revision 16 of this EOP is the current version and supersedes all previous EOPs. This revision 16 was approved on January 31, 2023.

1.4 Distribution List

Title	Name	Location
General Manager	Derek Graves	Master Document
Operations & Maintenance Manager	Waylon Merket	Electronic Copy
Control Operator	Curtis Harrison	Control Room DCS Panel
Control Operator	Eugene Boadle	Control Room DCS Panel
Control Operator	Joseph Thompson	Control Room DCS Panel

2. EMERGENCY Management Plan

PRE-EMERGENCY PLANNING/COORDINATION WITH OUTSIDE PARTIES

PRI has opted to not designate a fire brigade or HAZMAT team and will only train people to the extent necessary to respond defensively to emergencies. Under this option, PRI will rely on outside entities for offensive response to incidents. PRI has notified the Big Spring Fire Department, and Howard County Volunteer Fire Department of their response capabilities and options.

ADMINISTRATION AND IMPLEMENTATION

The Control Room Operator will be the Emergency Coordinator during the initial Facility response to the incident. This person is responsible for classifying the incident as an internal emergency or as an emergency that could affect people outside the facility boundary. This person shall also be responsible for determining whether assistance from off-site Emergency Response agencies should be requested. PRI classify emergencies in three main levels:

Incident: emergency that can be controlled by PRI personnel with no external aid such as, small spills or small fires.

Level 1: Event that can be controlled by PRI personnel with off-site assistance. The Big spring Fire Department and Howard County Volunteer Fire Department by mutual aid agreement.

Level 2: Event controlled by off-site emergency response parties. Full evacuation is required at this level. Entities such as the Big spring Fire Department, Howard County Volunteer Fire Department, HAZMAT response units, state troopers, county sheriff, and hospitals could be involved in this emergency level.

Emergency Response agency personnel who arrive on site to provide assistance will report to and provide assistance to the Control Room Operator. The CRO will remain in charge until:

The CRO is relieved by facility management; or

The emergency response is off site.

Local City and County Emergency Planning Committees exist to coordinate Facility Plans with local Emergency Operations Plans.

Howard County's Emergency Organization consolidates the existing agencies of the county government, departments of the municipalities which do not have full scale emergency management organizations, and resources of the private organizations which have accepted responsibility for emergency management functions. The County Emergency Organization, the participating agencies and private organizations are shown in the Big Spring / Howard County Emergency Management Services Plan.

2.1 Purpose

To be effective in handling emergencies, the company is committed to establish and implement the following programs:

Identify potential emergency risks;
Develop appropriate plans and procedures;
Assign responsibilities;
Provide resources and equipment;
Establish procedures for activation;
Provide emergency response agencies with relevant information;
Guide and coordinate emergency communications
Conduct training and drills;
Audit and review programs regularly.

Every employee is expected to read, understand and follow the emergency procedures set forth in this plan to prevent or minimize the ill effects associated with an emergency. Since an emergency may be sudden and without warning, these procedures are designed to be flexible in order to accommodate contingencies of various type and magnitude. Summary:

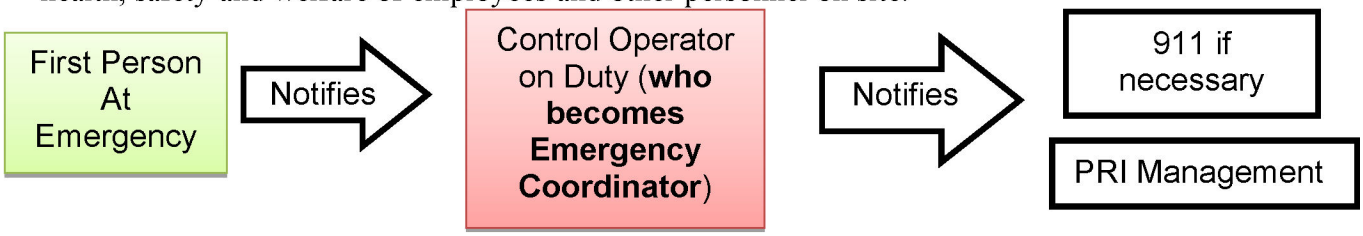
To provide simple directions as to who should do what and when in an emergency;

To know when and how to evacuate (and then return to workplace);

To transition to business recovery when required.

2.2 EMERGENCY NOTIFICATION PROCEDURE

Every PRI employee is responsible to report any incident that may threaten operations, the health, safety and welfare of employees and other personnel on site.



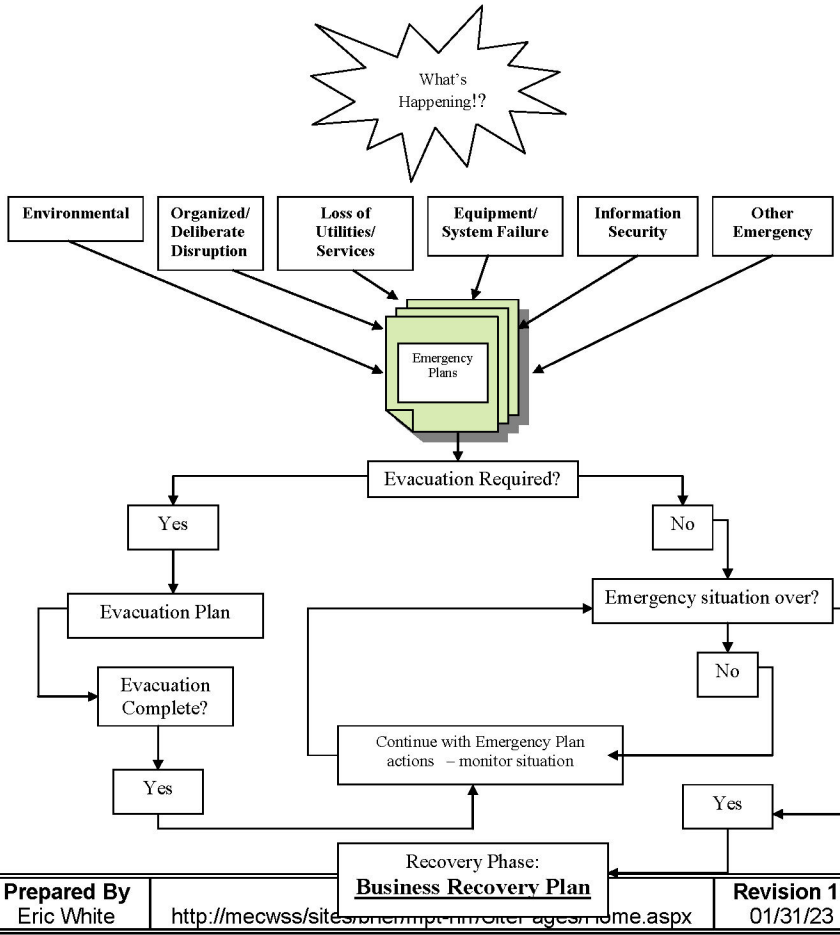
Upon notification of an emergency situation, the Control Operator on Duty shall act as **Emergency Coordinator (EC)** (the General Manager or the Operations & Maintenance Manager will take over upon arrival to the location).

The **Emergency Coordinator** shall immediately assess the situation and categorize the emergency as follows:

Fire
Earthquake
Severe weather (storms, flooding, etc.)
Environmental damage (spill or release)
Bomb threat
Intruder alert
'Other' emergency (theft, sabotage, compliance, cyber, refinery event, etc.)

Conduct emergency actions as appropriate.

2.3 Decision Logic Diagram – Emergency Actions



2.4 Chain of Command

In light of site-specific requirements, multiple coordination responsibilities may be tasked a single individual. Such tasking will be primarily based upon the number of employees available, and inherent site-specific knowledge that may be based upon the longevity of an individual's employment.

For the most part, plant personnel will assume coordinating positions and will be responsible for supplying information as appropriate to each team member.

2.5 Responsibilities

Coordinators at all levels will be knowledgeable about the Emergency Management Plan and related procedures as it applies to the whole concept and member specific requirements.

A team coordinator at any management level may elect to relinquish authority to an alternate in cases where the alternate possesses expertise in managing the specific emergency at hand.

Coordinators will appoint at least one substitute, provide a point of contact, list of responsibilities, and ensure the individual is available and capable to carry out assigned responsibilities. A coordinator may arbitrarily appoint local subordinate "Leaders" if available or required to provide assist and support preparation and implementation of duties. During an emergency event, all members will individually initiate and maintain a date and time activity log of events and situations that occur during implementation. (Who, what, where, when, why and how.)

A member of PRI Management will be responsible for all contact with media representatives, outside agency reporting and family communications.

On-Site Support Team

General Manager – Power Resources, Inc.

The General Manager, in consultation with the local Emergency Coordinator and other relevant parties, shall review the available information and circumstances of the incident in determining whether to declare the incident as an 'emergency' necessitating initiation of this Plan and BHER Business Continuity Plan.

The ultimate decision to declare an emergency and implement this Emergency Management Plan resides with the General Manager or his designee initiates a communication to the CEO indicating that the crisis management team is being activated. Only summary information will be available until the full scope of the incident can be determined. It will include:

Nature and scope of the incident or event

Issues related to life-safety, environmental, customer or stakeholder impacts and responses initiated

Contact information for the incident command center

Immediate resource needs requiring CEO attention

Proposed time and frequency of status updates

Subsequent status updates:

Provide updated status of incident or event

Describe action plan being implemented

Identify resource requests that require CEO approval or assistance

Emergency Coordinator (EC) – On-site Senior Manager

On notification of an incident the EC shall contact the relevant team members, and where necessary mobilize them to the proximity of the affected site to conduct an initial assessment of the nature and extent of the incident.

It is anticipated that the initial assessment and report (see appendix) for "Initial Incident Report") on the incident will be verbal via mobile phone with the General Manager providing in summary the following details as available:

- Nature and magnitude of incident;
- Anticipated casualties;
- Emergency and other authorities in attendance;

At all times company representatives will comply with instructions and guidance provided by the Emergency Services and other authorities. Personal safety, and the safety of others, is paramount and exposure to unnecessary risk shall be avoided.

During the plan execution phase, the EC coordinates the plan execution activities and provides critical communication link between the local Emergency Response Team and other business continuity teams.

Operations & Maintenance Manager

Will work closely with the EC to implement the Emergency Management Plan response activities in order to prevent loss of life, injuries, and to minimize damages. The appropriate manager will then organize and direct damage assessment and business recovery efforts.

Damage assessment personnel will collate timely, appropriate and adequate records of the incident. The scale and nature of the incident will inevitably influence the nature and detail of the information to be collected. The scope may be supplemented under guidance from the insurers, or their agent. However, such information is anticipated to include but not be limited to:

Photographic records and evident

Costs of contingency and recovery activities – direct and indirect

Schedules of items lost

Statements from witnesses

Schedules of salvaged items

The philosophy is to collate as much relevant information as possible rather than be prematurely restrictive or selective. Surplus or duplicate information will be filtered later.

Lead I&E Technician

Person who has the overall responsibility for determining the state of all critical IT components and controls. Will coordinate repair needs with corporate IT support.

Project Analyst

The Project Analyst will assist with directing all incoming and out-going communication to the General Manager and other team members. Will work with the Procurement Coordinator to acquire needed supplies, parts, contract labor. This individual will immediately begin securing needed critical employee supplies.

Senior Environmental Coordinator

Person who will work with the corporate environmental coordinators to ensure continued compliance with all environmental requirements. Will assist in other areas as needed during the event (safety, NERC).

2.6 Command Centers

The Command Center is the primary command and control location for emergency recovery activities. Command Center may be established in response to a potential threat/event or in response to the occurrence of a disastrous event.

The Command Center will provide a nucleus and staging point for both internal and external emergency services. It should be equipped with appropriate manpower and equipment to support all functions of the Crisis Management Team. Such equipment includes:

Communication equipment;

Emergency plans and procedures;

A log to record all actions taken during the crisis;

Necessary office equipment and supplies;

Appropriate maps and building plans.

Site Locations

In a "minor emergency" isolated to a single area or building and relatively distant from an operational center of control, the Command Center will be established at the main Plant Control Room.

In a "major emergency" isolated to a single area or building within close proximity to the main Control Room, the Command Center will be located within the plant Warehouse Office.

In a "major emergency" affecting the entire site area disrupting overall operations, the Command Center may be located off-site.

Alternative site – to be determined at time of event by EC. Possible locations include: TA Truck Stop, hotel conference room, 911 coordinator offices.

2.7 FIRE PREVENTION PLAN

Fire prevention measure are a critical part of the PRI plan, as such smoking is prohibited in all areas with the exception of designated smoking area in front of the main office building. Proper housekeeping and storage measures are to be maintained at all times.

The following is a list of the major workplace fire hazards and their proper handling and storage procedures, potential ignition sources and their control procedures, and the type of fire protection equipment or systems in place to control a fire involving them.

A list indicating the location of fire extinguishers throughout the facility is located in the Appendix of this Plan. The location of all water supply hydrants and monitors, fire hose cabinets, fire hoses, and foam carts are also listed in the Appendix.

WATER PLANT

The water plant contains various combustible materials. These materials are not stored near any heating source, lighting apparatus or equipment capable of igniting combustible materials of the type stored or handled in the Demin Bldg.

Portable fire extinguishers are located throughout the work areas, for the first line of fire defense.

LABORATORY AREA

A small laboratory is located inside the water plant building housing small amounts of flammable and combustible materials. No open flames or heating apparatus pose an immediate ignition factor in the lab area. The major hazard would be from a chemical spill resulting in an uncontrolled release of flammable or combustible liquids or vapors.

Portable fire extinguishers are the only means of fire suppression in the lab area.

GAS TURBINE BUILDING

There are two natural gas burning turbines located inside this building, with the major fire hazard being inside the turbine compartment.

Each gas turbine is equipped with a carbon dioxide extinguishing system for external fire protection. There are two halogenated extinguishing carts located at the northwest and southwest corners of the building. Portable extinguishers are also located throughout the gas turbine building. Additionally, each gas turbine generator (2) is cooled with hydrogen gas

which includes a carbon dioxide purge system that can be activated to vacate all hydrogen gas from the generator casing with the introduction of carbon dioxide.

STEAM TURBINE BUILDING

An above ground, 2,641-gallon lube oil reservoir is located on the first level of this three-level building. The steam turbine building is equipped with a fire sprinkler system, and portable hand operated fire extinguishers are located in the work areas of the steam turbine building.

MAINTENANCE SHOP

Major workplace hazards include assortments of containers ranging from aerosol cans to a 55-gallon drum of flammable cleaning solvent. Potential ignition sources include welding operations, heating and general maintenance. Additionally, the plants natural gas pressure control station is located just outside of the main shop overhead door. A combustion analyzer has been installed in the shop are to assist monitor the shop atmosphere to ensure there are no combustion hazards prior to using any spark producing equipment.

All heating and potential ignition sources will be controlled in the event of a fire or flammable liquid spill inside the maintenance shop. The employees in this work area will perform control actions.

The maintenance shop is protected by a fire sprinkler system, and portable handheld fire extinguishers are located in the shop area.

CONTROL ROOM

The major hazard in the control room is energized electrical equipment. This area contains non-emergency and emergency shutdown capabilities for the PRI facility, and is controlled by the control room operator.

Fire protection for the control room is provided by a halogenated extinguishing system and portable handheld fire extinguishers.

ENERGY MANAGEMENT ROOM

The energy management or computer room contains energized electrical equipment.

Like the control room it is protected with a halogenated extinguishing system and portable handheld fire extinguishers are close by inside the control room.

INSTRUMENTATION / MECHANICAL OFFICE

The instrumentation / mechanical maintenance office contains small amounts of flammable and combustible materials.
The instrumentation / mechanical office area is protected by a fire sprinkler system. Portable handheld extinguishers are also available.

COOLING TOWER

The major hazard is fire due to the combustible material of the cooling tower. The cooling tower is equipped with a deluge system for fire protection.

BULK HYDROGEN STORAGE SKID

The bulk hydrogen storage skid is located on the northeast corner of the property ad is used to supply hydrogen to the gas turbine generators. The skid is located in a low traffic area and covered to minimize contact with direct sunlight.

2.8 FACILITY EMERGENCY EQUIPMENT

INTERNAL COMMUNICATIONS AND ALARMS

Emergencies are reported to the control room operator via telephone, two-way radio, or by the Gai-tronics phone system.

EXTERNAL COMMUNICATIONS

Telephones are located throughout the facility.

Two-way radios are carried by operations personnel shift, and by other designated PRI employees. The radio provides for communication directly with the control room operator.

The external alarm system (Gai-tronics system) is used to warn personnel of various emergencies; i.e., fire, chemical spills, severe weather, or another emergency situation.

PORTABLE FIRE EXTINGUISHERS

Fire extinguishers are located at various points within all facility buildings.

WATER AVAILABILITY

Fire hydrants, monitors, fire hose cabinets and firehouses are located at various points throughout the plant. Locations are listed in the Appendix of this plan.

Trained PRI personnel will handle incipient fires. Area workers who have been trained in the use of fire extinguishers may assist in the handling of incipient fires. Big Spring Municipal Fire Department and the Howard County Volunteer Fire Department will respond to a major fire.

Portable fire extinguishers are designed for this purpose, but their successful use depends on the following conditions:

The extinguisher must be properly located and in good working condition.

The extinguisher must be properly rated for the Class of fire.

The fire must be discovered while still small enough for the extinguisher to be effective.

The fire must be discovered by a person ready, willing, and able to use the extinguisher.

****NOTE:** All portable fire extinguishers are rated to fight Class "A", "B", and "C" fires.

AFFF FOAM

Aqueous Film-Forming Foaming Agents, (AFFF), form water solution films on the surface of flammable hydrocarbon liquids.

PRI employees are not trained in firefighting and fire brigade procedures; therefore, it is understood that PRI personnel are NOT to use AFFF or the 1.5-inch fire hose in combating any flammable liquid fire.

The 1.5-inch hose lines, adapters, nozzles, and AFFF are to be used only to blanket moderate size spills of a flammable or combustible liquid, to prevent an ignition from occurring.

3. EMERGENCY RESPONSE

For this Plan to function properly, all response personnel must have an understanding of the general details of the incident. As soon as practical, the Control Room Operator should gather all relevant facts, assess the situation and develop a plan of action. The CRO should consider existing conditions, estimate future probabilities, review the details of the incident, and evaluate the level of response necessary to mitigate the incident. This evaluation should be weighed against the response capability of the facility. The following items should be considered when assessing the emergency:

- Time of emergency
- Location of the emergency
- Nature of the emergency
- Duration of the emergency
- Personnel exposures
- Equipment involved; collapse; exposure
- Root cause of the emergency
- Fire
- Weather conditions
- Potential hazard to life
- Additional assistance required / available
- Notification requirements, including those to off site and / or regulatory agencies

Protection of human health and safety is of paramount importance during any response. PRI property must be protected insofar as doing so will not increase risk to personnel. Finally, all

PRI Emergency Coordinators must make every attempt to minimize or eliminate threats to the environment.

The following procedures are written as guidelines. Every emergency is unique; as such no hard or fast rule exists. It is the obligation of the management of PRI, and those involved in emergency response, to be familiar with these guidelines and to refer to them, as needed, during the mitigation of any emergency incident.

The procedures below describe the actions to be taken by all responding personnel to potential situations at the PRI facility posing a real or potential threat to human health or safety and the environment.

3.1 EVACUATION

In the event of an emergency requiring a plant evacuation (including one due to a Refinery emergency situation; fire, H2S leak, etc.), the following procedure will be followed. It is important to gather and consider all pertinent information when determining whether or not a plant evacuation is needed and the best exit strategy. Things to consider; wind direction, location, exposure risk, safest gate route #1 or #4, assembly location, who should leave, and timing. Only in the event of imminent danger to personnel will the plant be put through an emergency shutdown. All other times the plant will continue to run until deemed unsafe and a controlled shut down will be performed.

PRI RESPONSE TO AN EVACUATION

CONTROL ROOM OPERATOR

Initiates the Gaitronics evacuation alarm and announces evacuation order for the affected area and / or buildings. Repeats the announcement. All on site personnel will report immediately to the control room for instructions on which gate to exit (#1 or #4).

If a full plant evacuation is ordered, the control room operator will commence the plant shut down in the safest, orderly way possible to both employees and plant equipment. The emergency shutdown of equipment will not be used unless the situation poses extreme danger and there is no time for a controlled shut down.

Note: Every employee shall evacuate the facility in the safest route possible if at any time they feel their lives are threatened or in jeopardy. However, it is critical that all employees be accounted for, so you should be sure the CRO or whomever is doing a head count knows your whereabouts. If the CRO and plant operator stay behind to secure the facility they should remain together at all times and remain in contact with lead person at evacuation point via two-way radio or cellular phone, and Delek Shift Supervisor (radio #33), Crude Unit Control Room or Safety Dept.

Will designate who remains on site if the emergency situation allows.

Will provide plant management with pertinent information necessary to make a decision regarding continued operations. This information will include, but is not limited to; length of time, gas analyzer readings, hazards, communications with Delek, and breathing air available.

Will don SCBA's if required due to a hazardous atmosphere (H2S, smoke).

If time does not permit management input, the CRO should use sound judgment in making a decision on continued operations. The plant should be secured in a manner that protects employees and equipment.

OUTSIDE OPERATORS

Will gather the H2S meter and a SCBA's and report to the Control Room.

PLANT PERSONNEL

Once the evacuation order is given, plant personnel will leave by the safest route determined in an orderly fashion.

Follow EC instructions.

PLANT MANAGEMENT

On evacuation, management ensures all personnel responsible for assisting in securing the plant are accounted for.

At the rallying area, determines accountability of all visitors, contractors, and vendors, (Use Visitor Log).

NOTE: The offsite assembly point is the east T.A. Truck Stop parking lot on Hwy 87 & I-20, unless otherwise specified during the emergency.

3.2 STANDARD PROCEDURES FOR SPILLS/LEAKS

Standard emergency response procedures have been developed for major potential hazards at the PRI facility. Major chemical hazards include acid, caustic, and jet fuel, all of which are stored in above ground storage tanks, (ASTs); hydrogen gas, water treatment chemicals, and various laboratory chemicals.

Note that the acid, caustic, and jet fuel ASTs, as well as the water treatment chemicals, have secondary containment dikes. These are advantageous as a built-in defensive response.

PRI personnel can respond defensively to an incident or release. This means they can control a release but cannot act aggressively to stop a release. Under OSHA regulations a higher level of training is necessary to respond aggressively.

In the event of an AST rupture, PRI must notify the Big Spring Municipal Fire Department and the Howard County Volunteer Fire Department for an aggressive response to stop the release. Once the release has been stopped, PRI's response personnel can take remedial action of neutralizing the spilled chemical and determining the proper disposal method.

Chemical releases from ASTs, or other storage that breach the containment dike can and must be controlled defensively by PRI's personnel, and controlled offensively by the Big Spring Municipal and Howard County Volunteer Fire Departments.

SPILL/ENVIRONMENTAL INCIDENT RESPONSE PROCEDURE

EMPLOYEE WHO IDENTIFIES A SPILL

The employee must inform the control room operator by two-radio or telephone, noting whether material is contained in the dike area, or has escaped the dike.

CONTROL ROOM OPERATOR

Obtains the following information from employee:

Name and location.
What the problem is.
Release contained in dike, or dike breached.
Estimate of amount released.
Anyone injured or contaminated.
Determine if employee is in a safe location, if not advice employee to move to another location and call back.
Advises employee help is on the way.

Notify Plant Management and give information on event.

Sound the Gaitronics Alarm and announce chemical release incident and location. Repeats announcement a minimum of two times.

Notifies other PRI employees.

Contacts the Big Spring Municipal and Howard County Fire Departments if instructed by plant management or if outside assistance is deemed necessary by CRO.

Note: When contacting local Howard County Emergency Services, (911), give the dispatcher the following information:

YOUR NAME
(432) 263-9000
Power Resources, Inc.
(enter through Gate #1 or #4) Fire trucks will use gate #4 or be escorted through refinery by DELEK personnel.

500 Refinery Road
Big Spring, TX 79720

Date, time, location spill or discharge:
Specific description of substance released/spilled; have MSDS available when you call.
Estimated quantity of release/spill.
Duration of release/spill (start and stop times if possible).
Name of surface water threatened by release/spill.
Source of release/spill.
Description of actual or potential water pollution or harmful impacts to the environment.
Actions already taken, are being taken, and will be taken to contain and respond to the release/spill.
Any known or anticipated health risks.
Name of Organizations/Agencies already contacted.
Any other information that may be significant to the response action.

In addition to the above-mentioned list, the TCEQ and others contacted might need some additional information not anticipated by this plan. The person reporting the spill should answer (to the best of his/her ability) any questions asked by the agency being reported to.

Take action to stop or minimize leak through operational controls (start a pump to transfer leaking product to another vessel, close valves from control room, etc.).

OUTSIDE OPERATOR

Responds to control room operator's call, and proceeds to the location of the emergency.

Dons appropriate personal protective equipment and advises control room if outside agencies are needed.

If the material is acid or caustic, verifies the neutralization tank level.

Will remain in contact with the control room via two-way radio and Gaitronics and will be directed by the Control Room Operator as needed.

Secure the area to prevent accidental entry (barricade tape, cones, etc.)

Take defensive measure to slow or stop the spill (ensure drains are closed or blocked, distribute spill socks/pads, etc.) At no point should the operator put himself in harm's way by entering immediate spill area or taking heroic efforts. Utilize spill containment kits located in downstairs air handling room or water plant.

Guide emergency response agencies as required.

MAINTENANCE PERSONNEL

1. Will report to the control room or spill area if directed by CRO for assistance as needed.

2. Assist as directed (spill kit, gather PPE, escort emergency services, etc.)

MANAGEMENT

Will assume EC responsibilities upon arrival.

Determine need for additional resources.

Conduct external reporting in accordance with agency requirements (see Simplified Guide in Control Room and work with Environmental Services.

Coordinate clean up responsibilities as necessary.

Conduct Internal reporting requirements as required (see below).

Reporting

These reporting guidelines below are to provide guidance on the internal monitoring, reporting, and recordkeeping of environmental spills within BHE Renewables. An **internally reportable spill** is a spill that has or may have the potential to harm human health or the environment. Internally reportable spills include, but are not limited to:

- Any externally reportable spill (done by management staff).
- Petroleum spills exceeding 1 gallon.
- Chemical spills exceeding 1 gallon.
- Spill of process water outside of the discharge paths covered by a National Pollutant Discharge Elimination System (NPDES) permit greater than 200 gallons.

NOTES:
1. A planned or managed release of any volume that is undertaken to repair/replace equipment or cannot be repaired immediately is not reportable. However, they must be preapproved by management. Such a release is usually contained in concrete or by other structures such that they do not contact the soil or natural waterways.
2. Small leaks must be reported to management and monitored at a routine frequency (depending on the rate of the leak). Any leak must have a work order in place for repair of the leak at the earliest opportunity to do so.

Mechanisms for reporting spills:

- Externally reportable spills are those exceeding the federal reportable quantities for the substances, or releases that are otherwise required to be reported by a permit condition or regulation. Externally reportable spills are communicated to regulatory, emergency response agencies and corporate Environmental Services Department listed in the

"Simplified Guide". Significant Event Reports which conduct root cause analysis and recommend corrective actions will be prepared following all official reporting.

- An internally reportable spill is any spill that meets the criteria above. A Significant Event Report will also be prepared for all internally reportable spills. Internally reportable spills must be reported to the Corporate Environmental Services Department.
- All environmental spills must be reported to the employee's manager, plant Environmental Health and Safety Coordinator and General Manager.

MITIGATION PLAN

Always evaluate leaks regardless of size and question what your response would be if leak or spill were larger.

Monitor weather conditions via internet and weather radio (what if water comes into contact with spill or leak, what if wind direction changes, etc.).

Be aware of additional hazards in the area (energized equipment, chemicals, etc.).

Get additional help as required.

Communications with CRO are critical.

Escort emergency response personnel from gate #1 or #4 to proper location.

Always don proper PPE.

Consult with SDS on proper handling, hazards and clean-up response.

Do not issue safe work permits for job task that put personnel at risk or near the vicinity of the spill or leak.

Properly secured adjacent areas from risk (close overhead doors, barricades, etc.).

3.3 MEDICAL EMERGENCY

CONTROL ROOM OPERATOR

Assumes control once notified of a medical emergency.

Will determine what type of assistance is needed based on communications from injured or persons in the area of injury.

Arranges for transportation to a medical facility if additional medical attention is needed. Contacts the Howard County 911 District to request an ambulance or arrange for plant transportation if medical emergency allows (minor type events). Notify emergency room or 911 dispatcher of injury and what emergency care procedures have been initiated by on site personnel.

Notify plant management and provides general description of employee injuries or illness, what procedures have been initiated, and current status.

Notifies the Delek Main Gate that an ambulance is in route to the plant and dispatch a PRI employee to the Delek Main Gate to lead the ambulance to the emergency location or if after hours request Delek personnel assistance (shift foreman, guard, etc.).

Assign other duties as required.

OUTSIDE OPERATORS

4. Will proceed to the accident site, remaining in contact with the control room via two-way radio and Gaitronics, to be directed by the Control Room Operator as needed. Provide frequent update communications so the CRO can determine additional assistance needs.

MAINTENANCE PERSONNEL

Will report to the control room or other area as directed by CRO for assistance as needed.

MANAGEMENT PERSONNEL

Will assume EC responsibilities upon arrival.

Make all notifications as necessary.

Accompany injured to emergency room if possible.

MITIGATION PLAN

Get additional help as required.

Provide escort from main gate to plant site.

Be aware of your surrounding and what caused the need for medical services.

Utilize all additional personnel resources (don't try to do it all yourself).

Make the person comfortable and do not move unless there is an immediate danger.

Communications with CRO is critical (what is happening, who, location, needs, etc.).

3.4 RESPONSE TO UNRESPONSIVE PERSONNEL

If the event is during normal business hours the CRO shall:

Attempt to contact the outside operator by radio, Gaitronics and by the telephone in the laboratory.

Sound the Gaitronics alarm.

Notify plant management of the emergency.

Dispatch all available personnel to conduct a thorough search.

Contact 911 if outside assistance is required

Notify Delek/PRI (Gate) Security that emergency services is in route.

Dispatch personnel to the Main Gate to lead emergency response personnel to the exact location

If the emergency occurs after normal business hours, or on a weekend, and the operator does not reply, the following shall be done by the CRO:

Notify the Delek Shift Supervisor (#33) or Crude Unit Control Room Operator – 263-9529

Notify the Delek/PRI (Gate) Security personnel on duty – 263-9272

Notify the PRI manager on call

3.5 FIRE RESPONSE RREQUIRING OUTSIDE ASSISTANCE

CONTROL ROOM OPERATOR

Obtains the following information from the employee:

Name and exact location of the fire?

The size of the fire?

Is anyone injured?

Can it be handled by on site personnel or is outside assistance required?

Determines if employee is in a safe location, if not advises employee to move to another location and call back.

Notify 911 and Delek Gate Guard

Sounds Gaitronics alarm system and announces the incident and the location. Repeats the announcement a minimum of two times.

Directs assistance to the operator or person reporting the emergency.

Have extra employees carry whatever emergency gear may be needed; fire extinguishers, SCBA's, 1st Aid Kits, etc.

Notifies Delek Shift Supervisor (#33) or Crude Unit control room of emergency.

Arrange for medical attention if needed.

Safety secure plant equipment as required.

Notify PRI management, and advises them of the situation.

Maintains constant communication between the control room and emergency location.

Complete or direct others to perform the below steps:
Roll call, send multiple escorts to gate, assign additional duties, evacuate non-essentials, etc.

OUTSIDE OPERATORS

Will remain in contact with the control room via two-way radio and Gaitronics, and will be directed by the CRO as needed (roll out hoses, direct emergency response agencies, take operational steps to prevent spreading or minimize damage, etc.).

MAINTENANCE PERSONNEL

Will report to the control room for a head count and assistance as needed or fire area as directed by CRO.

PLANT MANAGEMENT

Department managers will assume EC duties from CRO when arriving at plant site or emergency location.

MITIGATION PLAN

Know fire extinguisher locations prior to starting any work.

Ensure all flammable or combustible items are properly stored.

Always obtain a safe work permit (hot work) prior to using any spark producing tools.

Ensure lids are sealed on all trash containers.

Always have a fire watch that continues to monitor the area for a minimum of 30 minutes after work is complete.

At the first sign of a potential fire always get help on the way.

Strong housekeeping program.

3.6 TRANSFORMER ISOLATION FOR EVENT REQUIRING OUTSIDE ASSISTANCE

Note: due to transformers being in very close proximity to one another the ENTIRE plant is to be shutdown (not just the unit involved) and all flammable sources (natural gas at battery limits, do not vent hydrogen) isolated.

CONTROL ROOM OPERATOR

Obtains the following information from the employee:

Transformer name and exact location/problem?
The size of the fire/spill or issue?
Is anyone injured?
Is outside assistance required?
Determines if employee is in a safe location, if not advises employee to move to another location and call back. (**Note:** transformers type events cannot be controlled or handled by outside operator or other employees, so they need to stay far away from the immediate vicinity of the transformer event, due to risk of large explosion or over pressurization and potential for flying debris).

Notify 911 and Delek Gate Guard

Sounds Gaitronics alarm system and announces the incident and the location. Repeats the announcement a minimum of two times.

Directs all employees to maintain a safe distance and avoid being in the nearby vicinity.
Have extra employees carry whatever emergency gear may be needed; fire extinguishers, SCBA's, 1st Aid Kits, etc.

Notifies Delek Shift Supervisor (#33) or Crude Unit control room of emergency.

Arrange for medical attention if needed.

Safety secure plant equipment as required (see transformer isolation procedure on following pages).

Notify PRI management, and advises them of the situation.

Maintains constant communication between the control room and emergency location.

Complete or direct others to perform the below steps:
Roll call, send multiple escorts to gate, assign additional duties, evacuate non-essentials, etc.
Provide company radio to fire department liaison.
Isolate or block off roadways to prevent passage by non-emergency involved vehicles.

OUTSIDE OPERATORS

Will remain in contact with the control room via two-way radio and Gaitronics and will be directed by the CRO as needed (roll out hoses, direct emergency response agencies, follow CRO instructions, block of roadway with safety cones).
Assist with isolating equipment as directed by CRO.

Will remain a safe distance from the transformer involved in the event due to explosion risk and potential for flying debris.

MAINTENANCE PERSONNEL

Will report to the control room for a head count and assistance as needed and directed by CRO.

PLANT MANAGEMENT

Department managers will assume EC duties from CRO when arriving at plant site or emergency location.

MITIGATION PLAN

Know fire extinguisher locations prior to starting any work.

Ensure all flammable or combustible items are properly stored.

Always obtain a safe work permit (hot work) prior to using any spark producing tools.

Always have a fire watch that continues to monitor the area for a minimum of 30 minutes after work is complete.

At the first sign of a potential fire or issue always get help on the way.

Strong housekeeping program.

Follow transformer testing protocol.

Ensure proper fan operations.

Conduct preventative maintenance in accordance with industry standards.

To isolate GT-1 and GT-2 transformers:

GT 1 - T-1/T-4

T-1 – **Open** breakers **3040** and **3050** from the Cogen Panel, unless unit has tripped offline.

Open 52J from the Cogen Panel

Open T-1 fan breaker – located in **MCC 2A** – Cubicle **#3FDB**

Isolating **T-1** will isolate **T-4**.

GT 2 - T-2 /T5

T-2 – **Open** breakers **3020** and **3030** from the Cogen Panel, unless unit has tripped offline.

Open 52K from the Cogen Panel

Open T-2 fan break – located in **MCC 5A** – Cubicle # - **4FDB**

Isolating **T-2** will isolate **T-5**.

SPECIAL NOTE: PLANT UTILITIES WILL NEED TO BE FED FROM THE BLACKSTART AND MAINTENANCE GENERATOR, OR 52U, IN ORDER TO HAVE POWER FOR THE PLANT.

To Isolate the Steam Turbine transformer:

STG - T-3

T-3 – **Open** breakers **3010** and **3020** from the Cogen Panel

- **Open T-3** fan breaker– located in **MCC 2A** – Cubicle # - **4FDB**

Stop Maintenance Generator if it is running. This will be accomplished by closing 52U and allowing the Maintenance Generator to shut down on its own.

To isolate T-6 and T-7 transformers:

The following instructions are for the manual opening of breakers associated with T-6 and T-7. The Maintenance Generator should be shut down immediately, as well as the Blackstart if it is running. **Do not close 52U.**

T-6 and T-7 are both equipped with 110-volt fans, as well as heaters. The breakers for the transformer fans and heaters will need to be opened to shut off power. **The breakers for T-6 and T-7 fans are located in Lighting Panel F breaker panel** located on the **east wall** of the Main MCC.

1. **T-6 fan breaker is # 6**
2. **T-7 fan breaker is #8**
3. **T-6 heater breaker is #14**
4. **T-7 heater breaker is #16.**

Breakers 6, 8, 14 and 16 are labeled in Lighting Panel F

T-6

- When **52J** is **Opened** or trips **Open**, all power from **T-4** to **T-6** will cease.
- **Open T-6** fan breaker and heat breakers – located in **Lighting Panel F:**
  - **T-6 fan breaker is # 6**
  - **T-6 heater breaker is #14**

T-7

- When **52K** is **Opened** or trips **Open**, all power from **T-5** to **T-7** will cease.
- **Open T-7** fan breaker and heat breakers – located in **Lighting Panel F:**
  - **T-7** fan breaker is **# 8**
  - **T-7 heater breaker is #116**

It is also possible to isolateT-6 and T-7 from the Main MCC if for some reason it cannot be achieved from the Control Room.

Isolating incoming power (4160 volt) to **T-6** or **T-7**:

Open the following breakers by pulling the black knob located at the bottom of the breaker panel. Breaker panels are located on the **west** side of the 4160 breaker panel in the Main MCC.

T-6 4160 v. breaker is located on the **north** end by the breaker for Circulating Water Pump C

T-7 4160 v. breaker is located on the **south** end by the breaker for Circulating Water Pump B

Open breaker after knob.

Pull this knob first to trip

TO TRIP THE BREAKER, PULL THE BOTTOM KNOB OUT, THEN OPEN THE BREAKER HANDLE ABOVE THE KNOB

Isolating outgoing power (480 volt) from **T-6** or **T-7** can be achieved by opening breaker 52B or 52G. This breaker panel is located by the door leading to the MCC Battery Room. The breakers for **52B** and **52G** have large labels identifying them.

Open the following :

52B for T-6, 52G for T-7

Shut down the Maintenance Generator

To open 52B or 52G do the following:

Push the RED TRIP switch. It is labeled PUSH TO TRIP

T-8

The following instructions are for the manual opening of breakers associated with T-8.
Voltage coming into T-8 from Oncor is 12.5 Kva, and is stepped down to 4160 volts.
To kill power to the transformer manually:

Open 4160 breaker 52U in the Main MCC – located on the west side of the 4160 panel

Oncor will be required on site to remove fuses from their transmission line.

ONCOR Transmission Dispatcher 214-743-6900

To isolate the auto transformers AT-1 or AT-2;
AT1 and AT2

Oncor will be required to open up their side of their switchyard to isolate AT-1 or AT-2 from back feeding.
To isolate AT-1 or AT-2, Power Resources will need to do the following:

Open up the associated breakers feeding AT-1 or AT-2. Open the following breakers from the Cogen Panel unless already tripped, (for the correct unit):

3010 and 3050 – for AT-1
3030 and 3040 – for AT-2

Open the 138 kv Switchyard breaker in the Main MCC, (by the ASCO Switch) – DO THIS LAST. This breaker is located due south of the ASCO switch. If you are looking at the ASCO switch it will be to the left and is labeled:

225A BREAKER 138KV SWITCHYARD

ONCOR Transmission Dispatcher 214-743-6900

SPECIAL NOTE:

If the plant is black, (all turbines offline, and no power coming in from 52U), the above procedure does not have to be done with the exception of isolating AT-1 and AT-2 which will require assistance from ONCOR.

3.7 RESPONSE TO A NATURAL GAS LEAK

In the event of a natural gas leak, PRI personnel should immediately move to an upwind location from the leak and **immediately** notify the Control Room Operator of the exact nature and location of the leak. It will be up to the Outside Operator to ascertain the situation during the initial stages of the emergency as to which valves need to be closed.

PLANT PERSONNEL

Will report immediately to the control room, unless otherwise specified during the initial announcement.

Will go about task assigned by Plant Management, or the CRO.

If an evacuation order is given, plant personnel will leave, by what is determined to be the safest route, in an orderly fashion in accordance with plant evacuation procedures.

CONTROL ROOM OPERATOR

The CRO will alert plant personnel and management via the Gaitronics and two-way radio. The CRO will need to announce that all Hot Work Permits and Safe Work Permits are immediately cancelled. The CRO will also announce the assembly point for all personnel if it is another location other than the control room. Wind direction will play a critical part in determining where the initial assembly area may be located.

The following valves will isolate the entire plant or portions of the plant.

AY364A – Isolates the plant at the battery limits.
PIC 358 – Isolates the plant at the battery limits.
HV 660 – Isolates GT 1
HV 662 – Isolates GT 2
PIC 351 - Isolates the system downstream of the natural gas filters.

If the leak is of a nature that requires an emergency shutdown, the CRO will close the natural gas isolation valve AY364A from the IA.

Will notify the local 911 District if situation warrants outside assistance by Emergency Response Personnel.

The CRO will notify the Delek Shift Supervisor (#33) or Crude Unit Control Room, Oneok Westar, and EDF Energy Services of the leak and what actions are being taken.

Will determine need to evacuate and personnel needs.

Will maintain contact with plant management and Delek Safety, via telephone and two-way radio, for the duration of the emergency.

The CRO and Outside Operator will remain together at all times.

If time does not permit management input, the CRO should use sound judgment in making a decision on continued operations. The plant should be secured in a manner that protects employees and equipment.

OUTSIDE OPERATOR(s)

Will maintain continuous contact with the control room.

Will immediately attempt to make a determination of how bad the leak is without endangering themselves. **Under no circumstances is anyone to enter the gas cloud**.

Will monitor explosive limits with the portable gas meter and continually report the situation to the CRO.

Will continually monitor wind direction and estimate the wind speed.

PLANT MANAGEMENT

If on-site will assume EC responsibilities.

MITIGATION PLAN

Get additional help as required.

Revoke all hot work permits.

Be aware of weather conditions (wind direction).

Report all leaks regardless of size.

Isolate leak as soon as possible.

Never enter the vapor cloud.

Stay alert for other potential ignition sources and secure as necessary (motors, lights, etc.).

Trust your sense of smell (if you think you smell a leak you probably do).

Utilize all additional personnel resources (don't try to do it all yourself).

Communications with CRO is critical (what is happening, who, location, needs, etc.).

Ensure fire protection/detection systems are maintain for ready operations

Know where nearest fire protection equipment is located (extinguisher, hydrant, etc.).

Strong housekeeping program.

3.8 WEATHER EVENT (Extreme weather, tornado, electrical storm) Shelter in Place

In the event of extreme weather, PRI personnel should immediately move to a safest place and **immediately** notify the Control Room Operator of the exact nature of the event. It will be up to the exposed individual to ascertain the situation during the initial stages of the emergency and take immediate precautions to remain safe.

PLANT PERSONNEL

Will report immediately to the control room, unless otherwise specified during the initial announcement, or if in doing so they are exposing themselves to potential injury.

Will go about task assigned by Plant Management, or the CRO.

If an evacuation order is given, plant personnel will leave, by what is determined to be the safest route, in an orderly fashion in accordance with plant evacuation procedures.

If sheltering in-place is required, plant personnel will move to the closest building with interior walls and remain until safe to exit. PRI has identified two locations as the best sites for sheltering in place if required and depending upon your location at the time of the event (control room building or water plant).

CONTROL ROOM OPERATOR

The CRO will alert plant personnel and management via the Gaitronics and two-way radio. The CRO will need to announce that all Hot Work Permits and Safe Work Permits are immediately cancelled. The CRO will also announce the assembly point for all personnel if it is another location other than the control room.

Secure plant as deemed necessary for employee/equipment protection.

The following valves will isolate the entire plant or portions of the plant.

AY364A – Isolates the plant at the battery limits.
PIC 358 – Isolates the plant at the battery limits.
HV 660 – Isolates GT 1
HV 662 – Isolates GT 2
PIC 351 - Isolates the system downstream of the natural gas filters.

Determine site evacuation needs.

Will notify the local 911 District if situation warrants outside assistance by Emergency Response Personnel.

If time does not permit management input, the CRO should use sound judgment in making a decision on continued operations. The plant should be secured in a manner that protects employees and equipment.

Monitor weather radio broadcast.

OUTSIDE OPERATOR(s)

Will maintain continuous contact with the control room operator. Providing information on weather conditions, shelter location, and assistance required.

PLANT MANAGEMENT

If on-site will assume EC responsibilities.

MITIGATION PLAN

Shelter in interior walled rooms with no windows.

Inform others of your location.

Secure all items that could become airborne.

Remain in constant communications with other plant personnel.

3.9 SECURITY CONTINGENCY PLAN

PRI is an independent power producer located in Big Spring, Texas. PRI is an energy supplier with multiple sources of vulnerability for manmade disasters as natural gas is piped from the ONEOK pipeline to the site, electrical power is transmitted on the Oncor Electric grid, and PRI operates turbines, generators and steam boilers under high temperatures and pressures. The site, furthermore, could be a target for vandalism and theft. This Security Program defines the strategy for managing security as a **prevention measure** as well as applying guidelines from the United States Office of Homeland Security and United States Department of Transportation for counter terrorism.

This plan is designed to help PRI identify and respond to a significant future event that may or may not happen. Recognizing and reporting events or potential events is critical to the success of these plans. Every employee plays a key role in observing plant activities and reporting abnormal observations, controlling plant access and controlling access to cyber type operating equipment that others may want to destroy or control in order to harm others. The management team should refer to the corporate **Cyber Security Incident Response Plan** for additional detail and guidance on potential cyber security incidents, classification and responses.

United States Office of Homeland Security

The following threat conditions and Protective Measures are cumulative. Each successive level assumes that PRI is already implementing the protective measures associated with the preceding threat conditions, as appropriate. The following information provides details on the specific threat levels. When there is NO NTAS threat advisory, the following shall be done:

This condition is declared when there is a little or no low risk of terrorist attacks. The following measures should be maintained at all times as standard operating procedures:

- Control Operators should verify the identity of all employees and visitors (by using the lobby phone) and control access to the facilities at all times. The Control Operator shall be aware of any contractors working for PRI (control room sign in log).

- Ensure that existing security measures are in place and functioning:
  - All facilities perimeter fencing and gates
  - Communication to the Delek main gate is maintained
  - All area gates and doors locked
  - Cameras
  - Lighting

- Ensure that emergency communication maintains redundancy for both hardware and means to contact law enforcement agencies.

- Develop terrorism and security awareness. Provide annual training to employees on security standards and procedures. Provide additional training as needed.

- All personnel should report the presence of unknown personnel, unidentified vehicles, vehicles that are unusual, abandoned parcels or packages, and other suspicious activities. Be alert to vehicles parked for an unusual length of time near the PRI property.

- All employees, visitors and contractors should be aware of alarms, evacuation routes and evacuation areas. Emergency shutdown procedures shall be maintained in the Control Room.

1. Ensure that PRI emergency response can be mobilized and review emergency and security plans and procedures. Test security and emergency communication procedures and protocols annually at a minimum.

2. Inspect and repair if necessary, all perimeter fencing. Review all outstanding maintenance and capital project work that could affect the security of PRI.

3. Review all operation plans, personnel assignments, and logistical requirements that pertain to implementing higher threat conditions.

NTAS ELEVATED THREAT ALERT

An Elevated Condition is declared by NTAS when there is a credible risk of terrorist attacks. In addition to the measures listed previously, the following measures should be implemented:

Ensure that all perimeter gates are closed and locked. The Main Gate shall remain in remote operation. Inspect perimeter fences regularly. Ensure that all security systems are functioning and available for use during weekends and holidays.

Confirm that every visitor is expected and has a need to be at PRI. No unknown visitors shall be permitted inside the perimeter fence without an escort.

Secure all buildings and storage areas not in regular use.

Inspect on a more regular frequency than usual basis the interior and exterior of the plant, especially the area around all exterior above ground storage tanks.

Identify areas where explosive devices could be hidden.

Encourage that all personal, secure personal and company vehicles.

Do not open suspicious packages. Inspect all mail and packages coming into PRI.

Review communications procedures and backup plans with all employees.

Check to ensure that all telephones and two-way radios are in place and operational.

Increase the frequency of warnings required by lower threat conditions and inform all employees of additional threat information as available.

Review operation plans, personnel safety, security details, and logistical requirements that pertain to implementing increased security levels.

Confirm the availability of security resources that can assist with round-the-clock coverage of critical facilities.

NTAS IMINENT THREAT ALERT

An Imminent Threat Alert is declared when there is a warning of a credible, specific, and impending terrorist threat against the United States

In addition to the measures listed previously, the following measures should be implemented:

a. Continue locking all gates and requiring contact from the Delek guard shack at the main gate prior to entry. Randomly spot-check the contents of vehicles entering the facility.

b. During weekends, holidays and after hours ensure all gates, office doors, etc. remained locked. Employees or scheduled contractors are only authorized access to PRI.

c. Limit PRI access to visitors and contractors who have a legitimate and verifiable need to enter the facility. Require positive identification of all personnel entering the facility with NO EXCEPTIONS.

d. UPS/FedEx drivers are permitted to enter only after a plant employee has verified their identity. A plant employee must receive deliveries at the Main Gate if a 'substitute' driver is making the delivery.

e. Assign Plant personnel to assist with security duties by patrolling the area regularly and reporting to the General Manager as issues surface.

f. Survey the surrounding area to determine if activities near PRI (Delek) could create hazards that could affect PRI.

g. Advise the Howard County Sheriff and Texas Department of Public Safety Troopers that the alert level is at Imminent and advise them of the security measures being employed. Request an increase in the frequency of their patrols around PRI and report any suspicious behavior to PRI directly.

h. Cancel or delay all non-vital facility work conducted by outside contractors.

i. Employees working at remote locations shall be instructed to check in periodically.

j. Increase patrolling of the Plant at night by Operators. Check all security systems such as lighting to ensure that they are functioning. Increase lighting levels, as appropriate, to address the changing security needs.

k. Caution employees not to talk to outsiders concerning their facility or its operations.

1. PREVENTION MEASURES

The application of controlling unauthorized access to the facility and its equipment is a critical step in preventing sabotage type events. These procedures are designed to assist in combatting cyber-attacks, theft, potential damage to plant equipment and harm to plant personnel. One key prevention method is physical security which is accomplished by controlling and limiting access to key areas through locked doors (doors are to be locked and never propped open and by controlling combinations and updating as necessary).

DCS CONTROLS and COMPANY NETWORK/CYBER SECURITY

Company Computers- never leave unattended without logging off or locking office door.

Access - privileges to networks, and other sites (ERCOT, NERC, TRE, EPA, etc.) shall be terminated immediately for employees exiting the company to prevent access. Manager shall

notify corporate IT, Human Resources, complete Exit Check Sheet and terminate all access privileges previously granted to perform company business.

Password – must be protected and not shared. If you write your password down it should be protected like you do other personal information and passwords should be periodically changed (not posted in plain view to others).

Software Policies- All application software used on the DCS/Network is to be licensed to the company. No personal or unauthorized software is to be run on the DCS. This includes storage disc and thumb drives. Never disable anti-virus or firewall software.

Social Engineering – Try to extract information over the phone, via e-mail or in person. Some common tactics include claiming to be someone they are not (IT, company vice-president, officer). This may include using company employee names, acting as IT personnel, or sending an e-mail from a legitimate sounding company directing you to provide them with control system data. Below are ways to deal with Social Engineering:

If the person claims to be internal, ask for their phone number, employee number, and then call to verify the number.
Ask who authorized the request, and then call the person to verify.
Do not be intimidated by someone claiming to be a high-level person
Do not be afraid to say no or to question the request
Contact Management for assistance on how to respond.

Malware- To prevent malware from getting onto the DCS/Network, do not use these devices (floppies, CD's, DVD'S, Pin drives, or flash drives or sticks) unless you explicitly know the content and approved by management. Uses of these devices are prohibited and shall only be used with specific, individual/devices and management approval.

*If there appears to be a loss of plant control telemetry the cable can be unplugged from the wall jack in the energy management room. Marked with R**ed Danger Tag** on east wall. Information Technology and Management must be notified immediately.*

If you suspect a cyber security event (ransomware, loss of files, loss of control, un-normal behavior, etc.) has occurred on the network the following steps shall be taken immediately:

1. *Shutdown the device*
2. *Unplug network connection (server marked in EM room; 2-connections marked)*
3. *Notify IT immediately (1-515-242-4357) Option #9*
4. *Notify management*
5. *Do not re-start without IT approval*
6. *Notify other plant employees to be aware of possible event*
7. *Determine notification requirement per NERC guidelines and BHER BCP*

REMOTE ACCESS

Remote access is prohibited except under the below conditions.

Phone Line – No permanent phone lines are to be connected to the DCS. At times it may be necessary to temporarily use phone line connections for diagnostic purposes. Under these circumstances the following steps are to be followed:

Must be approved by Management.

Verification of person requesting dial-in (person must be known, or a call back is required to verify authenticity).

Call back is required to verify line disconnect.

Interlock defeat shall be completed by Control Room Operator.

Additional protective measures include:

Controlling or limiting access to locations that contain printers, routers, control systems, protective relays and other plant equipment used for controlling plant operating equipment through the use of locks.

PRI employees shall limit access to the main building by locking exterior doors and gates. Visitors are required to announce their presence at the front entrance and will only be allowed to enter after confirmation from a PRI employee that the visitor is planned. PRI employees shall attempt to pre-schedule all visitors and inform CRO of site visit.

The CRO will then unlock the door and a PRI employee will meet them upon entering the building.

Visitors will not be left unattended within the main building or allowed to wander the plant site un-attended.

All visitors must sign in and sign out on the visitor log (complete all fields).

Visitors are not allowed to wait in the control room, they will be escorted to the break room.

Computer monitors should be kept clear of sensitive information and confidential information kept concealed in folder or behind locked doors when un-attended.

Do not open emails with attachments from unknown individuals or companies. If you are unsure about attachments utilize the "Report Phishing" Icon on your email tool bar.

*Be aware of Phishing Emails, Executive Spoofing - look for mis-spelled words(unprofessional), use your cursor to hover over the email address to confirm email address, uncommon file names (HTML), utilizing executive names, pay attention to emails with ****STOP. THINK. External Email**** labels which are warnings that the email you are receiving is being sent from an external non-company source.*

RESPONSIBILITIES

For Transient Cyber Assets and Removable Media managed by PRI, personnel shall ensure the threat of Malicious Code is mitigated prior to connection to PRI's Cyber Systems.

For Transient Cyber Assets and Removable Media managed by third parties, PRI personnel shall ensure the threat of Malicious Code is mitigated prior to connection to PRI's Cyber System via On-Demand Device Acceptance or Advance Programmatic Acceptance. Corporate IT shall be utilized to assist with this process.

PRI shall ensure the appropriate documentation is maintained to demonstrate the mitigation of Malicious Code introduction.

DETAILS

a. For all Transient Cyber Assets (TCAs) and Removable Media (RM) managed by PRI, PRI personnel shall:

Identify and catalog all TCAs and RM.

Ensure antivirus software is installed on the TCA, that antivirus software definitions remain current, and antivirus scans (or active scans) are scheduled to be performed on a regular basis.

Limit the number of applications allowed to be installed on the TCA as necessary via an Application Whitelisting methodology.

b. On-Demand Device Acceptance – Prior to allowing any TCA or RM (owned by PRI or a third party) to be connected to plant Cyber Systems, PRI personnel shall verify one or more of the following via the completion of the On-Demand Device Acceptance Form (see ICP-Gov-10):

Note: If during device verification, PRI personnel determine additional mitigation actions are necessary to ensure cyber security, PRI personnel may implement additional mitigation activities (with the third party's support) or disapprove the device for use at the facility at their discretion.

If antivirus software is installed and implemented on the device, antivirus software definitions are current, and antivirus scans (or active scans) have been performed on the device recently (as appropriate). This may include ensuring that antivirus scans are performed at the time of inspection.

For any discovered Malicious Code, PRI personnel shall ensure all threats have been eliminated prior to connection to a Cyber System.

If application Whitelisting is implemented on the device.

If adequate System Hardening is implemented on the device.

If a Live Operating System (or software) is implemented on the media and modifications to the code are restricted through the use of Read-Only and Executable Only controls.

If any external wireless connectivity (hotspot, Wi-Fi, etc.) is disabled on the device while on site.

If the device is incapable of using methods that mitigate the introduction of malicious code (proprietary hand-held devices, etc.).

If an alternative method to reduce the risk of Malicious Code is implemented on the device. If so, PRI personnel shall ensure the details of the alternative method are recorded on the On-Demand Device Acceptance Form.

For any Removable Media (RM), if antivirus scans (or active scans) have been performed on the Removable Media recently (as appropriate). This may include ensuring that antivirus scans are performed at the time of inspection.

For any discovered Malicious Code, PRI personnel shall ensure all threats have been eliminated prior to connection to a Cyber System.

> Note: If antivirus scans are performed by PRI personnel using PRI Cyber Assets, the Cyber Asset must not be part of the Power Resources' Cyber System (SCADA, DCS, EMS, etc).

Advance Programmatic Acceptance – To allow a specified third-party organization to become exempt from On-Demand Device Acceptance, PRI personnel may review the third party's cyber security policies, procedures, background check requirements and/or documentation to determine if their implemented processes are acceptable. PRI personnel shall verify one or more of the following processes is enacted by the third party via the completion of the Advance Programmatic Acceptance Form (ICP Gov-10).

If antivirus software is installed and implemented on their devices, antivirus software definitions remain current, and antivirus scans (or active scans) are performed on the devices regularly.

For any discovered Malicious Code, the third party ensures all threats have been eliminated prior to connection to a BES Cyber System.

If application Whitelisting practices are implemented on their devices.

If adequate System Hardening practices are implemented on their devices.

If a Live Operating System (or software) is implemented on their media and modifications to the code are restricted through the use of Read-Only and Executable Only controls.

If their devices are incapable of using methods that mitigate the introduction of malicious code (proprietary hand-held devices, etc.).

If an alternative method to reduce the risk of Malicious Code is implemented on their devices. Power Resources personnel shall ensure the details of the alternative method are recorded on the Advance Programmatic Acceptance Form.

For any Removable Media (RM), if antivirus scans (or active scans) are performed on the Removable Media regularly.

For any discovered Malicious Code, the third party ensures all threats have been eliminated prior to connection to a BES Cyber System.

Ultimately, we need to comply with guidance documents and directions from corporate IT. Always consult for guidance on risks, acceptable equipment usage and proper implementation methods. Help Desk should be contacted for guidance (515) 242-4357.

RECORDS

Power Resources shall ensure all documentation, procedures, logs, and compliance records are retained for a period of at least 7 years unless directed by its General Manager to retain

specific evidence for a longer period of time as part of an investigation or an open compliance violation.

PRI shall keep the last audit records, and all requested and submitted subsequent audit records.

Most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, and therefore Transient Cyber Assets and Removable Media are needed to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. Transient Cyber Assets and Removable Media are a potential means for cyber-attack. To protect the Cyber Assets PRI utilizes this plan to mitigate the risk of malicious code introduction to Cyber Systems from Transient Cyber Assets and Removable Media. The approach of defining the plan provides a process that are supportable within PRI's organization and in alignment with its change management processes.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may interface with or run applications that support Cyber Systems and is capable of transmitting executable code to Cyber Assets.

Examples of these temporarily connected devices include, but are not limited to:

Diagnostic test equipment;

Equipment used for BES Cyber System maintenance; or

Equipment used for BES Cyber System configuration.

PRI strives to avoid implementing security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of Cyber Assets.

For Transient Cyber Assets and Removable Media that are connected to Cyber Systems, PRIs must be aware of the differing levels of requirements and manage these assets under the program that matches the highest impact level to which they will connect.

The following is additional methods to mitigate the introduction of malicious code.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to update the signatures or patterns and scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the risk that malicious software could execute on the Transient Cyber Asset and impact the Cyber Asset or Cyber System.
- When using methods other than those listed, PRI needs to document how the other method(s) meet the objective of mitigating the risk of the introduction of malicious code.

If malicious code is discovered on the Transient Cyber Asset, it must be mitigated prior to connection to a Cyber System to prevent the malicious code from being introduced into the Cyber System. PRI may choose to not connect the Transient Cyber Asset to a Cyber System to prevent the malicious code from being introduced into the Cyber System. PRI should also consider whether the detected malicious code is a Cyber Security Incident.

SABOTAGE AWARENESS

PRI continuously monitors the Department of Homeland Security's (DHS) National Threat System and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) Current Threat Levels for elevated conditions.

SABOTAGE RECOGNITON

Sabotage is generally considered motivated behavior intended to create disruptions in a work or social environment. It is often the work of enemy agents or disgruntled employees and can be the work of a single saboteur or a group. Sabotage generally includes destruction of property or obstruction of normal operations. Sabotage attempts are often tied to disruptive events in the workplace such as possible threats to an industry or region and labor unrest. Civil unrest can result in attempted sabotage where a specific group's cause may conflict with organizational, governmental or industry goals.

Sabotage events can be placed into one of three categories: Cyber, Physical, and Operational. This procedure defines PRI's procedures dealing with all of these incidents. Examples of each of these three categories will be discussed below:

There are **known** or confirmed sabotage events where there is no question that a deliberate act has been committed to disrupt operations. Some of the obvious may include:

- Tampering with transmission equipment / poles (Physical)
- Disrupting the supply of fuel to power a generation plant (Physical, Cyber)
- Disrupting operations by false or real threats (bomb, fire, etc.) (Operational)
- Causing intentional failure of critical machinery or systems (Physical)
- Deliberate cut of fiber optic lines supporting SCADA control or other essential communications (Physical)
- Disrupting or freezing control system by introduction of malware or virus (Cyber)

Or, events can be **suspected to be** sabotage and can look like every day abnormal operations such as:

- Loss of a line or major piece of equipment (Physical, Cyber)
- Trip of a major unit (Operational, Cyber)
- Relay mis-operations (Operational, Cyber)
- Loss of RTU communication circuitry (Operational, Cyber)

Suspected to be sabotage events should be investigated after the operational issues have been resolved to confirm the likelihood of sabotage.

If an incident has occurred and you can identify that the root cause of the event is sabotage, it is important to report the incident in the shortest time frame possible. Reporting of events is required when the cause is **known** or **suspected to be** of malicious origin. Reporting of events where the cause is uncertain, or unknown is mandatory.

Reporting outside of plant management is not necessary if it is considered highly probable that the cause is **NOT** of malicious origin - or until such time that a reportable cause is established.

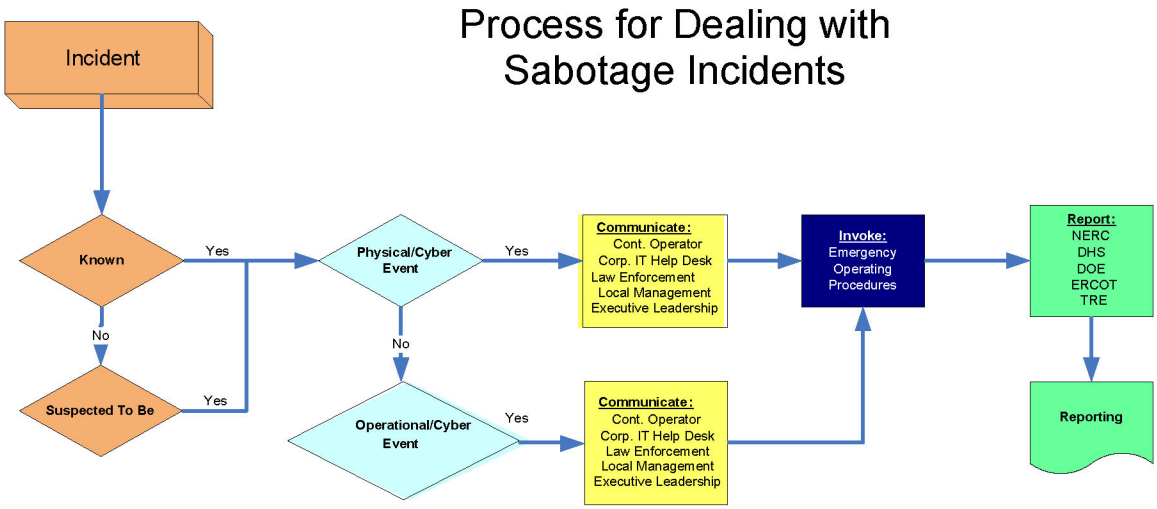
It is also important to understand some signs of **possible** sabotage threats. They may include:

- A large volume of unauthorized access attempts to critical facility
- Intelligence gathering – unauthorized people requesting information about operations, software, telecommunications, etc.
- Unauthorized physical surveillance
- Internal verbal or written threats to security, software, operations, or facilities by disgruntled employee and/or contractors
- External verbal or written threats to security, software, operations, or facilities by any person not directly associated with the Company
- Minor acts of vandalism at transmission substations, distribution substations supporting critical government agencies or distribution substations supporting power system operation facilities
- A series of minor acts of vandalism at numerous transmissions substations (within one control area or reported across interconnections) within a short period of time that demonstrate a possible plan to disrupt the Bulk Electric System

In today's post 9/11 world, recognition of sabotage events is crucial to the Company's efforts to protect the Bulk Electric System. If any of the above situations occur it is important to bring this to the attention of the General Manager and all operating personnel.

SABOTAGE RESPONSE

At PRI, the sabotage response process follows a well-defined path of recognition, evaluation, communication, action, and reporting. The following process diagram represents the decisions and actions that will be taken upon discovery of a sabotage event within the responsible entities:



Recognize Evaluate Communicate Act Report

Recognize – PRI recognizes the incident as a known sabotage event, suspected to be sabotage incident, or a warning sign that a possible sabotage event may take place.

Evaluate – PRI evaluates the event to determine the business area(s)/operating units that are impacted by the sabotage incident.

Communicate – all impacted business units/operating personnel, interconnections, and law enforcement need to be made aware of the sabotage event and the actions that are being taken by PRI. ***Contact these entities/agencies immediately!***

Act - each impacted business area should proceed to action to invoke specific business unit emergency operating procedures or portions of those operating procedures that are appropriate to the type of sabotage event that has occurred.

Report – After the immediate threat has been dealt with by PRI, it is necessary to supply a formal written report to NERC, ERCOT, DOE, and DHS specifying the details of the incident and any post incident actions that need to be followed up on. ***Follow up with a written report!***

NOTE: At any time during an event or suspected event, management or the on shift Control Operator can order the shutdown of equipment and evacuation if, in his/her judgment, there are strong indications of an immediate serious threat to the plant and/or its personnel.

Reports of system disturbances should also reflect if sabotage was the known or suspected source of the disturbance.

The following guidelines should be followed when filing a ***formal written report*** of a sabotage incident to ES ISAC (NERC) and include ERCOT. The suggested timelines for reporting should be accelerated whenever possible.

Security Breaches:

Physical Security Compromise – Unauthorized access of a person or a device through, circumventing, or damaging the physical perimeter.

Report when: unauthorized physical access to critical assets or critical cyber assets occurs.

Report within: 8 hours of detection or sooner, if possible.

Information Theft or Loss – Unauthorized removal of an item of value.

Report when: unencrypted information required to be protected pursuant to CIP standards is removed without authorization.

Report within: 8 hours of detection or sooner, if possible.

Suspected Activities:

Attempted Physical Intrusion – A detected effort to gain unauthorized access of a person or device through the physical perimeter but without obvious success.

Report when: the attempt is a concerted, focused effort to gain unauthorized physical access to critical assets or cyber assets.

Report within: 1 hour of detection or sooner, if possible.

Surveillance Activities:

Social Engineering – The attempt by an unauthorized person to manipulate people into performing actions or divulging information.

Report when: suspected or actual instances of social engineering occur.

Report within: 8 hours or sooner, if possible.

Photography – Taking still or moving pictures.

Report when: incident of photo is suspicious.

Report within: 8 hours or sooner, if possible.

Observation – Showing unusual interest in a facility; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.

Report when: activity is suspicious or unauthorized.

Report within: 8 hours or as soon as possible.

Flyover – Flying an aircraft over a facility; this includes any type of flying vehicle including an unmanned aerial vehicle (UAV) loitering over a site.

Report when: activity is suspicious or unauthorized.

Report within: 8 hours or sooner, if possible.

Threats:

Expressed Threat – Communicating a threat.

Report when: threat has a potential to damage or compromise facility or personnel.

Report within: 6 hours of receipt of threat, or sooner, if possible.

Weapons Discovered – Discovery of explosives.

Report when: explosives are discovered at or near a facility.

Report within: 1 hour of detection or sooner, if possible.

Attack (physical/communication) – Attack via physical or communications means.

Report when: suspected or actual; attacks against generation, transmission, or company owned or operated communication facilities or personnel occur.

Report within: 1 hour or sooner, if possible.

Cyber Attack- via control system must be reported with one (1) hour of incident:

Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations

Cyber event that causes interruptions of electrical system operations

Complete operational failure or shutdown of the transmission and/or distribution electrical system

Electrical System Separation (Islanding) where part or parts of a power grid remains (s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system

Load shedding of 100 megawatts or more implement under emergency operation policy

System-wide voltage reductions of 3 percent or more

Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system

Additionally, if any of the below occur and none of the above 7 items apply these items below must be reported within 6 hours of incident:

Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems.

Cyber event that could potentially impact electric power system adequacy or reliability

Fuel supply emergencies that could impact electric power system adequacy or reliability

SABOTAGE REPORTING

Sabotage Reporting at PRI is paramount to the interests of the Company, its customers, and the Federal, State and Local Governments we support. Industry and Government are especially dependent upon electric utilities to provide power that supports their critical infrastructures. This policy was created as a result of the increased risk of physical threats to the energy sector. It's important that management and staff recognize acts of sabotage so that a proper response can be taken, and appropriate communication can take place. Disturbances or unusual occurrences, suspected or determined to be caused by sabotage**,** must be reported to the appropriate systems, governmental agencies and regulatory bodies.

PRI has defined all its facilities and cyber assets that support the bulk electric system. PRI has established communications contacts with local FBI and developed reporting procedures as appropriate to their circumstances. The facility has in place, a call list of all local and federal law enforcement agencies that will respond to a sabotage event at one of these geographic locations.

The CRO first response is to contact local law enforcement agencies if a sabotage event occurs. PRI management will then contact Grid Operations at ERCOT to coordinate a formal written report to all required agencies including notifications and reporting requirements as defined in BHER BCP.

The following table directs who to contact immediately**(C)** and/or file a required written report **(R)** to under various sabotage incidents and threats:

Type	Executive Leadership	Corp IT Help Desk	Police	FBI	DOE	DHS*	NERC	ERCOT/ TRE
Physical Security Compromise	**C**		**C**	**C**			**R**	**R**
Information Theft or Loss	**C**	**C**	**C**	**C**			**R**	**R**
Attempted Physical Intrusion	**C**		**C**				**R**	**R**
Social Engineering	**C**	**C**	**C**	**C**			**R**	**R**
Photography	**C**		**C**	**C**			**R**	**R**
Observation	**C**		**C**	**C**			**R**	**R**

Flyover	C		C	C			R	R
Expressed Threat	C		C	C			R	R
Weapons Discovered	C		C	C	R	R	R	R
Attack	C	C	C	C	R	R	R	R
Intentional Misoperation of a Relay	C		C	C	R	R	R	R
Intentional Trip of a Major Unit	C	C	C	C	R	R	R	R
Cyber	C	C	C	C	R	R	R	R

Note: **C** – Communicate immediately
R – Report within guidelines
* - include appropriate State Department of Homeland Security.

- ***Contacts (government agencies for reporting sabotage incidents follow):***

Dept of Energy
Copies of EIA-417 (also referred to as OE-417) Schedule 1 and 2 reporting forms are available from DOE. Always check for the most current version from the DOE website using the link below. Cut and paste this link into the web address.

ftp://ftp.eia.doe.gov/pub/electricity/eiafor417.doc

To report physical infrastructure incidents, please contact DOE at doehqeoc@oem.doe.gov or (202) 586-5000.

Dept of Homeland Security (NICC)
To report physical infrastructure incidents, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

NERC
To report physical infrastructure incidents, please contact NERC at esisac@nerc.com or fax (404) 446-9770,or 404-446-9780 (24 Hour phone line).

ERCOT
To report physical infrastructure incidents, please contact ERCOT at 512-248-3100.
ERCOT TDC 512-248-3030 or 515-248-3105 (Shift Supervisor).

FBI
To report physical infrastructure incidents, please contact the Dallas Field Office at 972-559-5000
Email fbi.dallas@ic.fbi.gov.
Abilene field office at 325-675-8044 or Email fbi.abilene@ic.fbi.gov.
FBI Emergencies with Joint Terrorism Task Force at 858-565-1255.

TRE
To report physical infrastructure incidents, please contact TRE at 512-583-4900

Executive Leadership notification for reporting sabotage incidents:

Executive Leadership **(following order)**
Alicia Knapp, President, CEO, Berkshire Hathaway Renewables ("BHER") 515-242-3951 or 515-777-8354
Email: alicia.knapp@bherenewables.com

Utilize BHER Business Continuity Plan and BHER Cyber Security Incident Response Plan for detail on additional notification requirements, classification and contacts.

PLANT SECURITY PLAN

This program will primarily focus on monitoring plant facilities and adjacent equipment or structures (above ground), controlling entrance to the site based on the HSAS protective measures and defining the notification process.

Monitoring

The *Security Contingency Plan* established security practices and the United States Department of Justice, *The Citizen's Preparedness Guide* will be the nucleus for monitoring for a security breach for the site and surrounding area.

Plant and adjacent equipment at risk to attacks are as follows: (2) General Electric combustion turbine generator, (1) Hitachi steam turbine generator, (2) Deltak heat recovery steam generator, (1) connecting natural gas pipeline, (1) 138/345kV switchyard and connecting electrical lines and equipment, steam pipelines and raw water pipelines.

List of Facilities:

PRI:	Main Building	Above Ground
	Gas Turbine Building	Above Ground
	Steam Turbine Building	Above Ground
	Water Plant	Above Ground
	Switch Yard	Above Ground
	Cooling Tower	Above Ground
	Warehouse	Above Ground
STORAGE TANKS:	Jet Fuel	Above Ground
	Hydrogen (4)	Above Ground
	Caustic	Above Ground
	Sulfuric Acid	Above Ground

The portions of PRI are underground are less vulnerable to attack than the aboveground facilities. Therefore, this program will primarily focus on the above ground facilities.

PRI recognizes that the pipeline may be affected by terrorist acts not specifically directed at the PRI Facility.

PRI is located within the compounds of the Delek Refinery which is surrounded by chain link fencing and topped with barbed wire. Site access is controlled via Delek security guards. Visitors are not allowed through the gate unless prior notification has been provided by a PRI employee to the guard. All unscheduled visitors are held outside the perimeter until the appropriate PRI person can be contacted for approval to allow entrance. The PRI facility is surrounded by chain link fencing that is topped with strands of barbed wire placed at an angle of 45 degrees tilted outwards. Access is provided through locked vehicle gates or pedestrian gates/doors that are locked at all times. The PRI Site Access Control and Accountability

Guideline addresses control of key cards, door locks and key locks utilized to control access. Entrance into the main building is controlled via card readers or combination keypads accompanied by a camera system which is monitored 24/7 by the control operator. Access to the control room itself is controlled via locked doors which are monitored by a camera system, keypad and card readers. Visitors are only allowed access after approval is granted from the control operator and after a PRI employee is present to provide an escort. Visitors are required to complete a visitor's log which records name, time in and out, company, cell phone number and name of PRI employees they are visiting.

The control room is manned 24/7 and no visitors or contractors are ever allowed to occupy this room without a PRI employee being present. Access to PRI's Energy Management Room is through the control room only and these doors are locked at all times with key control managed by the control room operator. PRI personnel approved to access to these rooms are defined below:

PRI Management
PRI I&E Technicians
PRI Control Room Operators

All other access must be approved by the control room operator and with an escort from the above list only.

Access to the plant is controlled by locked gates as well and monitored via plant camera systems designed to allow tracking from one end to the facility to the other. The plant outside perimeter is well lighted and includes periodic inspections of doors, perimeter fencing and locking systems to ensure they are functional.

PRI personnel will monitor plant facilities and adjacent equipment as part of the day-to-day duties as established by plant operating procedures. The following are things that will assist in this process:

Know the routines and normal activities.
This will assist in identifying anything out of place or abnormal conditions.

Be aware and learn to spot suspicious packages and unknown items.
Do not shake, bump or shift suspicious items.

Survey the plant perimeter and areas that are not normal pathways.

Ensure functionality of all Gaitronics call box equipment and emergency sirens.

Change all access combinations when an employee exits the company.

Do not share combinations or door passes with contractors.

Notify management immediately if you suspect confidential information has been shared or passed to un-authorized individuals (combinations, plant access instructions, keys, personal information, etc.) If in doubt always report.

Access Control

This process is to guide PRI managers in the management of Key Cards / Fobs, keyed locks and the changing of combinations. This process related to employees, visitors and contractors.

Process

Key Cards and Key Fobs (RFID Door Controls)

Only the General Manager and Operations & Maintenance Manager are authorized to make the decision to issue a key fob or key cards.

Only the General Manager and Operations & Maintenance Manager have access to the key card control computer and spare key fobs.

All Employees are issued key cards or key fobs.

If a key card or key fob is lost, the affected employee, visitor or contractor must notify the General Manager or Operations & Maintenance Manager immediately. Access will be terminated for the lost device immediately upon notification.

Upon separation from the company, keys, key cards and key fobs are to be returned to the Company.

All Key cards and Fobs are kept behind a locked door within the Operations & Maintenance Managers office and deactivated until issued

RFID controlled door access for employees is as follows

Main admin bldg doors – all employees

Access to the water lab – all employees except the Project Analyst

Access to the switchgear room – all employees except the Project Analyst

Employees shall have their Key FOB or Key Card with them at work at all times.

Each quarter the General Manger or Operations & Maintenance Manager shall audit each person's key FOB or card to ensure each person still has the device originally assigned to him or her.

Keypad Locks

All employees are given the combination to the Admin Building keypad locks.

Keypad lock combinations will be changed when an employee separates from the Company, at the beginning of each year and if a security breach is suspected.

Changes are done by the Operations & Maintenance Manager.

Key Locks

Key locks are used on all personnel access gates around the facility to control access.

Collecting employee keys is an exit requirement when and when an employee separates from the Company and is done by the employee manager. Key locks will be changed if a security breach is suspected.

Key locks control access to the energy management room (server location), with keys being controlled by the control room operator and management staff. Access is only allowed to limited number of PRI employees as discussed above and all visitors will be accompanied if access is determined to be required.

Key Lock Boxes

Key lock boxes are used to secure the keys to the doors for the energy management room and switchyard.

Control operators given the combination.

Key lock box combinations will be changed when a security breach is suspected.

Visitors

Spare key Fobs are kept for visitor use and are customized for the specific visitor granting them access only as needed.

A BHE employee on site for an extended period may be given a fob that will be set to grant them access only as needed, typically access to the front double doors and the back door next to the lunchroom.

Contractors

Spare Key Fobs will be kept for contractor use.

It is rare that contractors are granted admin building access. For the most part contractors are escorted in the building or allowed in and out of the building by ringing a doorbell. If a contractor is allowed building access with a Fob it will only be for the hours of each day that they are on site and they will be granted access as needed, typically to allow them into and out of the public areas of the building to use the restroom.

Anytime a PRI employee suspects or knows that the Access Control Procedure has been compromised the control operator shall lock down the facility (no visitors or contractors), notify gate guard to prohibit all visitors and contractors from entering the facility. Account for all personnel on-site (contractors and visitors shall be escorted and accompanied to breakroom and not left unattended). Management should be notified immediately so that a corrective measure can be put in place immediately to determine risk and actions necessary to restore site access control. 911 called if deemed necessary.

IF A TERRORIST ATTACK OCCURS

In addition to the measures listed previously, the following measures should be implemented:

Augment security forces to ensure control of the facility and access to the facility. Establish surveillance points and reporting criteria and procedures.

Ensure all gates have been locked. Close and lock all roll down doors and lock all remaining exterior plant doors.

Inspect all vehicles entering the Plant including the cargo areas, undercarriage, glove compartments and other areas where dangerous items could be concealed. No entrants other than plant personnel.

Ensure that all vehicles on site belong to onsite personnel.

Increase security patrols of facility to two times per day minimum. Increase perimeter patrols and inspections of the plant.

Cooperate with local police or other authorities if they direct security measures. If necessary, request assistance from the local police agencies in securing the facility.

If there is a compelling reason to shutdown PRI operation, follow the appropriate shutdown procedures and evaluate the situation before resuming operations.

911 NOTIFICATION

A call to the local 911 emergency center is PRI's first response to a security breach or potential threat to PRI personnel, facilities and adjacent facilities. Below is the PRI process for notification of emergencies or potential contingency. A telephone list is included with the emergency telephone numbers; however, the 911 responding entity will call emergency management offices or services.

Delegation of Authority

Upon discovery of an emergency or potential contingency, the Control Operator on duty will be notified. The Control Operator will be the responsible Company representative to coordinate activities during the contingency, until relieved. The Coordinator is vested with the authority to call in additional employees, if deemed necessary. The Chain of Command will be Control Operator, Operations & Maintenance Manager and General Manager.

Notification of Authorities

When an incident has been verified, the Control Operator will immediately notify the on-call Manager. If the appropriate Manager cannot be reached, the General Manager will be notified. Outside response agencies will be contacted as deemed necessary by the Control Operator (i.e., Fire Department, Ambulance, Law Enforcement, etc.) It will normally be the responsibility of

the General Manager or his designee to notify State or Federal authorities, as well as Executive Leadership, should the emergency require notification. However, in the rare likelihood that a manager cannot be contacted the Control Operator shall contact senior management for guidance on these notifications.

In the event of a security breach or suspicious activity in the vicinity of the plant, the Control Operator shall notify Emergency Services at **911**, and provide the following information for reporting:

Full name and phone #: **Your name @ 263-9000**

Name and address of facility: **PRI's**
500 East Refinery Road
Big Spring, TX 79720

Type(s) of threat and danger: **Suspicious packages and activities, trespassing, etc.**

If available and safe to obtain:
Description of item, event or perpetrator
License plate number
Direction of travel
Circumstances of the situation

If person is injured communicate:
Person's condition
How it happened
Do not hang up first (allow 911 operator to hang up first).

4. PLANT RESPONSE TO A SECURTY/THEFT/SABATOGE EVENT/DELIBERATE DISRUPTION

In the event of a potential or actual sabotage, terrorist or security type of event, PRI personnel should immediately move to a safe location as instructed by the Control Room Operator.

PLANT PERSONNEL

Will report immediately to the control room, unless otherwise specified during the initial announcement.

Will go about task assigned by Plant Management, or the CRO.

If an evacuation order is given, plant personnel will leave, by what is determined to be the safest route, in an orderly fashion in accordance with plant evacuation procedures.

CONTROL ROOM OPERATOR

The CRO will alert plant personnel and management via the Gaitronics and two-way radio. The CRO will also announce the assembly point for all personnel if it is another location other than the control room.

Will notify the local 911 District if situation warrants outside assistance by Emergency Response Personnel.

The CRO will notify the Delek Main Gate and EDF Trading of the situation and plant emergency response needs/activities.

Will assess situation and delegate responsibilities as required, ensuring personnel safety at all times.

Will maintain contact with plant management and Delek Safety, via telephone and two-way radio, for the duration of the emergency.

The CRO and Outside Operator will remain together at all times.

If time does not permit management input, the CRO should use sound judgment in making a decision on continued operations. The plant should be secured in a manner that protects employees and equipment.

OUTSIDE OPERATOR(s)

Will maintain continuous contact with the control room.

Will immediately attempt to make a determination of the true situation without endangering themselves (was anybody seen, suspicious sightings, things that don't look right, etc.). **Under no circumstances will the outside operator put him or herself in harm's way.**

PLANT MANAGEMENT

If on-site will assume EC responsibilities and implement notifications/communications, procedures, etc. from the Security Contingency Plan (see previous section) and BCP.

3.10 Bomb Threat Procedure

Most bomb threats are received by telephone. Bomb threats are to be taken seriously until proven otherwise. Act quickly but remain calm and obtain information with the checklist on the following page.

IF A BOMB THREAT IS RECEIVED BY TELEPHONE:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.

2. Listen very carefully, be polite, and show interest.

3. Attempt to keep the caller talking to learn more information.

4. If possible, write a note to a colleague to call the authorities from a different phone; engineering office, control room cellular phone, etc.

5. If your phone is equipped with caller identification record the telephone number displayed.

6. Complete the Bomb Threat Checklist, (on following page), immediately. Write down as much detailed information as you can remember. Try to record the exact conversation, or as close to as possible.

7. Immediately upon termination of the call contact 911; DO **NOT HANG UP THE PHONE THE BOMB THREAT WAS RECEIVED UPON.** Use a different telephone to make the contact of law enforcement. The Control Room Operator can use the Control Room cellular telephone to contact 911.

IF THE BOMB THREAT IS RECEIVED BY A HANDWRITTEN NOTE:

Call 911 immediately.
Handle note as minimally as possible.

IF THE BOMB THREAT WAS RECEIVED VIA EMAIL:

Call 911 immediately.
DO NOT delete the email.

The BOMB THREAT CHECKLIST is on the following page. This checklist is to be filled out as soon as practical after receiving a bomb threat. There are two pages to the checklist.

BOMB THREAT CHECKLIST

Page 1 of 2

Date:_____ Time Received: _____ Time Call Ended: _____

Call Received By:_____

Phone Number Where Call Received (if known):

_____

ASK CALLER:

Where is the bomb located? _____

When is it set to detonate? _____

What does the bomb look like?_____

What kind of bomb is it?_____

What will make it explode?_____

Did you place the bomb? (circle correct response) YES NO

Why was the bomb place? _____

What is your name? _____

EXACT WORDS OF THREAT:

_____

_____

INFORMATION ABOUT CALLER

Where is caller located? (Background and level of noise):

_____

_____

Estimate Age: _____

Is voice familiar? If so, who does it sound like? _____

Other points: _____

BOMB THREAT CHECKLIST
Page 2 of 2

	Caller's Voice
	Male
	Female
	Accent
	Angry/Calm
	Excited
	Clearing throat
	Coughing
	Crackling voice
	Crying
	Deep
	Deep breathing
	Disguised
	Distinct
	Laughter
	Slurred/Stutter
	Lisp
	Loud/Soft/Normal
	Nasal
	Raspy
	Ragged
	Rapid

	Background Noises
	Animal noises
	House noises
	Kitchen noises
	Street noises
	Booth
	PA system
	Conversation
	Music
	Motor
	Clear
	Static
	Office machinery
	Factory machinery
	Local
	Long distance

	Threat Language
	Incoherent
	Message read
	Taped
	Irrational
	Profane
	Well - spoken

RECORD ANY ADDITIONAL COMMENTS:

3.11 PRI Response to Suspicious Mail

Organisms can infect the skin, the gastrointestinal system, or the lungs. To cause infection, the spores must come into contact with broken or abraded skin, swallowed, or inhaled as a fine dust. However, infection can be prevented even after exposure to spores by early treatment with the appropriate antibiotics. Spores can be dispersed in the air as a dust or can be carried on items such as mail or clothing. These guidelines emphasize preventing the spread of spores through careful handling and isolation of suspicious packages and their contents.

General Mail Handling

Be on the lookout for suspicious envelopes or packages; see the FBI Informational Poster on page 3 of this document.

Do NOT open suspicious mail.

Open all non-suspicious mail with a letter opener or another method that minimizes skin contact with the mail and is least likely to disturb contents.

Open mail with a minimum amount of movement.

Do not blow into envelopes.

Keep hands away from nose and mouth while opening mail.

Turn off fans, portable heaters, and other equipment that may create air currents.

Wash hands after handling mail.

Characteristics of Suspicious Packages and Letters

Letters or packages with any of the following characteristics should be considered suspicious and cause for concern, up to an including notification of emergency management services.

Discoloration, oily stains, or an unusual odor
Crystals, powder, or powder-like residue on the surface
Suspicious or threatening language on the outside of package or letter
Postmark that does not match return address or no return address
Restrictive endorsements such as "Personal" or "Confidential"
Distorted handwriting, block-printed or poorly typed addresses
Excessive tape or string
Rigid, uneven, irregular, or lopsided package
Package with soft spots, bulges, or excessive weight
Handwritten, block-printed or poorly typed addresses
Excessive postage
Title but no name or incorrect title
Misspelled addressee's name, title, or location
Misspelled common words
Addressee unknown or no longer with organization
Protruding wires or aluminum foil
Ticking sound
Unexpected mail from a foreign country

If You Receive or Discover a Suspicious Package or Letter

- **Do NOT open** the package or letter.
- **Do not shake, empty, or otherwise disturb its contents.**
- Put the package down and do not handle it further.
- Do not touch or try to clean up the substance.
- Alert others nearby.
- Do not remove ANY items from area.
- **DO NOT** use two-way radios, or cellular phones (radio signal have potential to detonate a bomb)
- **Leave the area immediately and gently close the door.**

After leaving the area:

Wash hands well with soap and water.

Contact the control room immediately. The Control Room Operator, CRO, will notify PRI Management, and if deemed necessary, Howard County Emergency Services will be notified, (911).

PRI will limit movements within the building to prevent spread of substance.

Initial PRI Response

Cutting off of electrical power, and the shutdown of ventilation systems serving the potentially contaminated areas.

Assist as directed by PRI Management and Emergency Response personnel

Perform additional decontamination activities as directed by the proper emergency management authorities

PRI Management Response

Directing further evacuation

Reporting the incident to Corporate Management

Compiling a list of the names of all potentially affected individuals, including those who were in area when the suspicious mail was encountered.

Providing this list to the appropriate authorities.

Work with local and state law enforcement agencies.

Contact of federal law enforcement

ONLY THE GENERAL MANAGER WILL SPEAK TO THE MEDIA.

FBI Advisory

If you receive a suspicious letter or package

What should you do?

1. Handle with care
   Don't shake or bump
2. Isolate and look for indicators
3. Don't Open, Smell or Taste
4. Treat it as Suspect!
   Call 911

If parcel is open and/or a threat is identified. . .

For a Bomb

Evacuate Immediately
Call 911 (Police)
Contact local FBI

For Radiological

Limit Exposure - Don't Handle
Distance (Evacuate area)
Shield yourself from object
Call 911 (Police)
Contact local FBI

For Biological or Chemical

Isolate - Don't Handle
Call 911 (Police)
Wash your hands with soap and warm water
Contact local FBI

Police Department _____

Fire Department _____

Local FBI Office _____

(Ask for the Duty Agent, Special Agent Bomb Technician, or Weapons of Mass Destruction Coordinator)

GENERAL INFORMATION BULLETIN 2000-3
Produced by: Bomb Data Center
Weapons of Mass Destruction Operations Unit

5. Special Notes about Anthrax

Transmission

Anthrax is not known to spread from one person to another person. *B. anthraces* spores can live in the soil for many years, and humans can become infected with anthrax by handling products from infected animals or by inhaling anthrax spores from contaminated animal products. Anthrax can also be spread by eating undercooked meat from infected animals. It is rare to find infected animals in the United States. Anthrax spores can be used as a bioterrorist weapon, as was the case in 2001, when *Bacillus anthraces* spores had been intentionally distributed through the postal system, causing 22 cases of anthrax, including 5 deaths.

Types of Anthrax Infection

Anthrax infection can occur in three forms: cutaneous (skin), inhalation, and gastrointestinal.

***Cutaneous*:** Most (about 95%) anthrax infections occur when the bacterium enters a cut or abrasion on the skin, such as when handling contaminated wool, hides, leather or hair products (especially goat hair) of infected animals. Skin infection begins as a raised itchy bump that resembles an insect bite but within 1-2 days develops into a vesicle and then a painless ulcer, usually 1-3 cm in diameter, with a characteristic black necrotic (dying) area in the center. Lymph glands in the adjacent area may swell. About 20% of untreated cases of cutaneous anthrax will result in death. Deaths are rare with appropriate antimicrobial therapy.

***Inhalation*:** Initial symptoms may resemble a common cold – sore throat, mild fever, muscle aches and malaise. After several days, the symptoms may progress to severe breathing problems and shock. Inhalation anthrax is usually fatal.

***Gastrointestinal*:** The intestinal disease form of anthrax may follow the consumption of contaminated meat and is characterized by an acute inflammation of the intestinal tract. Initial signs of nausea, loss of appetite, vomiting, fever is followed by abdominal pain, vomiting of blood, and severe diarrhea. Intestinal anthrax results in death in 25% to 60% of cases.

Symptoms for Anthrax

These symptoms can occur within 7 days of infection:

- Fever (temperature greater than 100 degrees F). The fever may be accompanied by chills or night sweats.
- Flu-like symptoms.
- Cough, usually a non-productive cough, chest discomfort, shortness of breath, fatigue, muscle aches
- Sore throat, followed by difficulty swallowing, enlarged lymph nodes, headache, nausea, loss of appetite, abdominal distress, vomiting, or diarrhea
- A sore, especially on your face, arms or hands, that starts as a raised bump and develops into a painless ulcer with a black area in the center.

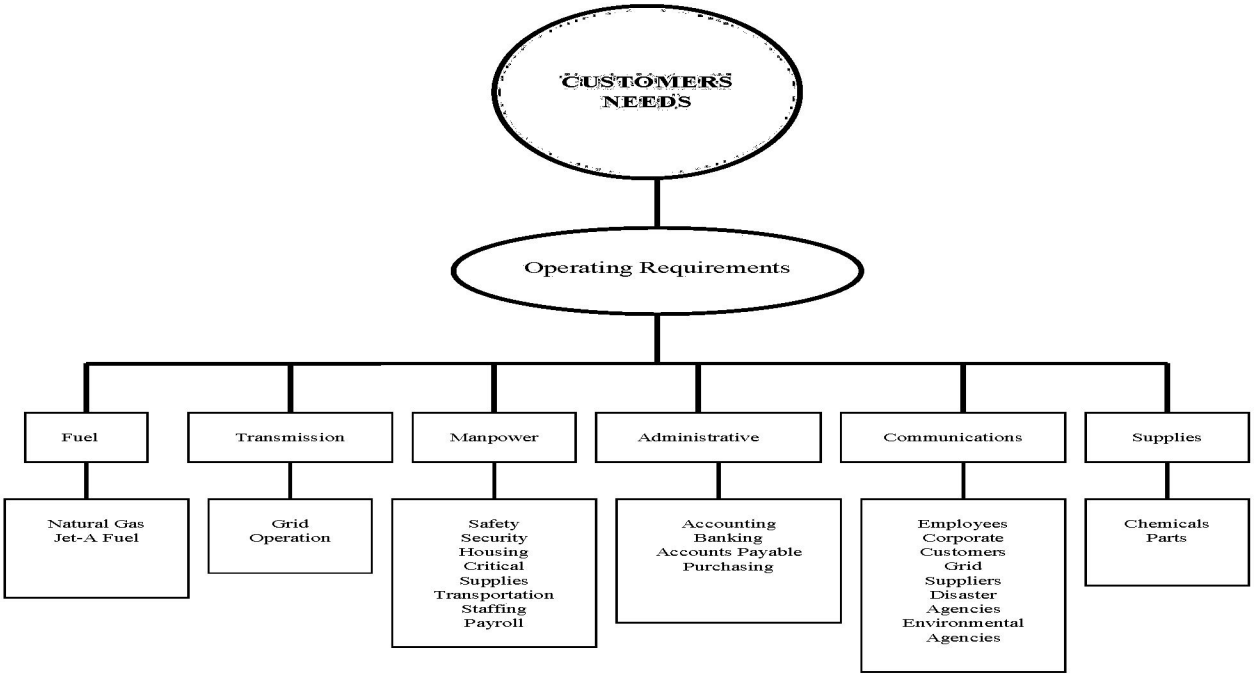
Treatment

Testing and treatment with antibiotics options are available.

A protective vaccine has been developed for anthrax; however, it is primarily given to military personnel. Vaccination is recommended only for those at high risk, such as workers in research laboratories that handle anthrax bacteria routinely. The antibiotics used in post exposure prophylaxis are very effective in preventing anthrax disease from occurring after an exposure.

3.12 PURPOSE

To provide a thorough review mechanism and effective direction that will enable PRI to respond and recover normal operations in a controlled expeditious manner during following an emergency event. The flow chart below was used as an outline in reviewing PRI's needs, and readiness.



3.13 REVIEWS

Initially, an outline was prepared identifying site-specific issues, potential impacts and common group issues. The results of these reviews were then used to determine PRI's readiness and ability to respond to a disastrous event, with the end goal being facility restoration in a safe and environmentally sound manner as quickly as possible.

PRI has emergency response procedures to address reasonably anticipated emergencies. Anticipated emergencies are based upon the analyses referred to in this section. Emergency events have been evaluated using the same rating system as applied to the PRI Risk Management Plan.

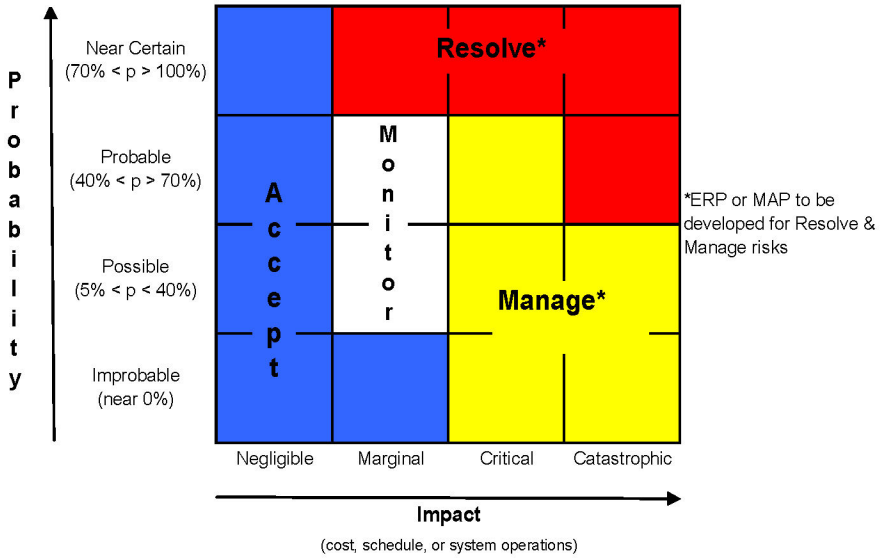
The following ratings are applied to the impact attribute:

4	Catastrophic	Failure of mission-essential service
3	Critical	Significantly degraded performance
2	Marginal	Moderate impact
1	Negligible	Inconvenience

The following ratings are applied to the probability attribute:

4	Near Certain	70% < p < 100%
3	Probable	40% < p < 70%
2	Possible	5% < p < 40%
1	Improbable	Probability near 0%

When the ratings are assigned, risks are plotted on the Emergency Priority Model forms on the following pages. The Emergency Priority Model is used to identify the appropriate mitigation strategy for the risk.



PRI did not have any items falling into the resolve category and currently has a total of 24 items falling under the manage category which are covered by this plan.

3.14 General Emergencies

PRI has examined each potential emergency with the focus being on the level of business disruption, which could arise from each. Potential emergency events have been assessed as follows:

POTENTIAL EMERGENCY	PROBABILITY RATING	IMPACT RATING	RESULT	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Tornado	2	3	Manage	Damage to plant equipment, loss of lives, supply interruptions.
Hurricane	NA	NA	NA	
Flood	NA	NA	NA	
Ice/Snowstorm	2	3	Manage	Equipment damage, manpower shortage, supply interruptions.
Drought	2	3	Manage	Loss of raw water supply or curtailment.
Earthquake	2	3	Manage	Equipment damage, loss of lives, supply interruptions.
Electrical Storm	3	2	Manage	Equipment damage, loss of lives.
Fire	2	3	Manage	Equipment damage, loss of lives.
Subsidence/Landslide	NA	NA	NA	
Freezing Conditions	3	3	Manage	Equipment damage, manpower shortage.
Contamination and Environmental Hazards	2	3	Manage	Equipment damage, permit exceedance, manpower shortage.
Epidemic	2	3	Manage	Manpower shortage, loss of lives, supply interruptions.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL
1	IMPROBABLE	1	NEGLIGIBLE

Organized and/or Deliberate Disruption

PRI has examined each potential emergency resulting from ‘organized disruption’.

Potential emergencies resulting from 'organized disruption' have been assessed as follows.

POTENTIAL EMERGENCY	PROBABILITY RATING	IMPACT RATING	RESULT	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Act of Terrorism	2	3	Manage	Equipment damage, loss of lives, supply interruptions.
Act of Sabotage	2	3	Manage	Equipment damage, loss of lives, supply

				interruptions.
Act of War	2	2	Monitor	Loss of manpower, supply interruptions.
Theft	2	3	Manage	Business interruption
Arson	2	3	Manage	Equipment damage, loss of lives, supply interruptions.
Labor Disputes	NA	NA	NA	

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL

Loss of Utilities and Services

PRI has examined each potential emergency resulting from loss of utilities and services.

Potential emergencies as a result of loss of utilities and services have been assessed as follows.

POTENTIAL DISASTER	PROBABILITY RATING	IMPACT RATING	RESULT	BRIEF DESCRIPTIONOF POTENTIAL CONSEQUENCES
Electrical Power Failure	4	1	Negligible	Loss of generating capabilities.
Loss of Gas Supply	2	3	Manage	Loss of generating capabilities.
Loss of Water Supply	2	3	Manage	Loss of generating capabilities.
Petroleum/Oil Shortage	2	2	Monitor	Potential impact to continued operations, manpower shortages.
Communication Services Breakdown	2	2	Monitor	Safety issue, hindrance to normal business operations
Loss of Drainage/Waste Removal	2	2	Monitor	Permit exceedences

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL
1	IMPROBABLE	1	NEGLIGIBLE

Critical Property Unit (CPU) Failure (BRPs)

Critical property units (CPU) consist of equipment or systems important to continued plant operation. PRI has examined potential emergency situations resulting from CPU failures, most of which were evaluated at the Monitor or Accept levels. The analysis of all of the PRI CPUs can be seen in the PRI detailed Risk Management Plan. Eight CPUs were evaluated at the manage level, and they are prioritized below.

POTENTIAL EMERGENCY	PROBABILITY RATING	IMPACT RATING	RESULT	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Internal Power Failure	3	2	Monitor	Loss of generating capability, equipment damage.
Air Conditioning Failure	3	2	Monitor	Loss of generating capability, equipment damage.
Turbine Failure	2	3	Manage	Loss of generating capability, equipment damage, employee risk.
Generator Failure	2	3	Manage	Loss of generating capability, equipment damage, employee risk.
Cooling Tower Failure	2	3	Manage	Loss of generating capability, equipment damage.
Control System Failure	2	3	Manage	Loss of generating capability, equipment damage.
Piping Failure	3	2	Monitor	Loss of generating capability, equipment damage, employee risk.
Boiler Tube Failure	3	2	Monitor	Loss of generating capability, equipment damage, employee risk.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL
1	IMPROBABLE	1	NEGLIGIBLE

Serious information Security Incidents

PRI has examined each potential emergency resulting from serious information security incidents.

Potential emergencies as a result of serious Information Security incidents have been assessed as follows.

POTENTIAL	PROBABILITY	IMPACT	RESULT	BRIEF DESCRIPTION OF

EMERGENCY	RATING	RATING		POTENTIAL CONSEQUENCES
Loss of Records or Data	1	1	Accept	Loss of critical information.
Disclosure of Sensitive Information	1	1	Accept	Impact company reputation, loss of competitiveness, legal ramifications.
IT System Failure	3	2	Monitor	Loss of critical information, impact to routine daily business functions.
Cyber Event	1	3	Manage	Loss of generating system controls, false indications, or uncontrolled manipulation of equipment.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL
1	IMPROBABLE	1	NEGLIGIBLE

3.15 Other Emergencies

PRI has assessed other emergencies as follows:

POTENTIAL EMERGENCY	PROBABILITY RATING	IMPACT RATING	RESULT	BRIEF DESCRIPTION OF POTENTIAL CONSEQUENCES
Workplace Violence	2	2	Monitor	Continued business impact, employee risks.
Public Transportation Disruption	NA	NA	NA	
Neighborhood Hazard	2	2	Monitor	Continued business impact, employee risks.
Health and Safety Regulations	2	3	Manage	Continued business impact, employee risks, and financial penalties.
Employee Morale	2	3	Manage	Continued business impact, employee risks.
Mergers and Acquisitions	1	1	Accept	Continued business impact, employee risks.
Negative	2	4	Manage	Continued business impact, financial

Publicity				impact.
Legal Problems	2	3	Manage	Continued business impact, financial impact, and negative publicity.

PROBABILITY RATING		IMPACT RATING	
SCORE	LEVEL	SCORE	LEVEL
4	NEAR CERTAIN	4	CATASTROPIC
3	PROBABLE	3	CRITICAL
2	POSSIBLE	2	MARGINAL
1	IMPROBABLE	1	NEGLIGIBLE

Key Business Processes

PRI has identified key business processes, in order of importance to its business, together with a brief description of the business process and main dependencies. After the identification of the key processes, PRI has concluded a review of the systems and believes that adequate backup systems or plans are in place.

KEY BUSINESS AREA		BRIEF DESCRIPTION OF BUSINESS PROCESS	MAIN DEPENDENCIES
1	Foxboro IA	Plant control systems	All plant equipment
2	On-line Real Time Market Information	Plant dispatch signal (AGC) and real time ERCOT pricing	Plant load changes
3	Oracle Financials	Financial accounting program	Plant inventory, purchasing, accounts payable
4	WAM	Work management system	Plant maintenance functions, cost tracking
5	E-mail Based Communication	Communication	Plant communication
6	Information Technology Services	Plant support systems	Data collection.

3.16 Financial and Operational Impact

PRI has established standard time-bands for measuring periods when, during an emergency, normal business services could become unavailable. These time-bands have been applied to each key business process and an assessment made of the financial and operational impact for outages. The structure is as follows:

TIME BAND	PERIOD OF MEASUREMENT
1	Up to 2 hours
2	2 – 24 hours
3	24 – 48 hours
4	2 – 5 days
5	More than 5 days

For each key process it has been necessary to make an assessment of the operational and financial impact of disruption to normal business operations. The financial impact has been assessed based on anticipated lost revenue plus projected costs of recovery.

ASSESSMENT OF OPERATIONAL IMPACT

BUSINESS PROCESS	TIME-BAND				
	1	**2**	**3**	**4**	**5**
	2 HOURS	*2-24 HOURS*	*24-48 HOURS*	*2-5 DAYS*	*MORE THAN 5 DAYS*
Foxboro IA Reporting	X				
On-line Real Time Market Information		X			
Oracle Financials					X
WAM					X
E-mail Based Communication					X
Information Technology Services					X

ASSESSMENT OF FINANCIAL IMPACT

For each of the time-bands the financial impact has been quantified. This was assessed based on anticipated lost revenue plus projected costs of recovery.

The definition of *"significant impact"* represents a level where customers will notice the outage and may receive an inadequate level of service response.

BUSINESS PROCESS	TIME-BAND				
	1	2	3	4	5
	2 HOURS	*2-24 HOURS*	*24-48 HOURS*	*2-5 DAYS*	*MORE THAN 5 DAYS*
Foxboro IA Reporting	$400,000				
On-line Real Time Market Information		$200,000			
Oracle Financials					$70,000
Work Authorization Management					N/A
E-mail Based Communication					$10,000
Information Technology Services					$10,000

PRI has an immediate response plan in place for emergency events. These plans focus on employee safety, equipment protection, proper communication, and the resumption of customer service in a prompt, organized manner.

Even though PRI may not be directly involved in an event, the ability to continue operations could be negatively impacted by the same essential elements (e.g. employees unwilling to come to work, key supplies interrupted or delayed, or transmission up or downstream from the facilities damaged or destroyed). PRI has developed detailed plans to deal with staffing issues, communication, continuation of key supplies, and other plant recovery needs.

PRI has identified the following key operating requirements that could negatively impact our ability to continue meeting customer needs. Contingency plans have been developed to assist in mitigating these potential risks.

4. NOTIFICATIONS/COMMUNICATIONS TO MEDIA AND PUBLIC

During an emergency situation warranting the distribution of information to the public, the General Manager, or his designee, will serve as Spokesperson for the media and public. The General Manager or his appointed spokesperson will have access to all necessary information, will provide timely and accurate information to local, state, and federal agencies and will seek reciprocal information from these agencies. Corporate Communications will assist with coordination of statements and information to be released to the media and public.

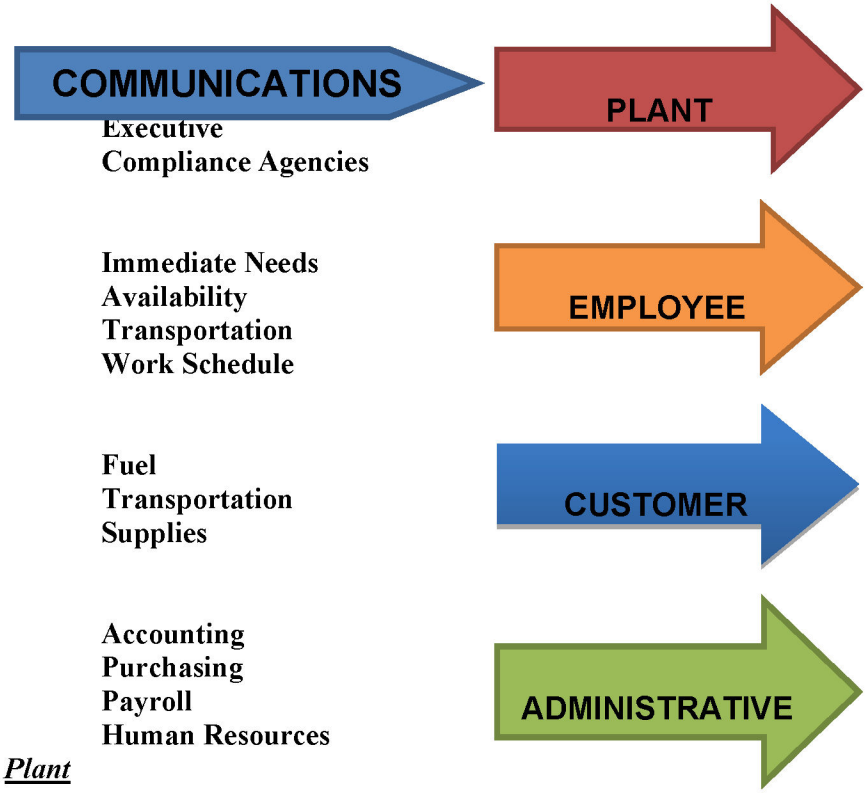
Public notification of the residences, businesses, etc. surrounding the facility will be the responsibility of the local / state officials. This notification will be carried out through existing systems, such as outdoor warning sirens, television, or radio announcements.

Rapid and proper communication is critical in order to ensure that recovery plans are functional. PRI has developed a recovery communication plan that identifies multiple communication options that can be used. After an event, clear communication is paramount in order to assess safety, plant damage, immediate physical employee needs, availability, transportation routes, and availability of necessary supplies and plant staffing requirements.

Communication is expected to be on-going with disaster recovery officials and regulatory/environmental agencies to report releases, sabotage events or violations, if mandated to continue running in a non-standard mode of operation (refer to notifications/communications section 3.10 for instructions).

The diagram below demonstrates communication needs and priorities necessary to restore normal operations

Note: *management personnel shall refer to the BHER Business Continuity Plan for additional detail and direction on notifications (see "personal notification procedures")*



Plant

Plant communication will be conducted in the same manner as used today. Critical contact information for all corporate support staff will be maintained on and off site by key plant response personnel both electronically and with paper back-up.

Employee

PRI maintains an employee call list that includes home telephone numbers, cell phones, and e-mail addresses. An additional call list will be maintained by human resources to assist with callouts during an event. Additionally, PRI's managers are provided with an employee contact list that will reside at their homes.

Corporate

The Information Technology department for Berkshire Hathaway Energy is housed in a secured facility in Urbandale, IA. PRI has two T-1 lines that transfer data continuously to the Urbandale servers with backups in place

Other than some possible data collection delays, there are no known operating support systems such as Oracle, WAM, etc. that would prevent continued facility operations.

Customer

Customer communication is an integral part of PRI's daily business. In order to ensure continued communication during an emergency event, customer contact lists are included in PRI's risk management data base and the contacts section of the plan.

Grid

The loss of communication with the utility grid is not expected to pose a significant risk to the PRI facility. Plant output can be controlled manually from the facility control room. The loss of grid communication would require the plant to run in manual load control since the required communication for Automatic Generator Control ("AGC") could not be accomplished. Contractual requirements would likely be excused under force majeure provisions. All employees realize the importance of establishing some means of communication with the transmission operator and QSE to ensure grid stability. Any abnormal operations would be subject to proper compliance notifications.

Suppliers

PRI has multiple vendor contacts for all non-fuel related materials and supplies. Vendor information is kept at the plant sites, as well as being accessible from Des Moines through the Oracle Financials system.

This section describes the procedures for the notification of on-site personnel, emergency response personnel, local, state, and federal agencies as well as corporate management. It is important to remember that **Corporate Communications** should be contacted prior to any notifications to news organizations or other public media outlets. Additionally, all notifications of this type should come from the senior manager on site. Each procedure contains methods and the sequencing of notifications.

6. NOTIFICATION OF ON-SITE PERSONNEL

The present means for the notification of personnel within the boundaries of the facility are telephone, P.A. system, or portable two-way radio.

Visitors to the plant and operational areas are assigned to a facility employee. This employee is responsible for informing the visitor of emergencies and taking protective action as necessary. Additionally, the warning alarm sirens are used to notify all personnel of an emergency and the need to report to the control room or other location if directed.

Facility personnel are trained as to what actions to take in an emergency prior to their work assignments; if not an individual who has been trained in emergency response procedures

must escort them. This training includes instruction on the methods of notification and the required actions in the event of an emergency.

7. NOTIFICATION OF CORPORATE PERSONNEL (management see BHER BCP)

Corporate personnel are contacted for all levels of emergencies, including Incident Level events. Notifications should be made as soon as practically possible even if minimal information is available. Notifications will generally be made by the senior manager on-site, however all employees have the right to contact corporate oversight for assistance at any time during an emergency event.

8. NOTIFICATION OF LOCAL GOVERNMENT (outside agencies)

The General Manager or his designee is responsible for insuring that the local government is notified of the emergency. Notifications should be coordinated through corporate communications or senior corporate personnel familiar with these types of communications (corporate environmental, corporate safety, corporate legal, senior executives, etc.).

HAZMAT RELEASES AND ENVIRONMENTAL NOTIFICATIONS

The Control Room Operator is responsible for the notification of the appropriate management personnel when there is a hazardous materials release. Hazardous material releases in excess of EPA reportable quantities will also be reported to the Local Emergency Planning Committee designee and the National Response Center.

The CRO is also responsible for notifying a member of Plant Management when abnormal conditions of environmental control equipment exist. The General Manager or designee will ensure that proper notifications to appropriate government agencies are made.

Notification will be made by the methods prescribed by the individual regulatory authority.

5. MEDIA & PRESS RELEASES

All media/press release information shall come from the senior manager on site and shall be approved by the General Manager or corporate communications. **Under no circumstances shall other plant employees communicate with the media/press or general public.**

Any employee who is contacted for information should inform the inquirer that "they should contact the appropriate site manager for information," and refer them to the media/press staging area or tell them to contact the Emergency Coordinator.

LOCAL GOVERNMENT RESPONSE

In order to provide the most efficient response to emergencies, all response and recovery activities must be coordinated through a central location or organization. The local Emergency Response Agencies will activate the Incident Command System, (approved by the National Fire Academy), if response to an emergency requires more than one agency to become involved.

For a complete discussion of the authorities, responsibilities, capabilities, and assignments of these Emergency Response agencies, please refer to the applicable Local and State Emergency Operation Plans.

If at any time, an emergency requires a response the facility and local agencies are unable to provide, the state may be asked to provide additional support to the response effort. If the response requires more than the state can provide, the Federal Emergency Management Agency may be approached to request federal aid be made available.

Several local organizations may also be available to provide support to an emergency response effort. These include voluntary organizations, religious organizations and business organizations. There is a list of Emergency Response Agencies, support organizations and their capabilities to provide resources in the Big Spring / Howard County Emergency Management Services Plan. The resources of the facility are also listed in this Plan under "Contacts".

6. STAFFING CONTINGENCY PLAN

PRI has identified four critical areas relating to staffing. The four identified areas are as follows:

- Availability
- Safety
- Security
- Housing

Even though it is not possible to plan completely against every hazard that poses a staffing risk, preparedness measures for the above areas help reduce the impact of these events if we take certain actions before an event occurs. As such, PRI has planned for staffing continuity to address the aforementioned areas to safeguard the interests of our business and our employees in an emergency event.

This plan is primarily for the guidance of full-time employees, temporary employees, and managers while carrying out PRI's ongoing operations during an emergency event that has the potential to disrupt facility operations. PRI recognized the need to serve all customer obligations despite the fact that a substantial number of employees may be absent for work. An emergency event has the potential to create a difficult and unnatural work environment, which places an increased burden on all employees who are able to report for work as normal. This Plan sets forth some of the policies and procedures that will govern our employees. However, many situations will develop that are not covered in this Plan. Those will have to be dealt with as they arise with the assistance of those employees able to report to work and others set up to assist in the response effort (see Corona Virus staffing documents for reference). Staffing contingency details are set forth in this Plan.

6.1 Staffing Contingency Policy

It is PRI's intent to maintain service to its customers to the fullest extent possible given the resources at hand. Success in operating during an emergency event is dependent upon the availability of employees and the full cooperation of all employees who continue to report for work in performing assigned tasks.

6.2 Assumptions

A. Safety and Compliance:

1. PRI places the safety of its employees and contractor personnel above any other consideration. During emergencies, field personnel work long hours and in many instances under unusual conditions which introduce hazards for the employee. All personnel should be alert to the increased accident potential of emergency work and take extraordinary measures to guard against accidents -- job planning should be emphasized. Safe procedures should be consistently practiced. The importance of working safely should be repeatedly stressed. Particular attention should be given the general welfare and morale of all personnel. The General Manager or his designee will be the primary contact for safety and compliance related issues.

B. Timing and Duration:

1. Emergency events can occur at any time with little or no warning. Therefore, it is critical that staffing plans be updated on a regular basis and kept readily available. The impact of such an event is indeterminate due to multiple variables that will not be identical during an event.

C. Personnel:

1. Operations activities during an emergency event would be conducted by contract personnel, management, available hourly personnel and other company personnel at remote locations not impacted.

7. Event Experience

A. Operations:

1. Successful operation during an emergency event will require a nucleus of experienced plant employees with the necessary knowledge and skills to perform normal work activities. The Plan also anticipates that qualified resources will be provided through staffing from third-party contractors and qualified personnel from throughout the Company. Such people qualified to lead and train others in this work can be found in managerial or supervisory positions in like operations within the company.

B. Special security measures:

1. Under the guidance of the General Manager, may be necessary during an event to properly control access to the facilities. Planning should include careful assessment of the locations where uniformed security guards will be needed. Prior arrangements must be made with a qualified agency to provide security guards when needed.

C. New work assignments:

1. Are often more strenuous and more hazardous than some normal employee activities; hence, extra diligence is required to avoid minor health problems and personal injury

accidents. Appropriate safety instruction, safety equipment, and well-planned procedures are necessary. All illnesses and injuries must be treated promptly and reported.

D. Proper training and testing:

1. To ensure replacement personnel have the necessary qualifications to complete the required tasks associated with their job duties during an event are essential. PRI's management team will work jointly with Environmental Services, Corporate Safety and other available employees to complete the necessary training and testing prior to any employee being released to perform a job task.

E. Awareness:

1. It is important to keep all employees well informed on staffing plans, employee availability, problems being encountered in the operation, and resolutions. Successful operations are dependent upon thorough communication regarding any issue both on and off the job.

8. Responsibilities for Detailed Plans and Execution

A. General

1. Continued operations are dependent upon available qualified staffing, a thorough analysis, and development of contingency plans to address the emergency conditions.
2. Available plant personnel will be assigned to duties where their qualifications are best utilized. Vacations or leaves of absence of persons required for plant operations will be cancelled or rescheduled.
3. Work schedules will be developed to meet PRI's needs. Two 12-hour shifts per day may be necessary. Where possible every effort will be made to allow at least one day in seven away from work for each employee.

B. Operations Coordination

1. The General Manager or his designee will supervise development and execution of the Plan including:
    - Determine the need and timing of a commitment to procure special materials, services and issue instructions to execute the Plan.
    - Direct the organization to make timely preparations for manpower to fill the needs of the operation. Authorize commitments for qualified contractors, qualified work leaders and the identification of available personnel.
2. When the likelihood of a disastrous event is apparent, the General Manager will alert key support personnel to make all timely preparations and will authorize commitments for materials, supplies, and special services required for continued operations.
3. Each functional department (see contacts) will assist with the coordination of needed activities under the direction of the General Manager.

C. Manpower Requirements

1. The General Manager will oversee and coordinate all plan activities including the development of a manning table to assure qualified people are available to meet all anticipated needs. Work schedules should provide for a minimum of one day in seven away from work for each employee if possible. The General Manager will develop a summary of requirements for uniformed security guards if needed, indicating specific location of anticipated assignments.
2. The Operations & Maintenance Manager will be responsible for maintaining continued plant operations with all available manpower resources from qualified contractors, plant employees, and other company employees who will perform the required operations tasks. General Manager and Operations & Maintenance Manager will coordinate training on site specific equipment.
3. The VP/Chief Accounting Officer will provide necessary accounting support to ensure all accounting/financial requirements are maintained.
4. The Manager of Environmental Services will provide the support necessary to ensure environmental compliance is continually maintained.
5. Human Resources will develop and maintain a list of employees who may be utilized for operations duties where their qualifications are best utilized to provide continued plant operations. Where personnel with special skills from outside the work group are required, the Human Resources Manager will assist with locating these individuals and arranging for on-site assistance.
6. Purchasing support will be provided by the Director of Procurement located in the Urbandale, IA.

D. Materials, Supplies and Services

1. The Operations & Maintenance Manager shall review the status of critical equipment, stocks of regularly used materials and supplies, and their availability on short notice. Based on this review, appropriate restocking of items shall be initiated where lack of supply would be critical.
2. The Operations & Maintenance Manager will review all maintenance needs and activities to determine staffing needs and work schedules.

E. Meals

1. It may be necessary to furnish employee meals. The General Manager will make necessary arrangements to ensure all employees are furnished meals and other necessities as needed.

F. Procurement Services

1. Purchasing
    - Those items of materials and supplies normally stocked for general use, such as motor vehicle fuels and lubricants, janitorial supplies, etc., should be stocked to the minimum levels or above.
    - An inventory of special materials or services required upon advance notice of an event will be made to verify availability on short notice. Any items requiring more than one-week lead time for procurement will be called to attention of the General Manager. This verification of availability will include such items as:

        Uniformed security guard services.

Catering service for hot food meal preparation.
Delivery service of mail and minor supplies.
Laundry service (clothing and bedding).
Nonperishable food items, as specified.
Other materials or services, as specified.

2. General Services Staff

   The Manager of Human Resources will be available to provide advice and counsel as required to personnel on duty. Human Resources will respond to all requests for aid from families of all employees.

9. Employees

A. Special Considerations - General

1. The Company places the safety of its personnel above any other consideration. In circumstances of an emergency event, personnel may be required to work long hours, and in many instances, in circumstances that are unfamiliar to them. All personnel must be alert to the increased accident potential in these circumstances and take extraordinary measures to prevent accidents. Carefully planned, safe-working procedures must be consistently used. Special training will be provided in safe work methods and procedures. Particular attention should be given to the general welfare and morale of all personnel.
2. Operator Qualification: All employees and contractors must use qualified employees for covered tasks. The successful execution of the Plan will largely be dependent upon the available resources with the required qualifications. Non-covered tasks may be performed by employees and/or contractors with the requisite knowledge and skills.

3. To the extent possible any contract work should be awarded well in advance of a work interruption.

4. Review the status of critical equipment, stocks of regularly used materials and supplies, and their availability on short notice. Start material procurement far enough in advance to ensure adequate supplies.

5. List of special materials, supplies, and services that will need to be acquired and on hand during an event. This list should be in sufficient detail for the Purchasing to verify its availability and lead time for delivery.

10. FUEL (Natural Gas)

Continued operations are dependent upon the availability of natural gas, a water supply and the ability to transport to the site. Transportation interruptions and possible supply restrictions could occur during an event. PRI does not have in-place storage capabilities for natural gas and would be dependent upon the restoration of the natural gas market, supply and transportation infrastructure for continued operations.

Natural Gas - PRI's dependency on others for fuel supply and transportation negates its ability to directly manage this risk, however, pre-event improvement in relationships and communication with counterparties will likely provide opportunity to expedite a recovery post event. Check with pipeline company to determine outage schedules and possible deferral or reduced down time options.

11. TRANSMISSION

PRI is wholly dependent upon others to maintain the supervisory control and physical integrity of the transmission grid. PRI does participate in event and recovery exercises with local control areas and their transmission operators to expedite a recovery post event.

12. ADMINISTRATIVE SUPPORT

Accounting

The vast majority of PRI's accounting and accounts payable functions are handled by corporate support at various locations outside of Texas. If there were a situation where an event rendered PRI inoperable, it is conceivable that corporate accounting could operate as it does today. If there were a situation where the corporate office encountered a disaster, certain key accounting personnel could work from a remote location, such as a home office or from an affiliate location. If corporate personnel were not available, PRI would first turn to the Berkshire Hathaway Energy Des Moines headquarters office. Many of the senior executives with Berkshire Hathaway Energy have the history and knowledge with this platform and could manage the accounting function and hire additional resources to staff as needed. Key business accounting processes have been reviewed and have established contingency plans in place to support continued business operations for PRI.

Bank Account

The Berkshire Hathaway Renewables treasury department maintains the listing of existing bank accounts and account numbers. Separate accounts and multiple bank accounts exist at each plant (revenue, investment, debt service, etc.). Accounts payable personnel keep back-up copies of pertinent bank account information on site. Additionally, minimum order quantities of check stock exist on site that can be used for small purchases.

VP Legal

Responsible for providing assistance with media/press releases, and all legal notifications.

Corporate Communications

Will assist with official media/press releases.

VP and Chief Accounting Officer for BHE Renewables

Will work with on-site managers to conduct a business impact analysis to determine the financial and operational impact and will assist with reporting and coordination of accounting needs. Will ensure that adequate arrangements are established for retaining appropriate expenditure records resulting directly from the incident.

Director of Risk and Insurance Management

Will establish and maintain communication with the company's insurers or their appointed agents. Will ensure that adequate arrangements are established for retaining appropriate records relating to the incident.

Director IPP Environmental Services

Will work directly with site environmental person to determine environmental impact and reporting requirements. Will provide assistance with all clean-up efforts and disposal. Environmental coordinator will be the primary point of contact for all state and federal safety agencies.

Manager HR & Administrative Services
Will provide assistance with implementing staffing contingency plans. Including deployment of staff welfare, counseling and support activity. Will work directly with on-site IT person to determine impacts to all critical control/communication equipment

IPP Procurement Project Manager
Will provide assistance with plant purchasing needs including service contracts, bid solicitations and procurement.

13.SUPPLIES

PRI has on-site spare inventories for most components that may be required, including some critical spares with business recovery plans. Spares inventory information is shared among platforms through the site risk management plans in order to enhance availability in the event of an emergency. Out-of-area vendors used by other Berkshire Hathaway Energy locations will be utilized in the event of an unavailability of local supply. Minimum inventory levels of bulk chemicals are maintained on-site and checked on a weekly basis. These chemicals can be procured from suppliers other than normally contracted, but may require sacrificing preferential pricing, terms, and conditions. PRI maintains relationships with other operating facilities having similar generating equipment, which may also be a potential source of prime mover hardware parts. Additionally, new contract language has been developed and is being negotiated in vendor service agreements and supply contracts.

14. PLAN TESTING/MAINTENANCE

PRI will update this plan on an annual basis and will conduct periodic testing to ensure proper plan functionality. Testing methods:
Tabletop reviews
Section testing
Simulations
Phone checks
Plan drills

Reviews will be conducted by plant management and the safety committee. Document control will be maintained by the Project Analyst.

12.0 Contacts

12.1 EMERGENCY PHONE NUMBERS

LOCAL EMERGENCY SERVICES (Local Law Enforcement, Fire, Ambulance) _____ **911**

ONEOK Westar Gas Emergency Dispatch _____ 1 800-562-5879

Poison Control Center _____ 1 800-222-1222

Texas Department of Public Safety:

Texas Department of Public Safety, Austin_____512-424-2000

Texas Department of Public Safety –Midland, TX
Communications (24 Hour Number) _____ 432-498-2366
or 432-498- 2131

Texas Department of Public Safety, Big Spring _____432-264-7777

Texas Ranger, Austin, TX_____512-424-2160
Lieutenant Clark_____432-498-2122
CID (Special Crimes Unit) _____432- 498-2361

Texas Ranger, Midland_____432-498-2120

Federal Bureau of Investigation:

FBI Abilene Regional Office_____325-675-8044
Agent Janet Thomas (Abilene) cellular _____ 325-668-8569

FBI Dallas Office _____ 972-559-5000

Howard County Emergency Management:

Howard County Local Emergency Coordinator……911

Big Spring Emergency Local Emergency Coordinator……..911

Other Emergency Telephone Numbers

Delek Refinery, Central Control_____432-263-9529

Qualified Scheduling Entity (currently EDF)_____ 281-653-5828

ONCOR Transmission_____214-743-6897

Luminant Real Time Operations_____214-875-9778

Dial 911

Scenic Mountain Medical Center	**(432) 263-1211**	
Police Department	**(432) 264-2550**	*
City Manager	**(432) 264-2401**	
Howard County Sheriff	**(432) 264-2244**	

Other Routine Business Contacts

DELEK Emergency Command Center	**(432)263-9541, 9542, 0r 9543**	*
DELEK Safety	**(432) 263-9426**	*
CRMWD "Raw Water"	**(432) 267-6341**	*
Oneok "Gas Control"	**(800) 562-5879**	
Main Entrance Gate	**(432) 263-9272**	
EDF Energy Services	**(281) 653-5828**	
DELEK Central Control Room	**(432) 263-9512**	
DELEK Main Gate	**(432) 263-9272**	
AON Insurance	**(402) 697-1400**	
Impairment Notification	**(800) 243-8222 Act#400517**	
Nalco (Randal Cotton)	**(432)-634-4103**	
Lee Rental	**(432) 263-6925, 517-0578**	
ERCOT	**(512) 248-3030**	

***Two-way radio located in control room**

12.2 PRI MANAGEMENT PERSONNEL

Derek Graves, General Manager _____ Cellular__ (712) 509-3749
Home_____712-749-7102

Waylon Merket, Operations & Maintenance Manager _____ 432-263-9002
Cellular _____ 432-466-6735

Ashley Lefler, Environmental Coordinator _____ 432-263-9005

CORPORATE IT HELP DESK (cyber events) _____ 515-242-4357

Communication of Security Information and the Current Threat Level:

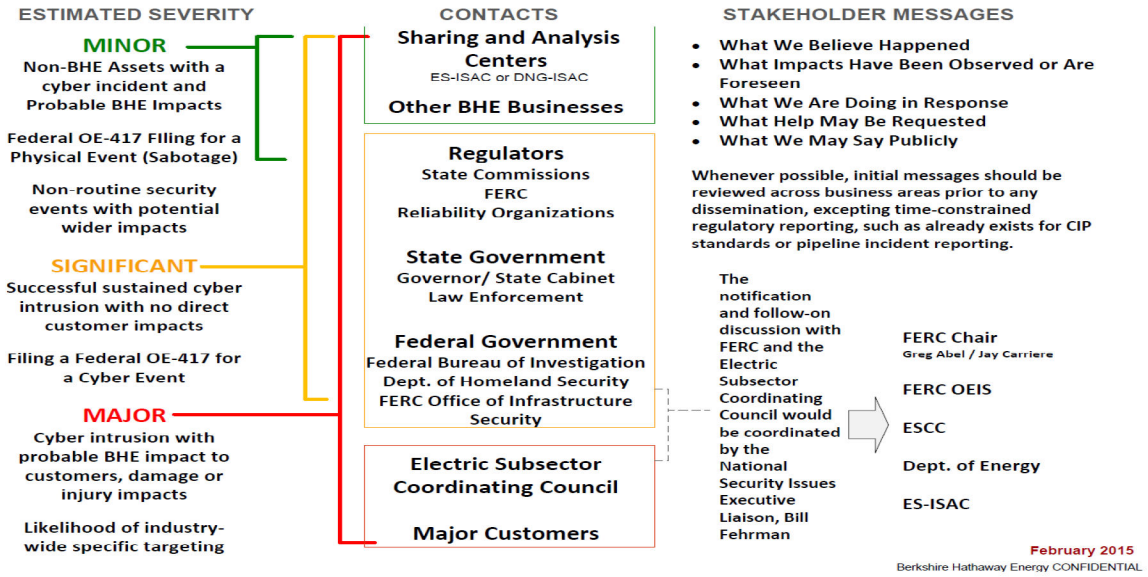
U.S. Department of Transportation
Pipeline and Hazardous Materials Safety Administration, (PHMSA)
National Response Center, (emergency reporting #) _____ 1-800-424-8802
PHMSA Office # _____ 202-366-4433

Current Terrorist Threat Level: http://www.dhs.gov/files/programs/ntas.shtm

12.3 CORPORATE

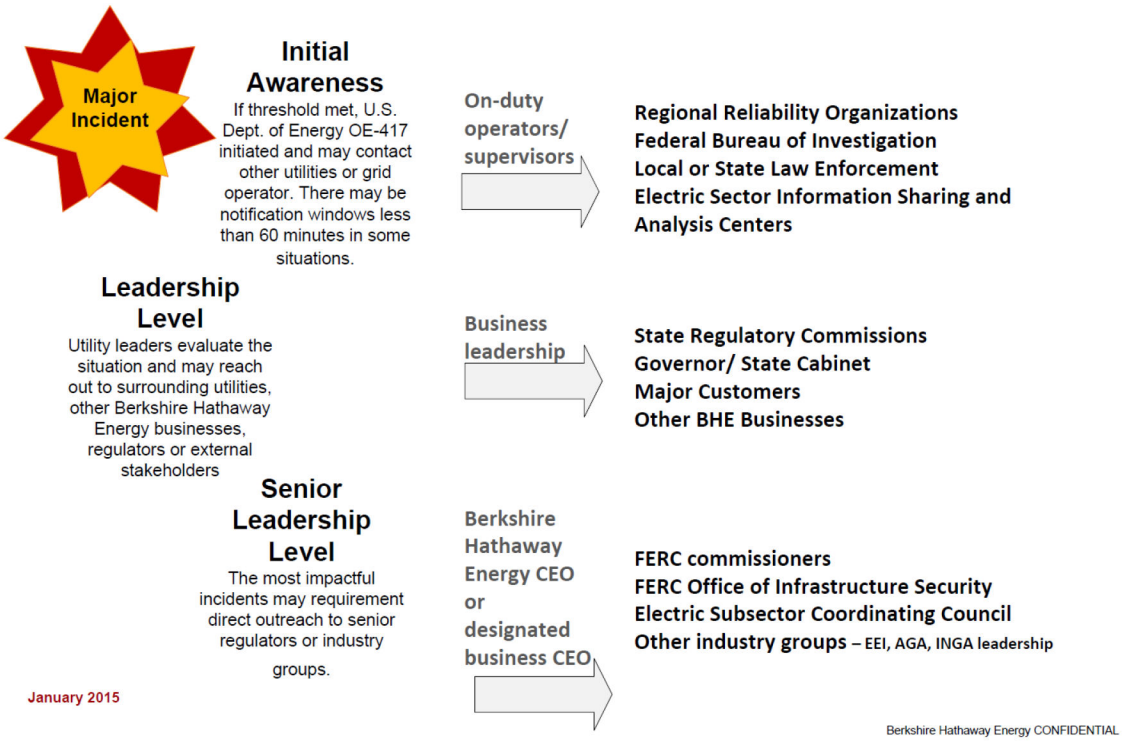
U.S. Security Notifications, Overview

Individual businesses will make a determination on the notification inclusion, order, timing and criticality dependent on the situation and known facts. Regulatory and contractual requirements vary by situation and the utility business profile.



Flow Chart - U.S. Security Notifications in an Electric Event

Individual businesses will make a determination on the notification inclusion, order, timing and criticality dependent on the situation and known facts. Regulatory requirements vary by situation and the utility business profile.



National Security Issues Executive Liaison
Roles and Responsibilities

The National Security Issues Executive Liaison is the U.S. federal agencies coordination point for Berkshire Hathaway Energy outreach within security or resiliency incident. The role is intended to meet the leadership obligation BHE has as part of the Electricity Subsector Coordinating Council, a joint industry-government policy coordination body. The role also reduces the time and resource demands for any single business to manage a security incident in the U.S.

- The National Security Issues Executive Liaison will generally be senior BHE executive with cultivated relationships with U.S. governmental leaders around security or resiliency issues.
- In a crisis, the National Security Issues Executive Liaison role will provide transparent, timely communication to appropriate parties inside and outside BHE.
- The National Security Issues Executive Liaison works in support of the BHE CEO and in close association with individual business CEOs and legislative/regulatory affairs personnel.
- Individual business will notify the National Security Issues Executive Liaison when significant security events occur or have the likelihood to occur.

Triggers	**To Activate**
If the FBI is expected to be notified as part of the businesses' response. Activation of the BHE Major Incident Notification Protocol for a security or resiliency event. Declaration of national emergency by the President of the United States. Declaration of emergency or disaster by a state governor that is or is likely to generate significant national impact. ➢	Activate the liaison role by contact the following persons in priority order: Alicia Knapp, President, CEO, BHER alicia.knapp@bherenewables.com 515-242-3951 515-777-8354 Peter Grandgeorge, MidAmerican Energy Company PAGrandgeorge@midamerican.com 515-281-2356 515-210-7018

Corporate Support- CONTACT LIST

Corporate Support Contacts

Alicia Knapp President & CEO BHER Office – (515)-242-3951 Cell – (515)-777-8354 e-mail: Alicia.knapp@bherenewables.com	Manager Insurance Maria Fedorchenko Office – (702) 402-1595 Cell – (702) 290-2346 e-mail: mfedorchenko@nvenergy.com
Rob Berntsen SVP General Counsel Office - (515) 242-4042 e-mail: Rob.Berntsten@bherenewables.com	Damian Vallas Procurement GM Office – (515) 242-3086 Home – NA Cell – (515)720-2999 e-mail: DMVallas@midamerican.com

Ashley Lefler Environmental & Safety Specialist O:432-263-9005 C:432-466-4472 e-mail: Ashley.lefler@calenergy.com	Burt Short Manager Human Resources & Admin Services Human Resources/IT Coordinator Office – (760) 348 – 4235 Cell – (760) 604-3820 e-mail: burt.short@calenergy.com
Tom Cross VP and Chief Financial Officer Accounting Office – (515) 253-4953 Cell – (515) 229-7359 e-mail: tcross@BHERenewalbes.com	Mid American IT Support 515-242-4357
Eric Bowen VP Wind and Gas Operations Office – (515) 281-2603 Cell – (515) 201-3680 Email: eric.bowen@bherenewables.com	Eric White Compliance Program Manager Office – (515)281-2676 Eric.white@bherenewables.com
Jennifer Cavanagh VP Human Resources Office – 515-281-2456 Cell: 515-281-2456 Email: JLCavanagh@bherenewables.com	

EMPLOYEE NAME	EXT #	HOME PHONE	CELL PHONE
Graves, Derek	9001		432-213-3063
Merket, Waylon	9002	682-583-6385	432-466-6735
Lefler, Ashley	9006	432-466-4472	325-242-5467
Boyles, Stevie	9005	925-580-1403	925-580-1403
Boadle Eugene	9000	432-263-4914	432-466-3676
Ponce, Joe	9000		325-812-1850
Harrison, Curtis	9000	432-394-4334	432-935-0451
Henry, Murphy	9000		432-816-4960
Hawkins, Curtis	9000	432-267-9656	432-935-9432
Thompson, Joe	9000		432-466-4171
Grant, Michael	9000		325-207-7464
Watson, Danny	9022		325-725-2255
Maddox, Ronald	9015		432-270-0820
Murry, Charles	9015		432-264-6364

Switchyard	9026	Univar- Acid	Fax 432-267-9772
Op's Office	9007	Emergency Order	Control Room Cell 432-213-0641
Control Room	9000	John 432-276-2473	Help Desk 515-242-4357
Breakroom	9011		Fire Protection System Impairment (AEGIS)
Shop	9033	Cary Services	201-508-2755 Acc# 400517
Warehouse	9010	David Veloz	ONCOR 888-313-4747
Conference Room	9013	325-260-9931 cell	Meter#111722524LG Premise #1483362
Demin Lab	9034	432-264-7919 office	[illegible]
Front Door			EDF - Tel # 281-653-1756 Real Time Desk 281-653-5[illegible]
Alon Gate Guard Cell	432-770-8229	Ice Guy- Sierra Springs	EDF - Cell # [illegible]-7702
Alon Shift Foreman	432-935-8155	Robert	McDonald Welding (Kerry) 325-207-1969
Alon Central	432-263-9512	432-210-0177 cell	Ray Kemper (Phillips Fab) 432-935-8327
Alon Water	432-263-9284		Cary Services 432-264-7919John Walker 325-260-881
Alon Gate	432-263-9272		Chris Evans 432-517-0578
CRMWD 800-687-2452	432-267-6070		Nalco - Jereme Sanchez (Main) 940-735-2423
Sid Richardson	432-263-7389 x 7		Nalco - Ashley Hillin (Alt) 325-665-7181
SWT - ON CALL	432-213-0760		Nalco - Randall Cotton (Boss) 432-634-4103
Well Field Meter #58967203			Nalco Emergency Reponse 800-424-9300

12.5 General Contractors
Staffing Agencies:

Granite Services International 1302 N. 19th Street Tampa, FL 33605 Office (813) 242-7400 Email: info@gsinc.com		Kelly Services 999 West Big Beaver Road Troy, Michigan 48084-4782 Office (248) 362-4444 Email: kfirst@kellyservices.com
PIC Company 1165 Northchase Parkway, 4th Floor Marietta, GA 30067 Office – (770) 850-0100 Email: marketing@picworld.com		

Security Agency:

National Security Services Office – (800) 970-3437 Email: GuardsToGo.com

Vendors:

Caustic Brenntag Office-432-367-9121 Fax-432-367-8266		Holiday Inn Express Office-432-263-5400 Fax-432-263-5401
Lime – Bulk Austin White Lime Office-800-553-5463 Fax-512-388-1220		Ferric Sulfate Brenntag Office-432-367-9121 Fax-432-367-8266
Lime – Bags Univar Office-800-777-3342 Fax-432-362-2704		Hydrogen – Bulk Air Liquide Office-800-323-1970 Fax-713-896-2123
Soda Ash – bulk Univar Office-800-777-3342 Fax-432-362-2704		Hydrogen – bottles B&J Welding Office-325-573-0404 Fax-325-573-0804 Air Gas Office-432-267-2332 Fax-432-263-1363
Soda Ash –bags Univar Office-800-777-3342 Fax-432-362-2704		Sulfuric Acid Univar Office-800-777-3342 Fax-432-362-2704

CO2-Bulk Air Liquide Office-800-323-1970 Fax-713-896-2123		Port a potty A+ Septic & Drain Office-432-263-9311 Fax-432-267-7045 Cell- 432-517-0222 Justin May
Office Rental Morgan Building & Spa Charles Wells Office-432-563-1807 Fax-432-563-5940		Bowl A Rama Snack bar 432-267-7485 Office-432-267-7484 Fax-432-267-1644
Air Gas Bottled Gas Office- 432 267-2332		

Contract Labor:

Phillips Fabrication Inc. Office-432-264-6600 Fax-432-267-7629 Cell-432-517-0399 Randy Phillips		
Shermco Office-972-793-5523 Fax-972-793-5542 Cell-469-586-9767 Randy Mazon		Utility Services Office-806-798-5990 Fax-806-698-6280 Cell-806-786-8290 Ben Kunkel Cell- 806-676-4729 Steve Carder
Advance Cooling Tower Office-432-523-3578 Fax-432-523-9328 Cell-432-664-3460 Steve Smith Cell-432-557-0227 Don Spurlock Cell-432-557-0405 Tracy Spurlock		Holiday Inn Express Office-432-263-5400 Fax-432-263-5401
Wood Group Office-281-319-0064 Fax-281-319-0068 Cell-713-206-9807 Chris Wilkinson		GE Office-731-672-3784 Fax-281-812-0634 Cell-713-818-4366 David Moreno Office-281-812-0634 Fax-972-245-3928 Cell-469-964-5777 Sean Henderson
Allied Power Group Office-281-444-3535 Fax-281-444-3529 Cell-713-399-9344 Fred Price		Eagle Construction and Environmental Office 800-336-0909 Big D Environmental Services 432-688-8100

Southwest Disposal Service Office 432-366-1833		General Electric David Moreno - Office 713-672-3784 Cell – 713-818-4366 Fax – 281-812-0634 David.moreno@ge.com
Hitachi, Ltd Taite Pernell – 403-278-1881 Cell – 403-278-1810 Fax – 403-589-0089		Phillips Fabrication 432-263-6600 Universal Construction 432-263-9503 Neighbors Well Service 432-263-8444
Shermco Industries Mike Moore Office 972-793-5523 Cell- 214-263-5809 Fax – 972-793-5542		Oncor Electric Delivery Office 432-264-5703 Cell 432-413-4810 Fax 432-264-5710
National Switchgear Roger Harrison Office 972-420-0149 ext. 228		Foxboro Corp Sherri Harris Office 469-737-3917 Cell 214-596-8894 Fax 469-737-3921 sharris@ips.invensys.com
Warren Cat 432-563-1863 432-571-4331 (fire pump rental)		Firehawk 806-351-0011 Simplex Grinnell 806-371-7890 Arrow Automatic Fire Protection 806-866-1071

15. Annexes

15.1 EXTREME WEATHER TEMPERATURES (Heat and Cold)

CONTROL ROOM OPERATOR

Monitor forecasted weather conditions.

Ensure implementation of **Plant Weatherization Plan (see Appendix).**

Call out extra manpower as deemed necessary.

Ensure protective safety measures have been implemented to prevent injury to employees (de-icier applied, proper clothing, frequent breaks, fluid consumption, etc).

Safely secure plant equipment as required.

Notify PRI management of major freeze or heat issues.

Maintains constant communication between the control room and outside operator.

OUTSIDE OPERATORS

Complete defined action items on **Plant Weatherization Plan (see Appendix).**

Keep CRO well informed of actions, observations, etc.

Take frequent breaks to hydrate, warm up or cool off.

Be aware of safety issues resulting from extreme weather conditions and take appropriate correction actions as necessary.

Seek help if required.

MAINTENANCE PERSONNEL

Will assist operations in addressing weather related issues as directed by managers or CRO.

PLANT MANAGEMENT

Department managers will assume EC duties from CRO when arriving at plant site and assist as needed.

MITIGATION PLAN

Monitor weather conditions via internet and weather radio.

Ensure heat trace circuits are properly functioning and maintain constant flows as directed by weatherization plan to prevent freezing.

Keep Energy Management Company apprised of plant operational issues.

Get additional help as required.

Utilize extra heating and cooling sources (fans, heaters, lamps, tarps, water).

Do not issue safe work permits for job task that put protective equipment operations at risk unless absolutely necessary.

Ensure all buildings are properly secured from the elements.

15.2 RESPONSE TO A PANDEMIC/EPIDEMIC EVENT (Disease, Ebola, etc.)

In the event of a Pandemic Event the below steps will be taken with a primary focus being on health and stopping exposure/spreading. One of the key steps is recognizing that a potential event is present and taking preventive step as defined below to prevent manpower shortages, loss of lives, environmental/safety risk, publicity and morale issues (worry, grief, inattention, family concerns).

AFFECTED EMPLOYEE

1. Will immediately notify CRO.

2. Should rapidly leave facility seeking nearest hospital, if unable to leave, self-isolate on company property (library), until medical help arrives.

CONTROL ROOM OPERATOR

1. Will notify 911 and determine the best method for seeking medical attention and isolation needs.

2. Designate someone to notify Emergency Room or care facility that an employee is in route and may have a contagious disease (get instructions on where to go and what to do upon arrival, etc.).
3. Sound gai-troncis system or use radio to notify all employees of potential event and with instructions to remain clear of the employee or isolation area (do not have a group meeting).
4. Notify plant management.
5. Lock down control room (no visitors). If visitors are necessary, the CRO can sign them in and have alternate employee meet them in front of building to conduct business.
6. Notify Delek Gate to prohibit any visitors to PRI with the exception of emergency response agencies.

OUTSIDE OPERATOR

1. Will maintain continuous contact with the control room.

2. Guide emergency response personnel to the proper location. Under no circumstances will the outside operator put him or herself in harm's way.

PLANT MANAGEMENT

1. If on-site will assume EC responsibilities and implement notifications/communications, procedures, etc. as deemed necessary. Refer to Corona Virus plans for guidance documents on staffing, supplies, housing, isolation steps, etc.
2.
3. Notify off-site employees or contractor who may have potentially been exposed.
4.
5. Establish daily conference call with all employees to provide updates.
6.
7. Distribute applicable event information to all employees (signs and symptoms, protective measures, treatments).
8.
9. Contact local health care agencies to determine if there are active cases within the county.

Additional steps to be taken based on severity, isolation needs and to minimize spreading or potential exposure:

1. Staffing

    - Minimize staffing levels (review scheduling needs) to only critical personnel necessary to maintain plant operations
    - Implement customized shift arrangements (split shift and/or segregated work locations)
    - Implement work from home options and corporate job support needs
    - Management team, project analyst, environmental coordinator
    - Suspend in-person contact where possible (maintain 3-feet separation distance)
    - Suspend in-person group meetings
    - Utilize Skype, screen sharing, Zoom, Facetime, etc.
    - Move necessary meeting if necessary, to a larger room where distancing can be maintained
    - Restrict use of common areas (maintain social distancing)
    - Restrict use of lunchrooms to single person only
    - Utilize facility in use signs to avoid accidental occupancy by multiple personnel (restroom, lab, library, warehouse)
    - Eliminate all non-critical site visits (contractors, deliveries, visitors)

- Only scheduled visitors will be allowed entry into the building and only after a discussion on how this will be handled, why it is needed, duration, etc.
- Visitors will not be allowed to enter control room and will be signed in by control room operator via phone call (no in person discussion)
- Establish remote delivery locations for high impact vendors (mail, deliveries, etc.).
- Utilize warehouse as initial drop off spot
- Consider well building at WDW-281 or front gate as alternative
- Adjust critical town runs to optimal low pedestrian traffic times (supplies)
- Purchase supplies in greater quantities to minimize town runs
- Utilize delivery service utilizing drop off point
- Determine optimal town run times to avoid high traffic times
- Suspend all non-critical planned maintenance activities
- Contact contractors to determine what steps are being taken within their organization to minimize or detect the spreading.

2. Isolation Steps
    - Lockdown control room entrance doors
    - Change door combinations and lock all gates
    - Notify Delek Gate to prohibit access to all PRI visitors without prior approval
    - Utilize on-line meetings, phones, e-mail, etc. for performance of LOTO, permits, etc. (verbal authorizations and approvals via phone or email)
    - Eliminate travel where possible (travel plans must be approved by management)
    - Consider off peak times, alternative transportation methods, size of meeting, possible variance alternatives
    - Implement mandatory workstation sanitation needs
    - Wipe down workstations at start and end of each shift (computers phones, doorknobs, commonly shared devices
    - Utilize protective barriers (gloves) for commonly shared devices (doorknobs, keypads, locks, cabinets, etc.)
    - Place disinfectant sprays and wipes in immediate vicinity of commonly shared devices
    - No sharing of work tools (pens, water dispenser, clip boards, phones, etc)
    - Each person will bag their own trash and dispose of prior to exiting facility.
    - Consider early detection methods (temperature, testing methods)

3. Supplies
    - Double per-established minimum inventory levels of infection control supplies (mask, sanitizer, gloves, towels, etc.)
    - Maintain adequate supply of bottled water/food (Patriot Kit, Microwaveable Dishes, canned goods, etc.)
    - Ensure adequate supplies are available for on-site showers, bedding, clothes, hygiene products, bedding, etc.
    - Secure additional rest room facilities, rental trailers for lodging.

- Determine need to purchase additional plant operating supplies (chemicals, reagents, fuel)

4. Communications
   - Utilize alternative communications tools (gai-tronics, radios, cell phones and computers).

5. Review and utilize additional External Resource Options
   - Accounting- process payables, increase spending limits, reporting
   - Human Resources – assist with staffing needs (counseling, time-off, etc.)
   - Communications – corporate will assist with external/internal communications
   - IT – provide additional laptop computers, wireless cards, etc.

MITIGATION PLAN

1. Implement additional protective hygiene measures.
2.
3. Consider additional isolation measures for plant employees.
4.
5. Monitor alerts and news updates via internet.
6.
7. Limit access to control room to only essential operating personnel.
8.
9. Trust your instinct (if something looks suspicious or unsafe it probably is).
10.
11. Immediately report any signs of illness.
12.
13. Get additional help as required.

15.3 Water Shortage Annex

Water Supply - PRI has multiple sources of water supplies (Delek, CRMWD, well field). In the event of a water shortage PRI would take the following steps to conserve water:

A. Minimize blowdown steams to bare minimum (cooling tower, evaporative coolers)
B. Work with water vendor to adjust treatment program needs to protect equipment while optimizing re-use options (cooling tower cycles, backwash reduction)
C. Reduce or stop continually flowing sample streams
D. Remove evaporative coolers from service
E. Adjust RO reject streams for water conservation (consider 80/20 reject)
F. Hold off on demineralizer train regenerations until mix bed fails
G. Discontinue or reduce water sales
H. Reduce steam blowdown

I. Optimize NOx steam injection
J. Maximize demineralizer train throughput (do we need to regin)
K. Determine backwash needs and possibility of delaying
L. Maximize well field production
M. Discuss other supply options with CRMWD
N. Divert RO reject to cooling tower
O. Maximize purchase options from all suppliers
P. Consider trucking options or temporary pipeline supply options

Each item will be evaluated to determine best possible outcome based on water shortage duration and generation needs. Operations personnel will be instructed as appropriate to conserve water usage.

Constant communications with all outside parties is critical to the success of this plan (plant status, how can you help, willing to review and consider all options, etc).

15.4 Restoration of Service Annex

If the emergency situation involved a release of hazardous material, appropriate areas of the plant will be monitored to determine the extent of contamination and concentration. When Re-Entry to a contaminated area is required for inspection or work, the activity will be preplanned, and Plant Safety Policy will be followed.

In cooperation with the local and state agencies, an evaluation will be completed, and recommendations made regarding performance of procedures, personnel, and equipment for re-entry into the evacuated areas.

The objectives following any emergency declaration will be to alleviate the consequences of the event and to take those steps to minimize any effects on the health and safety of plant personnel and the public. Once the emergency situation has ended, the goal will be to restore the plant to normal operating status. For some situations, such as an incident involving a natural phenomenon that has no effect on the plant operation, the emergency situation may not require any change from normal operations; therefore, no formal transition will be required. In circumstances that may involve suspected or actual damage to the plant, a transition will be appropriate. This transition is defined as the **RECOVERY PHASE**.

The General Manager will determine when the Recovery Phase begins. The following guidelines, as applicable to the specific situation, will be observed prior to ending the emergency:

The affected equipment is in stable condition and can be maintained in that condition indefinitely.

Releases of hazardous materials to the environment have ceased.

Fire or other similar emergency conditions no longer constitute a hazard to personnel or equipment.

Once the above conditions have been satisfied, the General Manager will announce that the emergency is terminated, and the plant is in the Recovery Mode. PRI recognizes that the success of this plan will be dependent upon the magnitude of the event and the availability of employees. The PRI facility staffing level consist of 17 employees, requiring employees to work very closely together, and to perform multiple job recovery tasks, with the key focus on employees, safety, equipment protection, compliance, and facility restoration.

The generating plants within BHE Renewables are geographically separated by vast distances and operated independently. The fact that they share similar operating philosophies and primary daily functions gives PRI an advantage in supporting or covering many job functions needed to maintain customer service during local and regional events.

15.5 Hurricane Annex

Not applicable to Projects as none exist within hurricane evacuation zones identified by TDEM

15.6 Cyber Security Annex

A. The purpose of this procedure is to specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) in relationship to Cyber Security Incident Response.
B. Responsibilities
    1. Power Resources personnel and contractors shall notify the Operations Manager of any actual or suspected Cyber Security Incidents.
    2. Operations Manager shall take appropriate responses to Cyber Security Incidents and notify the Plant Manager and CIP Senior Manager.
    3. General Manager, CIP Senior Manager or designee, and Operations Manager shall coordinate on Cyber Security Incident investigation, classification, reporting, and mitigation.
        - Technical Support and Security personnel shall assist in the investigation, classification, reporting, mitigation, and response to Cyber Security Incidents as requested.
    4. General Manager shall ensure that the Cyber Security Incident Plan is updated as necessary.
C. Immediate Response