Example Security Plan

Section 1

PURPOSE:

This Security Plan constitutes the "Standard Operating Procedures" relating to physical, cyber, and procedural security for all (Utility) hydro projects. It contains a comprehensive overview of the (Utility)'s security program, and in some sections, makes reference to other relevant plans and procedures. Security personnel, operators, and selected hydro personnel shall be familiar with the information and procedures associated with this Security Plan.

Distribution: A copy of this plan shall reside in each of the following locations:

- Headquarters Security Operations Center
- Hydro Project Control Rooms
- Systems Operations Center
- Emergency Action Plan Manager
- Plant Managers
- General Counsel (Legal)
- Chief Risk Officer

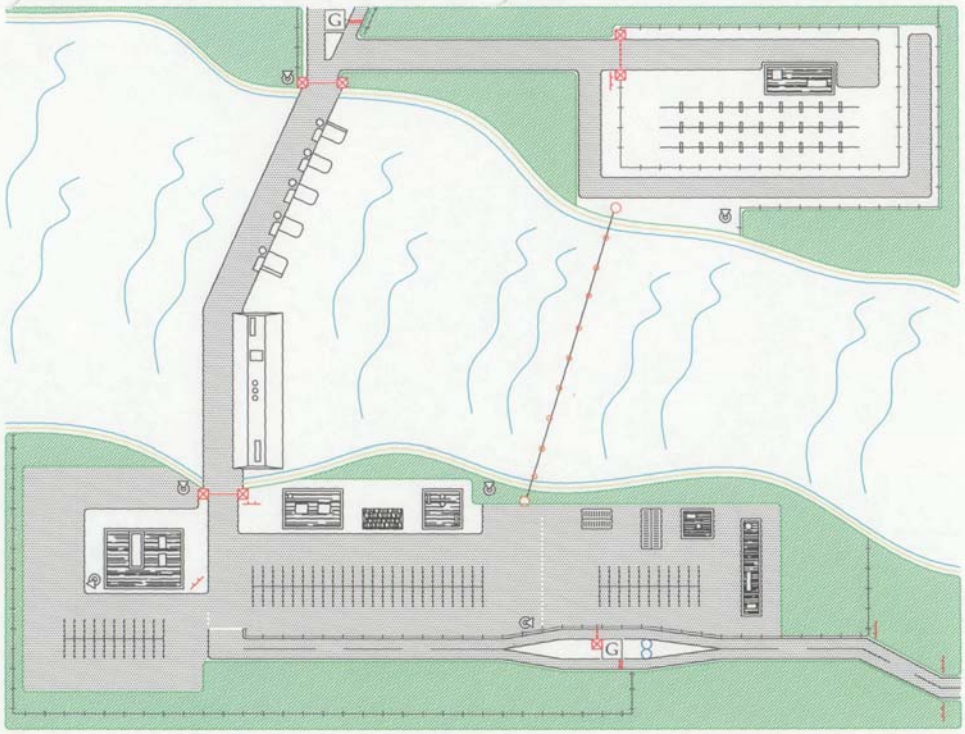
Revision Date: April 29, 2010

Section 2

SITE MAPS:

These site maps reveal the restricted areas of each hydro project, as well as the physical security layouts that protect such areas. The measures listed below are incorporated into the security layouts, and shall be utilized to control and enforce access to the restricted areas:

- Guard posts (with barriers and "Tiger Teeth") - located at each access point
- Placement of fencing, locked gates, barricades, and signage
- Placement of signage and buoy lines - upstream and downstream of dam
- Electronic Access - Identification/access badges issued to employees and approved contractors. Doors and barrier arms can be activated by: 1) employee displaying access badge, or 2) operated by on-site guard, or 3) operated remotely from Security Operations Center.
- "Hydro Access Request" - screening process for contractors and visitors
- Security camera monitoring - 1) Security staff (Security Operations Center), 2) control room operators, 3) Systems Operations Center personnel, 4) Regional dispatch center for law enforcement and fire services, and 5) the State Patrol.
- Intrusion alarm monitoring - 1) Alarm Central (contracted monitoring agency), 2) Security staff (Security Operations Center)
- Contracted guards -- inspection patrols
- Law enforcement - observation patrols



Security Symbol Key

Pole Mounted, Pan/Tilt/Zoom CCTV	G 24/7 Manned Guard Post
Barrier Arm	Vehicle Arrest Bollards
Swing Gate	Security Signage
Tiger Teeth	Boat Barrier
Security Fencing	

Nikolai Tesla Hydro Electric Project

Bill Kamenski | 04/20/10

Section 3

HYDRO PROJECT Critical Physical Dam Related Assets	External access	Physical Security	Detection	Delay	Response	Response Time		Assessment (external)	Assessment (internal)	Security Assessment	Security Plan		Cyber Security
Dam (Structure)													
Spill Gates/Controls													
Intake Units													
Transformers													
Powerhouse													
Generator Floor													
Control Room													
Switchyard													
Transmission													
Abutments													
Fishway Structure Penetrations													
Irrigation Structure Penetrations													
Recreation Structure Penetration													
Visitor Center													
Maintenance Galleries													
Domestic Water													
HazMat storage													
CPME													
CDP&R													

Section 4

SECURITY SYSTEMS:

The (Utility) utilizes a number of security systems designed to help fulfill its security mission. These systems complement the policies, procedures, and measures that form the (Utility)'s robust security program.

The (Utility)'s security systems include:

1. Fencing & Gates

   Fencing is the first layer of security at all of our Hydro projects, Transmission/Distribution points, and (Utility) facilities. The (Utility) has standardized on 8-foot fencing, using tension wire in lieu of bars, placing fence barbs up, and securing the bottom of the fencing below grade. Access points/gates are secured through one of the following methods: Manually opened and secured with a heavy duty (Utility) approved pad lock, electronically accessed with card credential, or electronically accessed with remote gate fob. All perimeters and access points are monitored 24/7 by CCTV or contracted security guards.

2. Exterior Lighting

   Exterior lighting has been strategically placed throughout the (Utility) to emphasize and highlight perimeters, gate and Guard Post access points, entry points into buildings, and areas of interest. Lighting can be activated by motion or photo-cell. Exterior lighting serves as a deterrent, as well as to aid in monitoring of the (Utility)'s CCTV system.

3. CCTV

   The (Utility) has deployed over 100 CCTV cameras throughout the county. These cameras have Pan/Tilt/Zoom (PTZ) capabilities, and are strategically placed throughout the projects. Via our unique Fiber Optic infrastructure, these camera signals are sent back centrally to the (Utility)'s headquarters office where they are recorded 24/7. From this central point, Security has the ability to monitor and control all cameras. In addition, Security shares control and monitoring of these cameras with the Hydro projects, System Operations (Dispatch), Engineering staff, as well as three local law enforcement agencies and Regional Dispatch Center. This CCTV system is monitored 24/7.

4. Electronic Access Control

The (Utility) utilizes a comprehensive Electronic Access Control system, which has been installed throughout the projects and facilities. These card access points secure doors to buildings, access gates, and barrier arms. Through this technology, Security is able to effectively track and control access. Each employee and contractor is required to wear an identification/access badge which is individually tailored for specific access. The (Utility) has also installed a CIP-specific Electronic Access Control system which ensures restricted access to Critical Cyber Asset areas. These Electronic Access Control systems are monitored 24/7.

5. Intrusion alarms

Intrusion alarms are utilized throughout the (Utility). These alarms serve two important functions:

- Provide 24/7 monitoring in remote locations where staff is not always present.
- Installed in all CIP-designated spaces.

The alarm sensors include door/window contacts, motion detection, and glass break. These Intrusion alarm systems are monitored 24/7.

6. Security Guards

The (Utility) contracts the services of a private security company. Guards are stationed at the Hydro Projects. Additionally, "patrol" guards are assigned to conduct security checks of the (Utility)'s properties -- including the hydro projects.

7. Law Enforcement Support

The (Utility) has developed strong partnerships with the local law enforcement agencies. These agencies support the (Utility)'s security mission through collaborative training & exercises, observation patrols, response to incidents, and proactive meetings.

(UTILITY) Closed Circuit Television (CCTV)

CCTV cameras, controls and monitoring have been upgraded and expanded to increase critical infrastructure protection and to:

- Provide enhanced security and safety at (Utility) facilities;
- Provide operational viewing of (Utility) projects;
- Provide safety alerts or response to a major event.
- Provide emergency responders with video coverage (where available) of critical incidents.

Use of (Utility) CCTV is appropriate for security, safety, operational and/or emergency responses.

Use of (Utility) CCTV is not appropriate for monitoring or assessing employee productivity.

Use of (Utility) CCTV is not appropriate for monitoring, without cause, the legitimate behavior or personal conduct of an individual or group of individuals.

General Information:

(Utility) cameras are viewed, controlled and/or <u>recorded</u> at:

1. 911 Regional Dispatch Center 24/7
   (only the cameras being actually viewed on 's three monitors)
2. State Patrol Regional Dispatch Office 24/7
   (only the cameras being actually viewed on WSP's three monitors)
3. Hydro project control rooms (Operators) 24/7
4. County Emergency Management Office
   (only the cameras being actually viewed on CCEM's monitor)
5. (UTILITY) Security Offices 24/7 / 3rd floor Comm Room (HQ)

(Utility) Cameras may be viewed and controlled, but not recorded, at:

6. (UTILITY) System Operation Control (Dispatch) 24/7 and Back-Up Control Center
7. Distribution Crew Dispatch Office (HQ)
8. Hydro Plant Operations Offices (5th floor)
9. Visitor Center, Deputy Station, CM Conf Room
10. Engineering Services Conference Room
11. Fleet Services / T&D Operations / Tech Shop
12. HQ Operations Exec Office

Section 5

MAINTENANCE & TESTING:

The (Utility)'s security systems and equipment shall be properly maintained and tested in order to ensure its continuous and effective operation.

- Maintenance is performed in accordance with the manufacturer's recommendations and guidance.

- Whenever feasible, Maximo (computer program) is used to schedule and track routine maintenance.

- Routine maintenance is performed by a trained group of (Utility) employees who possess the necessary levels of mechanical and technical competence. These individuals are substantially assigned to one of the following work areas: Maintenance Department, Technician Shop, Facilities Department, and Security Division.

- Reference: The Security Division maintains a separate, comprehensive plan in accordance with ***NERC Standard CIP-006-2, Physical Security Program for the Protection of Critical Cyber Assets.*** Maintenance and testing (R8) is described in this plan.

- The (Utility)'s Maintenance and Testing Program is consistent with FERC guidelines.

Section 6

(Utility) Issued Keys:

Purpose

This policy is to be used as a reference when issuing keys within the (Utility). It will also explain our policy for returning keys, reporting lost or stolen keys, the use of unauthorized duplicate keys and loaned keys.

The key system will be entered into the computer-based Key Control Program for on-going maintenance and will be maintained by the Key Administrator. The Facilities Department will program cores and cut keys, and the Key Administrator will issue keys.

1. Issuing Authority - Keys will be authorized in writing for issuance to employees of the (Utility) by one of the following individuals:

    a) General Manager

    b) Executive Managers or their designees

    c) Department Directors or their designees

    If keys are requested from one Business Group that would access another Business Group, written approval will be required from Directors of each unit.

    All approvals will be routed through the Key Administrator. Only in an emergency will a key be issued by Building Maintenance Foreman without the Key Administrator's prior knowledge, and it will require the approval of a Department Director. When a key is issued under these circumstances, the Building Maintenance Foreman will notify the Key Administrator as soon as possible.

2. Who is authorized to have specific keys - Access will be given only to areas where need can be demonstrated.

3. Keys will not be loaned and should not be left unattended - All keys issued on a "permanent" basis should be retained in the possession of the person to whom issued. Keys may not be transferred directly from one employee to another. Avoid the practice of leaving keys on desks, counter tops, etc, or loaning to others.

4. Lost/Stolen Keys - Any person losing a key must report the loss to his or her superintendent/supervisor immediately, who will then report the loss to the Key Administrator. The Security Department along with the Facilities Department will make a determination as to whether the system has been compromised and if a core change is necessary. If a core change is required, that expense will be borne by the department that misplaced the key.

5. Examples of Estimated Core Change Costs

   a) $2,500 - To re-key the substation master

   (Utility) Keys are valuable and should be safeguarded accordingly. Changing keys/cores includes labor, travel time, and materials and requires rescheduling of resources.

6. Duplicated keys - **It is against (Utility) policy to duplicate keys.**

KEY CHECK-OUT PROCEDURES

To maintain consistency and provide predictability, specific checkout procedures shall be followed:

1. Temporary key checkout - Temporary key checkout shall be for a period of 24 hours or less. Any authorized individual will be permitted to check out a key on a temporary basis. The Department Director or his designee shall grant authorization in writing. The individual receiving a temporary key shall provide photo identification at the time of key checkout, upon request. Keys checked out on a temporary basis shall be returned within the 24-hour period. If the individual needs the key for a longer period of time, the key will be checked in and subsequently checked out again.

2. Temporary-loan keys - Vendors and contractors may be authorized to have temporary-loan keys. A Department Director or his designee may authorize in writing the use of temporary loan keys only through the use of the attached temporary-loan key authorization form. Vendors/Contractors will acknowledge all keys received and report all lost or stolen keys immediately. Vendor/Contractor will return all keys within five days of termination of work. If keys are not returned within five days of project completion and it is determined a re-core is necessary, it shall be at the vendor/contractor's expense.

3. Permanent Key Check-out - Permanent keys are issued to employees for the purpose of allowing the employee to access the areas in which they are regularly assigned duties. If keys are requested from one Business Unit that would access another Business Unit, written approval will be required from Directors of each unit. A record of all keys issued will be kept on an employee key authorization form (see attachment), and maintained by the Key Administrator. New employees will be issued keys for their work needs as indicated by the Department's Director on the intent to hire form. Keys shall be issued to new employees by the (Utility) Security Coordinator at the time the new employee is issued his or her I.D./access badge.

KEY CHECK-IN PROCEDURES

1. Key(s) Check-in - When employment with the (Utility) has been terminated, all keys will be returned and noted on the employee authorization form by the Key Administrator. Responsibility for collecting the key(s) shall rest with the Supervisor of the terminating employee. Failure on the part of a Supervisor to collect key(s) from terminating employees may require a key core change, as per Section III, *Lost/Stolen keys.*

ADMINISTRATIVE PROCEDURES

Key Administrator and Building Maintenance Foreman will oversee the management of the keying system of the (Utility).

The design of the (Utility) keying system recognizes four (4) systems, including Distribution, Generation, Facilities, and Administration.

Keys will be recorded and tracked by Key Administrator on an employee authorization form and the Keystone 600 Computer Program with the following information:

- Employee last, first & middle name
- Employee number
- Key marks & numbers
- Date issued
- Term of issuance
- Date returned
- Signature
- Position

The Facilities Department will cut and mark all keys after the Key Administrator has made a key request.

All cores and hardware will be ordered or combined by the Facilities Department after a request has been received from the Key Administrator. The use of all hardware installed in (Utility) locks must be approved in writing by the Facilities Department.

All key core combinations will be determined by the Keystone 600 software and maintained by the Key Administrator or Building Maintenance Foreman.

Contact Information

Security Department

Reference

Policy #704 - Employee, Contractor and Visitor Identification Badges
Policy #104 - Employee Separation Policy

Formerly: _____ Administrative Instruction #31: Key Policy Manual

Section 7

Employee, Contractor and Visitor Identification Badges:

Purpose
This policy provides information on the (Utility)'s Identification Badge Program. The purpose of the program is to enhance the security and safety of (Utility) employees and customers of the (Utility)'s physical and financial assets. The (Utility) realizes the added burden that increased security measures can place on all employees however, security is of utmost concern. It is our desire to work collaboratively as additional measures are imposed to improve the security program.

Each employee/contractor/visitor is responsible for the integrity and safekeeping of his or her badge.

Employee Badges:

1. Employees of the (Utility).

    a) All employees must wear their approved (Utility) Employee Photo ID Badge when entering Secured Areas of the (Utility). Secured Areas are identified as (Utility) buildings and inside the fenced areas of the hydro projects.

    b) The badge must be worn above the waist and be visible at all times to others while in (Utility) buildings with public access and administrative areas.

    c) While performing work in other areas, employees are required to have their badges readily available. Display practices may be modified by Director-level personnel for special work conditions.

    d) Only (Utility)-approved badge display devices (lapel/pocket clips, armbands and lanyards) will be allowed.

2. Any employee who forgets his/her badge should immediately advise his/her supervisor and contact the nearest badge station to obtain a replacement Employee Photo ID Badge. If the badge station attendant does not recognize the employee, or a current picture is unavailable on the badging computer base, the employee's supervisor or supervisor's designee must verify the employee's identification.

3. Any employee who misplaces or loses his/her badge should immediately contact his/her supervisor and the Security Department. After hours, contact the Security Department through System Operations at Ext. 4000. A replacement Employee Photo ID Badge will be issued.

4. Any person, including employees, not wearing a badge in a Secured Area should be questioned by other employees, security guards or other authorized personnel to follow the provisions of this policy.

5. When entering any access-controlled area by vehicle, each vehicle and each occupant must stop to display the proper ID Badge.

6. When entering any access-controlled building or elevator, employees must not allow entry of another person unless the individual displays a proper ID badge.

7. Non-compliance with this policy or any breach of (Utility) security procedures should be reported immediately to your supervisor or the appropriate area security guard.

8. Badges should not be worn off-site unless for official business.

9. All employees serving as Sponsors shall comply with the provisions for contractor and visitor badges.

10. Violation of this policy may lead to disciplinary action, including possible termination.

<u>Contractor Badges</u>:

1. A Contractor is a vendor, supplier, professional service representative or consultant ("Contractors") who has business with the (Utility).

   a) Contractors are required to sign in and receive an identification badge if they will be accessing Secured Areas of the (Utility).

2. Contractors who will be on (Utility) facilities for only one day or less will be provided a Visitor Badge.

   a) Security guards, switchboard operators and receptionists will be trained to issue Visitor Badges to Contractors entering (Utility) facilities.

   b) Contractors should be instructed to wear their badges properly while in Secured Areas of the (Utility).

   c) The employee or project manager whom the Contractor wishes to see will become the "Sponsor" of the Contractor.

   d) Sponsors will be contacted to escort all Contractors into and from Secured Areas.

3. At the request of a Sponsor, a Contractor who will be on (Utility) facilities for more than one day, or who will not be escorted by a Sponsor, will be issued a Contractor Photo ID or Access Badge.

    a) Contractors should be instructed to wear their badge while in Secured Areas of the (Utility).

    b) The badges must be returned to the Sponsors or issuing personnel at the end of each project.

4. Sponsors who authorize photo ID badges for Contractors will be required to make arrangements prior to the work-start date. Pertinent information must be given to designated security badge providers. Time must be allowed at the beginning of a project for photos to be taken and badges to be created for each Contractor representative. [Example: Having a contract crew install fish monitoring equipment at a hydro project will require that the (Utility) engineer or Fish and Wildlife employee be responsible for providing the necessary information, in advance, to the designated badge provider.]

5. Contractors who misplace or lose their badges must immediately notify their Sponsor or (Utility) Project Manager and the Security Department. After hours, contact the Security Department through System Operations at Ext. 4000. A replacement Contractor Photo ID Badge will be issued.

    a) Any Contractor not wearing a badge in a Secured Area should be questioned by employees, security guards or other authorized personnel to follow the provision of this policy.

6. Questions regarding where to obtain a Photo Contractor ID Badge should be directed to (Utility) Security.

<u>Visitor Badges:</u>

1. A Visitor is any individual who is conducting business with the (Utility) (other than those customers in public reception areas to pay bills, etc.) or <u>a family member or guest visiting a (Utility) employee</u>.

2. All visitors to the Headquarters Complex and hydro projects (other than customers conducting business in public reception areas to pay bills, etc., visitors attending open-access commission meetings in the auditorium) are required to sign in and receive a visitor's badge if they will be accessing Secured Areas of these facilities. Exception: Areas open to the general public at Rocky Reach during the season the project is open to visitation by the Public.

3. Visitors who will be on (Utility) facilities for only one day or less will be provided a dated Visitor Badge.

    a) As a courtesy, Sponsors who have visitors arriving for scheduled meetings may provide notice to the designated security badge providers in advance.

b) Security guards, switchboard operators and receptionists will be trained to issue Visitor Badges to visitors entering (Utility) facilities.

c) Visitors should be instructed to wear their badge properly while in Secured Areas of the (Utility).

d) The employee or department the visitor wishes to see will become the "Sponsor" of the visitor.

e) Sponsors will be contacted to escort all visitors into and from Secured Areas.

4. If you have questions regarding where to get a Visitor ID Badge, please contact (Utility) Security.

5. Visitors who lose their badges must immediately notify their Sponsor or the issuing personnel.

Separation of Employment, Completion/Termination of Contractor Services:

Upon separation of employment or completion/termination of Contractor services, (Utility) ID badges must be returned to the supervisor, Sponsor, (Utility) Security, Human Resources or security guard immediately.

Contact Information

(Utility) Security Director, Security Systems Manager or Security Specialist

Formerly:	Administrative Instruction: Employee, Contractor and Visitor Identification Badges
Effective Date:	
Date of Amendments:	

Section 8

(Utility) Security Measures:

Policy #708

Purpose

This policy addresses the responsibility of all employees to comply with (Utility) security measures. Employees and contractors are prohibited from tampering with or obstructing the view of (Utility) security cameras and/or security-related equipment. This policy also addresses interfering with or disabling any other security-related measures.

The (Utility) relies on comprehensive security systems and measures to ensure our employees, contractors and visitors remain safe and our critical assets are protected. Many of these security measures are required by federal law due to the nature of the (Utility)'s facilities. All employees are expected to know and support the security measures related to their jobs.

Security cameras strategically placed throughout the (Utility) have an integral role in security. Unauthorized interference with these cameras can jeopardize people and facilities. Therefore, no employee shall knowingly tamper with or obstruct the view of any security camera or security-related equipment.

The (Utility) has carefully implemented a number of other integrated security measures, including but not limited to: electronic access control, restricted access, intrusion alarms, locked doors/gates/windows, fencing, and signage. No employee shall knowingly disable, circumvent, bypass or compromise any of the (Utility)'s security measures.

Any employee having knowledge of any tampering with, circumvention of or breach of security or security measures shall notify either their supervisor or the Security Division immediately.

Investigations of alleged violations of this policy will be conducted under the direction of the Security director. If the director is unavailable, then the general counsel/chief compliance officer will assume such responsibility. At the conclusion of the investigation, any employees found to be in violation of this policy will be subject to disciplinary action, up to and including termination of employment.

Contact Information

Director- Security Division

Formerly:	New
Effective Date:	
Date of Amendments:	

Section 9

Sabotage Recognition and Reporting:

1.0 PURPOSE

(Utility) facilities are considered critical infrastructure as defined in the National Infrastructure Protection Plan. Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities and systems, and the bulk power system. Such attacks could have cascading effects throughout the economy and society. The purpose of this procedure is to provide guidance to staff on recognizing and reporting potential sabotage events.

SCOPE

What: This document serves as guidance for employees in recognizing and reporting suspicious or unusual activities that could potentially be considered sabotage.

Who: All (Utility) employees

2.0 ROLES AND RESPONSIBILITIES

The following roles and duties are assigned under this program:

2.1 Security Personnel - Responsible for investigating reports of suspicious activities, and for sharing appropriate information with System Operating Personnel, local law enforcement, and investigative authorities. Security Personnel are further responsible for gathering and retaining records of sabotage related events and for reviewing and updating related procedures.

2.2 System Operating Personnel - Responsible for providing the details of suspicious activities related to potential or actual sabotage to appropriate parties within the interconnection, as well as submitting Disturbance Report Form OE-417 in the event of a system disturbance.

3.0 SABOTAGE REPORTING AND RESPONSE PROCEDURES

3.1 Recognizing Potential or Actual Sabotage Activity:

The key to protecting critical facilities is to be conscious of activities in or around critical facilities. Early detection and recognition of potential or actual sabotage events are critical.

Sabotage can be described as a direct effort to disrupt (Utility) operations by destruction, obstruction and/or subversion. Sabotage may be motivated behavior intended to create disruptions in a work or social environment.

Sabotage may be the work of terrorists, hostile individuals or disgruntled employees. It could be the work of a single saboteur or a group of people. Civil unrest can result in attempted sabotage where a specific group's cause may conflict with organizational, governmental or industry goals.

Sabotage attempts may be tied to disruptive events in the work place, such as possible threats to an industry or region and labor unrest. Sabotage events can be cyber, physical and/or operational and may include things like:

- Tampering with transmission towers/poles (physical]
- Disrupting operations by false or real threats (bomb, fire, etc...)(operational)
- Causing intentional failure of critical machinery or systems (physical)
- Deliberate cut of lines supporting SCADA control or other essential communications (physical)
- Loss of a line or major piece of equipment (physical)
- Trip of a major unit (operational)
- Relay intrusions (operational)
- Loss of RTU communication circuitry (operational)

There are a number of suspicious activities that may indicate a potential or actual threat of sabotage. Examples include:

- A large volume of unauthorized access attempts to a 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 any person not directly associated with the (Utility)
- External verbal or written threats to security, software, operations, or facilities by any person not directly associated with the (Utility)
- Minor acts of vandalism at transmission or distribution substations which support critical government agencies or substations that support power system operation facilities
- A series of minor acts of vandalism at numerous transmission 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

It is often difficult to determine if any single activity is an act of sabotage. Employees are must report any activity that appears suspicious in nature. Security personnel will investigate and make the determination if further action is needed.

3.2 Reporting Acts of Potential or Actual Sabotage:

(Utility) employees, who observe an act, event, unusual conduct, unusual inquiry, any questionable or suspicious activity involving (Utility) physical and/or cyber facilities, or personnel, should consider such activity a potential threat. It is the responsibility of all (Utility) employees to report suspicious activities to the Security Department.

Collect and report to Security personnel the following information regarding any suspicious activity:

- Date and Time
- Location
- Physical description of the suspected individuals or vehicle license
- Description of the suspicious activity witnessed

(Utility) employees should report suspicious activity as soon as possible to the (Utility) Security Division. This can be accomplished by initiating a telephone call directly to Security at (telephone), or by submitting a Suspicious Activity/Incident Reporting Form located on the Security Division's webpage.

3.3 Security Personnel Response and Reporting Guidelines:

(Utility) Security Division personnel are responsible for gathering detailed information regarding suspicious activities and relaying that information to System Operations.

The (Utility) Security personnel are also responsible for contacting, coordinating and reporting any such activities to local law enforcement for investigation and response. Suspected acts of sabotage, as well as verified acts of sabotage will be reported to the following investigative agencies:

- Federal Bureau of Investigation (telephone)
- Joint Terrorism Task Force (telephone)
- Washington State Fusion Center (telephone)
- Department of Homeland Security (telephone)/ www.nicc@dhs.gov
- FERC (telephone)
- ES-ISAC http://www.esisac.com

3.4 System Operations Personnel Response and Reporting:

System Operations personnel are responsible for notifying the (NERC Region) Reliability Coordinator as well as other parties within the interconnection deemed appropriate to the circumstance (i.e. neighboring balancing authorities)

Acts of sabotage may potentially result in a system disturbance. In such cases, System operations personnel will submit a Disturbance Report Form OE-417 within the applicable time frame as outlined in System Operating Instruction No. 16.

4.0 DOCUMENT MANAGEMENT AND RECORDS RETENTION

4.1 Document Retention

Documentation shall be maintained that demonstrates current compliance with CIP-001 including procedures, reporting records and any other applicable data needed to demonstrate compliance.

Documentation of non-compliance or evidence used as part of an investigation shall be retained as directed in Section D.1.3 of NERC Standard CIP-001.

Revision History

Owner	Rev. Date	Ver.	Assignment Change	Approved By

References:

NERC Standard CIP-001 System Operating Instruction 16

PUD Today | Back

suspicious activity/incident reporting form

If you suspect a security incident (personnel, physical or cyber), you must take two steps immediately to report the problem:

1. **Call Security at 6[redacted] or call System Operations at [redacted]**
2. ***Fill out the form below.***

[redacted] considered critical infrastructure as defined within the National Infrastructure Protection Plan.

Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities and systems, as well as having cascading effects throughout the economy and society.

Any [redacted] employee who identifies or observes an act, event, unusual conduct, unusual inquiry, questionable or suspicious activity involving [redacted] physical or cyber assets or personnel or the Interconnect should consider such activity as a potential threat and possible precursor to an act of sabotage.

ALL FIELDS ARE REQUIRED.

All information provided will be kept strictly confidential.

Your Information

Name : -- choose one --

What is the best method to contact you ? -- choose one --

Incident Information

Incident Date : and time: : :

Leave blank if UNKNOWN.

Type of Incident : -- choose one --

Incident Activity : -- choose one --

Priority : -- choose one --

Location of Incident :

Witnesses :

Incident Description :

Actions Taken :

Verbal Report To :

Date of Verbal Report :

Cancel | Print | Submit Report

This data is managed from the IncidentReports.accdb database.

T[redacted]

Report Suspicious Behavior and Activity

SURVEILLANCE
Are you aware of anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, etc., near a key facility?

DEPLOYING ASSETS
Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility?

SUSPICIOUS PERSONS
Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment, or near a key facility?

SUSPICIOUS QUESTIONING
Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding a key facility or its personnel?

TESTS OF SECURITY
Are you aware of any attempts to penetrate or test physical security or procedures at a key facility?

ACQUIRING SUPPLIES
Are you aware of anyone attempting to improperly acquire explosives, weapons, ammunitions, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification for a key facility or to legally obtain items under suspicious circumstances that could be used in a terrorist act?

DRY RUNS
Have you observed any behavior that appears to be preparation for terrorist activity, such as mapping out routes, playing out scenarios with other people, monitoring key facilities, timing traffic lights or traffic flow, or other suspicious activities?

Call 911 if there is an emergency or immediate threat.
Call the nearest Joint Terrorism Task Force (JTTF) to report suspicious activity or behavior (see below).
Submit information electronically at https://tips.fbi.gov

Albany (518) 465-7551	Cleveland (216) 522-1400	Kansas City (816) 512-8200	Newark (973) 792-3000	Richmond (804) 261-1044
Albuquerque (505) 889-1300	Columbia (803) 551-4200	Knoxville (865) 544-0751	New Haven (203) 777-6311	Sacramento (916) 481-9110
Anchorage (907) 276-4441	Dallas (972) 559-5000	Las Vegas (702) 385-1281	New Orleans (504) 816-3000	Salt Lake City (801) 579-1400
Atlanta (404) 679-9000	Denver (303) 629-7171	Little Rock (501) 221-9100	New York City (212) 384-1000	San Antonio (210) 225-6741
Baltimore (410) 265-8088	Detroit (313) 965-2323	Los Angeles (310) 477-6565	Norfolk (757) 455-0100	San Diego (858) 565-1255
Birmingham (205) 326-6166	El Paso (915) 832-5000	Louisville (502) 583-3941	Oklahoma City (405) 290-7770	San Francisco (415) 553-7400
Boston (617) 742-5533	Honolulu (808) 566-4300	Memphis (901) 747-4300	Omaha (402) 493-8688	San Juan (787) 754-6000
Buffalo (716) 856-7800	Houston (713) 693-5000	Miami (305) 944-9101	Philadelphia (215) 418-4000	Seattle (206) 622-0460
Charlotte (704) 377-9200	Indianapolis (317) 639-3301	Milwaukee (414) 276-4684	Phoenix (602) 279-5511	Springfield, IL (217) 522-9675
Chicago (312) 431-1333	Jackson (601) 948-5000	Minneapolis (612) 376-3200	Pittsburgh (412) 432-4000	St. Louis (314) 231-4324
Cincinnati (513) 421-4310	Jacksonville (904) 721-1211	Mobile (251) 438-3674	Portland (503) 224-4181	Tampa (813) 253-1000
				Washington, DC (202) 278-2000

To download this poster, visit www.US-CERT.gov

DHS/PD/OIP/HMD/Feb06/v1.0

Section 10

THREAT ALERT GUIDELINES

GREEN - BLUE - YELLOW
ORANGE - RED

Physical Response Guideline for Threat Alert Level

GREEN (Low)

- **Normal security operating standards and procedures.**
- **General workforce awareness.**
- **Security, Threat, and Disaster Recovery Plans reviewed and updated. Annual review as a minimum.**

Physical Response Guideline for Threat Alert Level

BLUE (Guarded)

- **Work force alert to unusual activities and whom to report such activities.**
- **Operational plans and procedures up-to-date, to include:**
    - **Security, Threat, Disaster Recovery, and Fail-Over plans.**
    - **Other Operation Plans as appropriate, i.e., transmission control procedures.**
    - **Determine availability of additional security personnel.**
    - **Determine responsiveness of medical emergency personnel.**
- **Review all data and voice communications channels to assure operability, user familiarity, and backups function as designed.**
- **Review fuel source requirements.**

Physical Response Guideline for Threat Alert Level

- **Implement GREEN and BLUE measures, if not implemented.**
- **Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and employee access control is enforced.**
- **Identify critical and on-call personnel.**
- **Establish communications with law enforcement agencies.**
- **Identify additional business/site specific measures as appropriate.**

Physical Response Guideline for Threat Alert Level

ORANGE (High)

- **Implement measures GREEN, BLUE, and YELLOW.**
- **Place all critical and on-call personnel on alert, consider tabletop exercises.**
- **Ensure all gates and security doors are locked and actively monitored either electronically or by "random walk-by procedures".**
- **Implement enhanced screening procedures for personnel and deliveries.**
- **Limit access to facilities to essential personnel.**
- **Coordinate with fuel suppliers, as necessary.**
- **Inspect site fuel storage and HAZ-MAT (hazardous material) facilities.**
- **Increase liaison with law enforcement and emergency services.**
- **Coordinate critical security programs with adjacent utility organizations.**
- **Consider emergency utility operations/procedures appropriate to available threat intelligence.**
- **Media releases should be reviewed with Security/Alert Level Coordinator prior to release.**
- **Additional business/site specific measures as appropriate.**

Physical Response Guideline for Threat Alert Level

Red (Severe)

- **Implement measures GREEN, BLUE, YELLOW, and ORANGE.**
- **Stop all tours and visitors.**
- **Establish contacts with medical emergency personnel.**
- **Secure all entrances and critical service facilities, such as substations, etc. Consider use of armed security personnel.**
- **Stop all mail and package deliveries directly to site.**
- **Inspect all vehicles entering site.**
- **Fully brief all personnel on emergency procedures.**
- **Establish frequent communications with all law enforcement agencies.**
- **Review plan for returning to Threat Level - ORANGE, YELLOW, BLUE, or GREEN status.**
- **Additional business/site specific measures as appropriate.**

NATIONAL HOMELAND SECURITY THREAT LEVEL

GUIDELINES

Recommended Actions for Individuals, Families, Communities, Schools, Businesses and Government

NATIONAL HOMELAND SECURITY Threat Level Guidelines

User's Guide

The Homeland Security Threat Level Guidelines are designed to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to authorities, the people of the United States, State of Alabama and Tuscaloosa County.

The Homeland Security Advisory System has drawn controversy and criticism, yet no one is yet to come up with a better system. The current guidelines have been refined since they were first released by the U.S. Department of Homeland Security. They now better reflect the recommended actions to be taken by individuals, families, communities, schools, business and government.

The guidelines consist of warnings and instructions in the form of a set of graduated *Threat Conditions* that increase or decrease as the risk of the threat rises or lowers. At each condition, a corresponding set of recommended actions to further reduce vulnerability or increase response capability during a period of heightened alert.

The system is intended to create a common vocabulary, context and structure for an ongoing discussion about the nature of the threats confronting us, and the appropriate protective measures that should be taken in response. It seeks to inform and facilitate decisions.

From lowest to highest the Threat Conditions correspond to various colors. They are:

Low=Green Guarded=Blue Elevated=Yellow High=Orange Severe=Red

The higher the Threat Condition, the greater the risk of terrorist attack. Risk is a function of the probability of an attack corresponding to the potential gravity of its effects. The

National Threat Level is assigned by the U.S. Department of Homeland Security. The system is based on a calculated assessment of risk, based on the quality of the threat information. This quality is based on (but not limited to) the credibility and degree of corroboration of the threat information. The assigned Threat Condition will be evaluated at regular intervals to determine if the level should be adjusted to better define the threat locally. Remember, assignment of a specific threat level does not mean there will or will not be a terrorist attack. The levels are only an indicator of risk.

In addition to the actions recommended in this pamphlet, individuals, businesses and organizations should incorporate standard safety plans and procedures. At home, have a safe place to go to shelter-in-place, a supply of non-perishable foods for self-sufficiency for 72-hours, a gallon of water per person/per day, a flashlight and a battery-powered radio. At work, develop a safety plan.

Homeland Security Advisory System Guidelines

Below are the recommendations for responding to the various levels of terrorist threats. These are not requirements but are suggestions for Homeland Security.

Risk of Attack	Action for Individuals, Families and Neighborhoods	Action for Businesses	Action for Schools
LOW **(Normal operating condition, no threats detected)**	• Develop a disaster plan • Create a disaster kit • Make a plan for your pets if you need to evacuate • Explore volunteer opportunities and volunteer organizations	• Develop a written Emergency Response Plan to address all hazards and natural disasters • Develop an emergency communications • Develop a plan to relocate facilities if needed	• Develop a written Emergency Response Plan to address all hazards and natural disasters to secure safety of students and faculty. • Create an emergency communication s plan containing family contact numbers for students.
GUARDED **(Received threats that do not warrant actions beyond normal liaison notifications. Agencies operate on normal day-to-day conditions.)**	• Follow actions at lower level • Be alert to suspicious activity and report it • Store disaster supplies and replace outdated items • Develop an emergency communications plan with family and friends • Provide volunteer services	• Follow actions at lower level • Be alert to suspicious activity and report it • Establish a dialogue with community leaders and organizations, emergency management, government agencies and utilities about disaster preparedness • Ensure emergency communications plan is updated and equipment is purchased	• Follow actions at lower level • Be alert to suspicious activity and report it • Conduct safety training and emergency drills following the school's written Emergency Response Plan • Ensure the emergency communication plan is updated
ELEVATED **(Intelligence or an articulated threat indicates a potential for a terrorist incident. However, there is no credible threat.)**	• Follow actions at lower levels • Be alert to suspicious activity and report it • Store disaster supplies and replace outdated items • Develop and emergency communications plan with family and friends	• Follow actions at lower levels • Control parking, consider erecting barriers • Contact private security firm for security risk assessment and to determine availability of support • Be aware of suspicious packages • Identify visitors and their destination • Increase security for public events	• Follow actions at lower levels • Ensure that all emergency supplies are stocked and ready • Routinely inspect interior and exterior of building • Be aware of suspicious packages • Identify visitors and their destination • Increase security at public events

HIGH **(A threat assessment indicates a potential threat is credible.)**	• Follow actions at lower levels • Increase alertness to any suspicious activity and reort it • Review your disaster plan • Exercise extra caution when traveling • Develop alternate routes to work or school • Continue volunteering • Be alert at public events	• Follow actions at lower levels • Control entry to parking lot, consider erecting barriers • Restrict parking near building • Conduct random interior and exterior building checks • Limit visitors to essential functions only • Contact vendors and suppliers and identify their employees • Limit building entry points • Exercise extra caution when traveling	• Follow actions at lower levels • Discuss school's written Emergency Response Plan with faculty and staff • Be prepared to alter or cancel school day and public activities • Provide security for traveling groups • Control entry to parking lot, consider erecting buildings • Restrict parking near building • Conduct random interior and exterior building checks • Limit visitors to essential functions • Increase security at public events
SEVERE **(An incident has occurred or is imminent)**	• Follow actions at lower levels • Cancel any travel • Contact employer to determine operational status • Consider canceling attendance at public events • Monitor broadcast media for updated information	• Follow actions at lower levels • Consider need for closing • Consider reducing work force to essential employees only • Be ready to work from an alternate site if evacuated • Monitor broadcast media for updated information • Increase 24/7 facility security	• Follow actions at lower levels • Activate school Emergency Response Plan • Close school if recommended by authorities • Check all IDs and provide escorts for those entering building • Be prepared to evacuate • Ensure Emergency Alert Radio is operational • Monitor broadcast media

Government Response

Risk of Attack	Action
LOW	• Develop and maintain Emergency Operations Plans and Standard Operating Procedures • Conduct training and exercises • Ensure communications capabilities and interoperability
GUARDED	• Follow actions at lower level • Review physical security for all facilities • Restrict unauthorized entry to sensitive areas • Ensure all employees wear visible picture identification • Be alert to suspicious activity and report it
ELEVATED	• Follow actions at lower levels • Remind all personnel to be suspicious and inquisitive and maintain heightened awareness of people, vehicles and activities • Increase spot checks of specific high-risk targets/facilities. Check for suspicious or unattended packages. • Do not leave emergency response or other government vehicles unattended. If it is necessary to leave the vehicle, lock it and check the vehicle and its chassis underside before opening doors and starting engines. • Move vehicles and objects (trashcans etc.) away from buildings. • Lock and regularly inspect all buildings, rooms and storage areas not in use. • Randomly inspect interior and exterior of buildings • Inspect suspicious packages
HIGH	• Follow actions at lower levels • Limit access points to critical infrastructure and facilities to absolute minimum and strictly control entry procedures. • Restrict parking near government buildings. • Increase security patrols. • Erect barriers and obstacles to control traffic flow at key facilities. • Limit access of vendors and suppliers. • Limit access to only a main entrance. Check all visitors' purpose, intent and identification. Ensure that contractors have valid work orders and employees are legitimate. Escort all visitors to sensitive facilities. • Keep critical response vehicles in a secure area.
SEVERE	• Follow actions at lower levels • Keep all vehicles away from buildings • Consider closing all government facilities to the public and/or reducing workforce to only critical personnel • Search all briefcases, packages etc. • Increase security patrols

The world has changed since September 11, 2001. We remain a Nation at risk to terrorist attacks and will remain at risk for the foreseeable future. At all Threat Conditions, we must remain vigilant, prepared, and ready to deter terrorist attacks.

For further information, download a copy of *Terrorism: Preparing for the Unexpected* at http://www.redcross.org/services/disaster/keepsafe/terrorism.pdf.

Section 11

EMERGENCY RESPONSE:

Emergency response shall be in accordance with an "all-hazards" approach. Such incidents/events may include:

- Bomb Threats
- Fires
- Earthquakes
- Hazardous Materials Release
- Floods
- Windstorms
- Civil Disturbances
- Pandemic Flu
- Serious Accidents
- Criminal Activity

The (Utility) shall implement the principles of the Incident Command System (ICS) when managing significant incidents/events. Implementation may include:

- Assemble an Incident Management Team **(organizational chart attached).** Assignments will be based upon individual qualifications and positions.

- Coordinate with internal and external stakeholders (i.e. law enforcement, fire services)

- Establish Unified Command when appropriate

Emergency Action Plans (EAPs) - The (Utility) maintains EAPs for each of its Hydro projects. These EAPs should be referenced during the course of any emergency. Information contained in these EAPs includes:

- Notification Flow Chart
- Project Description
- Responsibilities
- Inundation Maps

EMERGENCY TELEPHONE NOTIFICATION

Security: (Names and telephone numbers)

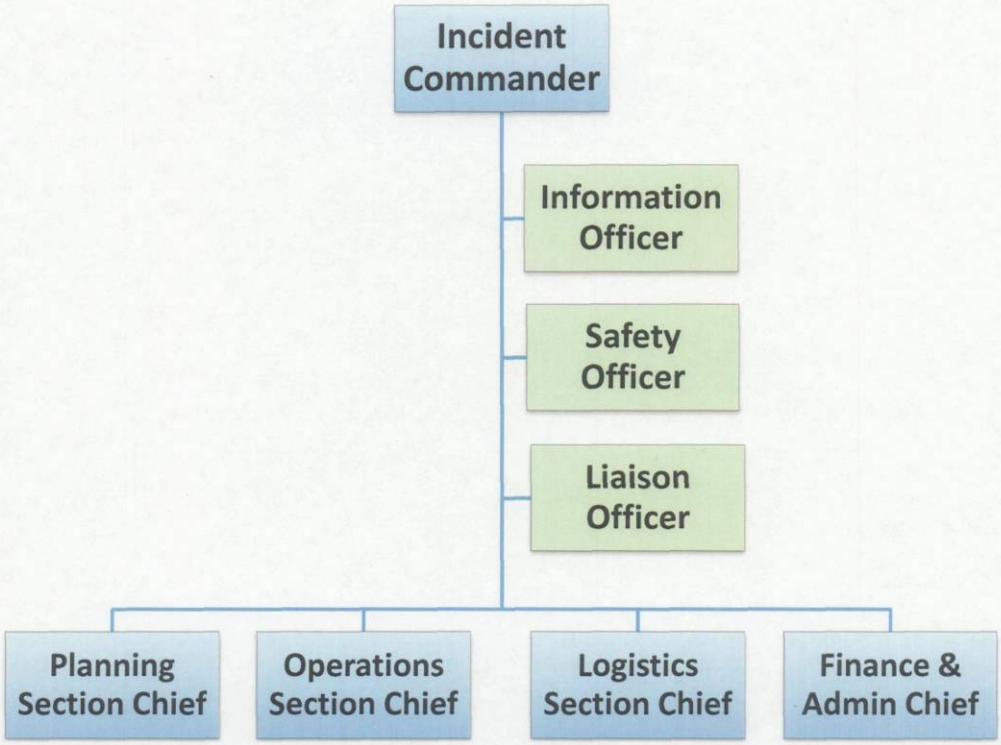
Non-emergency	(telephone number)
Emergency	9 – 1 – 1

System Operations (telephone number)

Control Rooms

Hydro Project A	(telephone number)
Hydro Project B	(telephone number)
Hydro Project C	(telephone number)

[redacted]
Incident Management Org Chart



OBJECTIVES

1. Maintain operation of *critical business functions* and delivery of essential services.
2. Protect the health & welfare of our employees.
3. Protect [redacted] assets.
4. Effectively communicate to our employees and our stakeholders.

GUIDANCE - Suspected Explosive Devices

What might indicate "suspected explosive devices?"

- Package or other object unexplained or out of place.
- Short piece of pipe
- Tinfoil
- Sawdust
- Brick dust
- Wood chips
- Electrical wire out of place
- String or fishing line
- Dirty ropes (fuses)
- Partly open drawer
- Fresh plaster or cement
- Disturbed carpeting
- Loose electrical fittings
- Greasy paper wrapping

1. Do not touch the device.

2. Evacuate and cordon off the IMMEDIATE area surrounding the suspicious device.

3. Call 9+911 or 911 and designate individual to meet emergency responders upon arrival.

4. Call Security
   - Notify Safety
   - Notify GM or next Executive Manager available
   - Notify Systems Operations
   - Notify Communications Division

5. UTILIZE STANDARD TELEPHONES ONLY. Do not activate mobile (2-way) radios or use cellular telephones.

6. Refer to Emergency Action Plan as appropriate

GUIDANCE - Suspicious Mail

CHARACTERISTICS OF SUSPICIOUS PACKAGES AND LETTERS:

- Excessive postage.
- Handwritten or poorly typed addresses.
- Incorrect titles for recipient.
- Addressed to no particular person in (Utility).
- Title, but no name.
- Misspellings of common words.
- Oily stains, discolorations.
- Plain envelope with no return address.
- Excessive weight.
- Lopsided or uneven envelope, thick or lumpy package.
- Ticking or buzzing sound, sloshing sound or unusual smell.
- Protruding wires or aluminum foil.
- Excessive security material such as masking tape, string, filament tape, etc.
- Marked with restrictive endorsements, such as "Personal" or "Confidential", or alternatively, "Open This Envelope."

IF YOU RECEIVE A SUSPICIOUS UNOPENED ENVELOPE OR ENVELOPE THAT APPEARS EMPTY:

- Call Security
    - Notify Safety

IF YOU RECEIVE A SUSPICIOUS PACKAGE:

- DO NOT OPEN
- DO NOT PANIC
- DO NOT TOUCH, SMELL, TASTE OR TRY TO ANALYZE THE SUBSTANCE
- LEAVE IT and evacuate the room
- KEEP others from entering
- Compile a list of others who were in the immediate area to ensure complete follow-up.
- Call Security
    - Notify Law Enforcement
    - Notify Safety
    - Notify GM or next Executive Manager available.

IF YOU RECEIVE A SUSPICIOUS UNOPENED ENVELOPE WITH POWDER WHICH SPILLS OUT:

- Leave it and evacuate the room.
- Wash hands with soap and water.
- Call Security.
  - Notify Law Enforcement
  - Notify Safety
  - Notify GM or next Executive Manager available.

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

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 carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by e-mail:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected Delivery
- Poorly handwritten
- Misspelled Words
- Incorrect Titles
- Foreign Postage
- Restrictive Notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- Follow your local guidelines
- Federal Protective Service (FPS) Police
  1-877-4-FPS-411 (1-877-437-7411)
- 911

BOMB THREAT CHECKLIST

Date: _____ **Time:** _____

Time Caller Hung Up: _____ **Phone Number where Call Received:** _____

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (Background and level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice

- ❑ Accent
- ❑ Angry
- ❑ Calm
- ❑ Clearing throat
- ❑ Coughing
- ❑ Cracking voice
- ❑ Crying
- ❑ Deep
- ❑ Deep breathing
- ❑ Disguised
- ❑ Distinct
- ❑ Excited
- ❑ **Female**
- ❑ Laughter
- ❑ Lisp
- ❑ Loud
- ❑ **Male**
- ❑ Nasal
- ❑ Normal
- ❑ Ragged
- ❑ Rapid
- ❑ Raspy
- ❑ Slow
- ❑ Slurred
- ❑ Soft
- ❑ Stutter

Background Sounds:

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

Other Information:

_____

_____

Threat Language:

- ❑ Incoherent
- ❑ Message read
- ❑ Taped
- ❑ Irrational
- ❑ Profane
- ❑ Well-spoken

_____

_____

_____

Homeland Security

Building Evacuation

Reasons to evacuate may include:

- Fire
- Bomb Threat
- Power Outage
- Earthquake
- Water/Gas Leak
- Hostage Situation

Methods of Notification

1. Intercom system
2. Alarm.
3. Direct or electronic from authorized emergency personnel.

Do Not

1. Use elevators.
2. Gather in lobbies.
3. Bring disabled individuals into stairwells without fire department approval.
4. Open a door without first checking for heat.
5. Run or panic.
6. Re-enter the building until authorized.

Disabled individuals or others who need assistance should:

1. Be assisted by Floor Wardens (Sweepers).
2. Be evacuated only under the direction of authorized emergency personnel (i.e. Fire Department).

Course of Action:

- Emergency recognized.
- If the emergency is a fire, delegate another employee to try to extinguish it with the nearest fire extinguisher.
- Call 9+911 or 911.
- Intercom announcement:
    - **"Attention, Attention, Attention.**
    - **An emergency has been reported.** o
      Evacuate the building at once.
    - **Use the stairs.**
    - **Avoid the elevators."**
- **Preserve any and all evidence,** if applicable, and remain accessible for discussion with law enforcement personnel.
- **Do not touch any suspicious items** or suspected bombs.

Employee Responsibilities:

1. Each employee is expected to know the location of the fire extinguishers, emergency exits, and first aid supplies.
2. Extinguish the fire by using a portable fire extinguisher if safe to do so and if you have been trained to use a fire extinguisher.
3. Evacuation Route-Preplan your escape route based on your familiarity with the building. Always take the nearest stairwell. All stairwells are fire corridor rated.
4. Do not re-enter the building.
5. Regular review of attached floor plans and evacuation plan maps is recommended.

Floor Wardens (Sweepers):

1. Recognized as a designated authority in the event of an emergency.
2. Responsible for the evacuation in their designated area and will assist other floor wardens as need.
3. Equipped with identifying apparel and a flashlight.
4. Responsible for complete evacuation.
5. Responsible for knowing the general identity and physical ability of employees in the area.
6. Familiar with the location of emergency exits, emergency equipment, and trained in emergency response procedures.

Section 12

GENERAL STATEMENT:

(Contracted Security Company) provides contracted services to the (UTILITY). This manual addresses policies, procedures, and information associated with these services.

This manual is intended to serve as a guide to (Contracted Security Company) employees, so they may understand the expectations of conduct and performance. This manual will assist them in making decisions and carrying out their duties in a manner consistent with those expectations. It should be noted that this manual is not intended to address every situation that may arise. (Contracted Security Company) employees are expected to use good judgment in all situations.

TABLE OF CONTENTS

SECTION I - Rules of Conduct

1. Guards shall conduct themselves in a professional manner at all times. They shall treat everyone with courtesy, dignity, and respect. Guards should remember that they not only represent (Contracted Security Company), but also the (Utility).

2. Guards shall not sleep or engage in any activities or personal business which would cause them to neglect or be inattentive to duty (i.e. playing games, watching non-work-related television/videos/DVDs). Guards shall not read a book, magazine, or newspaper while on duty and in public view, except as may be required in the performance of duty.

3. Guards shall not engage in conduct which:

    a. Impedes the ability of (Contracted Security Company) and/or (UTILITY) to effectively fulfill its responsibilities.

    b. Causes a lessening of internal or external confidence in the ability of (Contracted Security Company) and/or (UTILITY) to perform its functions.

4. Whenever someone approaches the guard post, guards shall exit the guard shack and deliver a proper greeting. Guards shall ascertain the person's intentions, and respond with appropriate assistance and/or direction.

5. Guards shall maintain strict confidentiality regarding all matters that are sensitive in nature.

6. Guards must be proficient in the proper operation of equipment such as telephones, radios, computers/keyboards, and others as required.

7. Guards will wear their issued (UTILITY) photo ID Badges whenever on duty.

SECTION II - Appearance Standards

1. Uniforms and equipment shall be kept neat, clean, and in good repair. Guards should remember that a professional appearance helps gain the respect and confidence of others.

2. Hair and all other grooming styles shall be neat and conservative in appearance. Any styling or accessories (i.e. body piercings, non-conservative tattoos, etc.) that detract from a "professional image", as determined by the (UTILITY)'s Security Division, will be prohibited.

3. Guards will wear black undershirts, black socks, and black footwear. Any exceptions must be authorized by the Division Manager or Guard Supervisor.

4. Guards will wear a (Contracted Security Company) approved hat.

5. Guards shall keep their stations and vehicles clean and neat. Garbage containers shall be emptied during the last shift, daily.

SECTION III - Post Operations

1. GATES/BARRIER ARMS

    a. Post #2 and Post #5 have a designated "visitor" entry lane, and a designated "employee" entry lane. The employee lane is restricted to only employees. Employee badges are identified by a blue stripe with the wording "EMPLOYEE". All other traffic must proceed through the visitor's lane (including any employee not in possession of his/her badge).

    b. Guards shall require all persons who enter through the visitor's lane to stop and produce valid identification and/or issued badges. Guards shall raise/lower barrier arms for each individual vehicle, and not allow more than one vehicle at a time to pass through. These identification/access procedures shall be followed each time an occupant attempts to enter the property - no matter how many times that person has already entered and departed.

    c. Some employees may arrive on bicycles and attempt to enter through the "exit" lane. On these occasions, guards shall direct the bicyclist through the "employee" lane, where the bicyclist must swipe his/her badge. (Note: When a bicycle passes through, the barrier arm may not automatically close. In these cases, it may be necessary for the guard to lower the barrier arm by dragging an object, such as a chair or shovel, across the pavement cuts.)

    d. Any mechanical problems with the barrier arms should be reported as soon as possible.

2. CAMERA MONITORING

    a. Guards shall monitor the security cameras relative to their assignment. Guards shall maintain a record of their monitoring and any activities they observe.

    b. Guards are authorized to move the security cameras only for security-related reasons.

c. Guards shall report any activity of "significant interest'* to the Guard Supervisor and the Security Director immediately.

d. Guards shall report suspicious (potential criminal) activities to.

3. SECURITY ROUNDS

a. At the beginning of each round, Guards shall first notify Control. Then, they shall announce their departure on the security channel and lock up their posts before departing. While making their rounds, Guards shall take their keys, portable radio, scanning wand, and appropriate PPE.

b. Guards shall report each location upon their arrival. They shall check all doors and locks, making certain to scan all buttons with their wand.

c. When outside their security vehicle, Guards shall leave the vehicle running and activate the emergency lights. Guards shall wear required PPE and orange coat or reflective vest.

4. PATROL SCHEDULE

a. Hydro A: November 1st through March 14th (Hydro A Park/Visitor Center is closed to the public) - Guards shall conduct one round at the end of their shift.

b. Hydro A: March 15th through October 31st (Hydro A Park/Visitor Center is open to the public) - After the park/Visitor Center closes for the evening, Guards shall sweep the property to ensure all visitors have departed. Guards shall also lock the restrooms. ((UTILITY) staff will unlock the restrooms
in the morning.) Guards shall report any discovery of graffiti or vandalism.

c. Hydro B: Guards shall conduct one round prior to ending their shift.

d. Guards at Hydro A and Hydro B shall not conduct their round simultaneously.

5. SAFETY EQUIPMENT

a. Guards shall wear their issued hard hats whenever they are outside of their vehicle during the making of rounds.

b. Wherever designated, guards shall wear the required personal protective equipment (PPE) — hard hat, eye protection, ear protection, protective footwear.

c. Public-Safetv/Response Personnel -- During "emergency" situations, responders (law enforcement, fire, medical) shall be allowed to enter the property without being stopped or challenged. Whenever responders arrive under "normal" (non-emergency) conditions, Guards shall greet them and offer appropriate verbal assistance. It is not necessary to issue visitor badges to responders. After normal business hours, Guards shall notify the Control Room that a responder has entered the property. Guards shall record this information on their daily activity log (DAL).

2. EMERGENCY EXCEPTIONS - PERSONEL RISK ASSESSMENT

a. The Personnel Risk Assessment (PRA) program is designed to enhance the protection of Critical Cyber Assets (CCA), by ensuring persons who access CCA areas do not pose an unacceptable risk to the reliability of the Bulk Electric System. Subsequently, the (UTILITY) enforces strict procedures regarding unescorted/escorted access.

b. During rare and exigent circumstances (i.e. fires, medical emergencies, criminal activity), it will be necessary to allow emergency responders (law enforcement, fire, & medical personnel) access into Critical Cyber Asset areas. In these cases, exceptions from the normal Critical Infrastructure Protection (CIP) standards must be allowed. During such circumstances, **the**
(UTILITY) Security Division will provide direction to (Contracted Security Company). This direction may include stationing a Guard on site, outside of the CCA area. The Guard's primary responsibility shall be to monitor access. The Guard shall record the identities and affiliations of all personnel who enter, the times of entry/exit, and a detailed description of activity.

SECTION VI - Chain of Command

1. NOTIFICATIONS

a. Guards shall immediately notify the appropriate Security and/or (Contracted Security Company)
personnel whenever the following occurs:
- Emergencies
- Incidents of notable interest
- Situations requiring supervisory guidance
- Situations of uncertainty

b. Guards shall contact the Guard Supervisor for all other matters involving general inquiries, suggestions, supply requests, etc.

c. Succession of Command for SECURITY is:
   - Director
   - Security Systems Specialist
   - Security Access Manager

d. Succession of Command for (Contracted Security Company) is:
   - Division Manager
   - Guard Supervisor
   - Night/Day Watch

2. DAY/NIGHT WATCH AUTHORITY

a. The Day/Night Watch acts under the authority of the Guard Supervisor, and will occasionally provide direction to the guards.

SECTION VII - Care & Operation of (UTILITY) Vehicles

1. (UTILITY) vehicles may be used only for official business.

2. Guards are authorized to operate (UTILITY) vehicles only on (UTILITY) property.

3. Vehicles shall be kept locked when parked, unless Guards are in immediate attendance.

4. Guards shall keep vehicles clean - both interior and exterior.

5. Guards shall obey all laws, and drive in a careful and prudent manner at all times.

6. Guards shall transport any person in a (UTILITY) vehicle, except in the line of duty or with supervisory approval.

7. Code-carrying designees are responsible for refueling the vehicles.

8. Guards shall complete an inspection form at the beginning of each shift. Guards shall record the checking of fluids, observations of damage, discovery of defective equipment, etc. Any discovery of "new" damage shall be reported to the Guard Supervisor immediately.

9. Guards shall not change the pre-set radio frequencies in any (UTILITY) vehicle.

SECTION VIII - Credentials & Badges

1. BADGE TYPES

   > **Electronic Access** -- This Badge Type has properties that allow it to operate doors, gates and barrier arms.

   > **ID Only** — This Badge Type does not have properties that allow it to operate doors, gates, and barrier arms.

2. BADGE COLORS

   The (Utility) currently utilizes eight Badge Colors:

   > **Blue:** Current and retired employees
   > **Silver:** All Law Enforcement, Guard Service, and First Responders
   > **Red:** Contractors without the authority to enter Hydro Project Plants
   > **Green:** Contractors with the authority to enter Hydro Project Plants
   > **Purple:** Professional Services consultants and specialty contractors
   > **Light Blue:** Vendor/Delivery badges
   > **Pink:** Contractor Day Use badges
   > **Yellow:** Visitor badges

3. BADGE VISUALS

4. VISITOR BADGES -- ISSUANCE

   Visitor badges may be issued to persons who have business-related appointments, or guests of employees.

   When issuing visitor badges, Guards shall obtain photo-identification, telephone numbers, and vehicle license numbers. This information shall be recorded in the Visitor Log. Guards shall not issue any badge without first verifying the identity of the visitor(s). If the visitor is unable to produce identification, Guards shall call the Security Division (or respective Control Room) to gain permission for badge issuance and access. Guards will record the name of the person who authorized the access.

   If the visitor has an appointment, the Guard shall call the person they are visiting to confirm the details of the visit.

   Occasionally, employee family members will arrive on site. These persons will also require issuance of badges. (For young children, it is acceptable to record the names and not issue badges.)

5. TEMPORARY EMPLOYEE BADGES -- ISSUANCE

   Occasionally, (Utility) employees will arrive on site without their issued access badge. In these cases they may be issued a Temporary Employee Badge. Guards shall record this information on their DAL.

6. RETIREE BADGES

Whenever a retired (UTILITY) employee requests access, Guards shall:

- Match the badge photo to the person.
- Call the person the retiree intends to visit, and confirm permission to enter.
- Allow entry. No visitor badge is necessary, provided the retiree has a badge in his/her possession. If not, a visitor badge shall be issued. *(Note: a "Retiree " badge does not guarantee entry unless an active employee on site agrees to the visit.)*
- Guards shall record the information on their DAL.

SECTION IX - Radio & Communications Procedures

Guards shall adhere to the following procedures whenever using (UTILITY) radio equipment:

1. The "Security" channel shall be used for all radio communication. Guards shall communicate in a clear and professional manner at times.

2. Once every hour (during the day), Post #2 shall conduct a radio check. Example: **"All posts, this is Post 2, making a 0810 Radio Check."** All Guards on duty with a radio will respond. Examples: **"Post 5, Patrol and Night/Day Watch."**

3. When Post #2 or Post #5 depart for their security checks, they shall advise the other Guard. Examples: **"Hydro A Security leaving on security rounds at 2100." "Hydro B Security back from security rounds at 2100."**

4. All Guards on patrol (Patrol, Hydro A/Hydro B Security) shall advise their location upon arrival. Upon departure, they shall advise their destination. Examples: **“Patrol leaving (Contracted Security Company) office, en route to Headquarters." “Patrol arriving at Headquarters." “Patrol leaving Headquarters area secure, en route to Fish & Wildlife."**

5. Whenever Guards call out their status, Post #2, Post #5, and Night/Day watch will answer **"Post (2 or 5) and Night/Day Watch received (or copies)."** If the radio traffic is unclear, Guards shall ask to repeat. Example: **"Night/Day Watch to unit responding, please repeat your radio traffic."** If the radio traffic is still unclear, Night/Day Watch should make contact via cellular telephone and then broadcast the message. Example: **"Night/Day Watch received or copies, Patrol arriving at Destination".**

6. Whenever Patrol receives an alarm call, they shall it out over the radio. Example: **“Patrol received an exterior door alarm for destination at 2130."** At this point, Night Watch (if on duty, otherwise, Post #2) will respond over the radio. Example: **"Night/Day Watch received (or copies) Patrol received an exterior door alarm for destination at 2130."**

7. Whenever Guards initiate security sweeps, they shall identify themselves, their location, and the current time. Example: **“Patrol doing a security sweep of Destination for an unlocked door at 2215."** Night/Day Watch (if on duty, otherwise, Post #2) shall acknowledge by repeating the radio traffic. Example: **"Night Watch received, Patrol doing security sweep of Destination for an unlocked door at 2215."** When the security sweep is completed, Guards shall identify themselves and advise the status of their sweep. Example: **“Patrol finished with security sweep of Destination, area is secure at 2230."**

8. Patrol units shall announce their status whenever they are out of the vehicle. Examples: **“Patrol out of the vehicle at North End restrooms at destination." “Patrol back in the vehicle, restrooms are secure".**
Night Watch shall acknowledge by repeating the radio traffic.

9. Patrol units shall be specific in reporting their locations and activities. When encountering persons in the park at night, Guards shall explain the hours of closure and direct them to leave. Guards shall record all relevant information (i.e. physical descriptions, vehicle license numbers) and advise over the radio. Example: **“Patrol observed (#) subject(s)/vehicle(s) at destination, they were advised to leave (if after hours)."** If the subjects remain in the park, Guards shall make the appropriate notification. Example: **“Patrol to Night Watch, subject(s)/vehicle(s) are still in the area, preparing to call."** Post #2 and Post #5 will copy/receive and Night Watch will repeat. Example: **"Night Watch (copies or received) Patrol, preparing to call at destination at (time)."**

10. Whenever a Guard is conducting a security sweep, or is out of the vehicle, the Night/Day Watch (if on duty, otherwise, Post #2) will conduct "status checks" every 2 minutes. These checks will continue until the Guard responds that he/she is secure/clear. Example: **"Night Watch to Patrol, status check".**
Response: **“Patrol clear" (or state problem).**

11. The calling of is the responsibility of the security officer in direct contact of the situation, since he/she is in the best position to relate complete and accurate information. This information must be passed on to the Night/Day Watch as soon as possible.

12. The calling out of license plate numbers over the radio is at the **Patrol's discretion.** License numbers having any relevance (to the Guards' security duties) shall be recorded on the DAL.

Section 13

INFORMATION TECHNOLOGY/SCADA:

The (Utility) is committed to protecting its Critical Cyber Assets.

- The SCADA network is physically isolated from other networks, with one exception: One
  specific host on SCADA is allowed to send certain data through a proxy-based firewall to a
  specific repository on the corporate network.

- Reference: The Security Division maintains a separate, comprehensive plan in accordance
  with ***NERC Standard CIP-006-2, Physical Security Program for the Protection of Critical***
  Cyber Assets.

- Attached: Administrative Policy - CIP Cyber Security Policy

CIP CYBER SECURITY POLICY

Table of Contents

Overview

Background:

As technology has progressed, concern regarding the protection of Bulk Electric System Critical Cyber Assets has grown as well. In 2003 the North American Electric Reliability Corporation (NERC) Board of Trustees approved the implementation of Urgent Action Cyber Security Standard 1200 (UA 1200), which eventually evolved into the NERC Critical Infrastructure Protection (CIP) standards. The stated purpose of the CIP standards is "to protect the Critical Cyber Assets (hardware, software, data, and communications networks) essential to the reliability of the bulk electric system." On January 17, 2008 the Federal Energy Regulatory Commission (FERC) issued order 706 approving NERC CIP standards and making them mandatory and enforceable pursuant FERC authority.

Purpose:

The purpose of this Policy is to clearly demonstrate the commitment of the (Utility)'s management to the security and protection of cyber assets deemed critical to the operation and reliability of the Bulk Electric System. Management is dedicated to fostering a culture of compliance among all employees. The information contained herein is intended to serve as a framework and provide guidance to (Utility) staff in the management, access to and protection of Critical Cyber Assets.

Scope:

This Policy applies to all (Utility) personnel, contractors, and vendors. This Policy sets the direction, gives broad guidance, and defines the requirements for cyber security related processes, programs, and actions across the (Utility). This Policy should be considered in conjunction with administrative policies regarding internal compliance.

Leadership Responsibility

The (Utility)'s Executive Manager-Operations Group (or an equivalent position of responsibility and scope within the (Utility)'s senior management) shall serve as the Senior Manager with overall responsibility and authority for leading and managing the (Utility)'s implementation of and adherence to Standards CIP-002 through CIP-009. As such, the Senior Manager's responsibilities include annual review and approval of the (Utility)'s CIP Cyber Security Policy as well as approval of any exceptions to that Policy. The Standards call for specific actions by the Senior Manager. As allowed by Standards CIP-002-2 through CIP-009-2, the Senior Manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented as required under Standard CIP-003 and approved by the Senior Manager.

The Senior Manager is responsible for ensuring that adequate resources are dedicated to cyber security and CIP related compliance activities. Day-to-day responsibilities for cyber security and CIP compliance activities are delegated to others based on job function.

In accordance with CIP-003, R2 the contact information for the Senior Manager is included herein:

Name:
Title: Executive Manager - Operations Group
Date of Designation:

Responsibilities

Cyber security is the responsibility of all (Utility) employees, contractors, and vendors.

The (Utility) is committed to consistent enforcement of this Policy and cyber security. This Policy is a directive in compliance with federal reliability standards. All responsible managers and supervisors are required to communicate this program to appropriate employees and implement this Policy. Employees are responsible to know and understand their roles and responsibilities.

The following (Utility) positions oversee and implement cyber security for all Critical Cyber Assets owned by the (Utility). The references to specific position titles apply to positions with equivalent responsibility and scope in the event there is a change in personnel or titles:

Executive Managers: Provide additional leadership, guidance and oversight of the cyber security programs and activities.

(Utility) Compliance Manager: The (Utility) Compliance Manager is responsible for independent review of compliance policy, programs, and processes to verify compliance with NERC CIP standards. The Compliance Manager is also responsible for updates to this policy, and ensuring annual senior management reviews and approvals.

Regulatory Compliance and Policy Development Manager: Ensures compliance with NERC CIP standards through oversight of operational programs, processes and procedures. Further responsibilities include: resource coordination, regulatory reporting, tracking and monitoring of standards, communication of requirements, and compliance documentation management.

Director - Security Division: Responsible for the development, implementation, and enforcement of the (Utility)'s Physical Security Plan. The Director -Security Division has additional responsibilities of managing and monitoring the day-to-

day activities related to physical security and ensuring CIP compliance goals and deadlines are met. Other responsibilities include the implementation and management of Physical Security Perimeter Access Control and Monitoring systems, which facilitate the protection of Critical Cyber Assets.

Operations Reliability Manager: Responsible for recommending and managing cyber security operational procedures and resources designed to protect the (Utility)'s Critical Cyber Assets and ensure compliance with applicable NERC Reliability Standards. The Operations Reliability Manager has additional delegated responsibilities of managing and monitoring the day-to-day activities related to cyber security and ensuring CIP compliance goals and deadlines are met.

Control System Engineers/Analysts ("CSE Group"): Under the direction of the Operations Reliability Manager, the Control System Engineers/Analysis (CSE Group) are responsible for the development, deployment and maintenance of the (Utility)'s Critical Cyber Assets, including control system networks. The CSE group is responsible for identifying, implementing, and documenting the hardware and software used to meet NERC CIP requirements.

Critical Asset Manager: (Utility) managers with oversight for critical Bulk Electric System Assets as defined within the methodology developed pursuant to NERC Standard CIP-002 are responsible for approving and revoking access to Critical Cyber Assets and/or their associated information.

Critical Cyber Asset Identification

The (Utility) uses a risk-based assessment methodology to identify Critical Cyber Assets (CCA). This methodology was developed pursuant to NERC Standard CIP-002. The assessment focuses on the potential impact to the reliability of the Bulk Electric System should critical systems be lost or compromised.

Critical Asset Identification

Using the risk-based assessment methodology the Transmission Systems Department Manager shall identify Critical Assets. The Critical Asset List is developed and maintained in accordance with the procedure for the *Identification of Critical Assets.* The information contained therein is considered classified pursuant to CIP-003, R4 and will be disseminated according to the (Utility) ***Administrative Policy - Public Disclosure of Documents*** and the ***CCA Information Classification and Protection Program.***

Critical Cyber Asset Identification

(Utility) Critical Cyber Assets are identified by further applying the risk-based methodology to the list of Critical Assets. The list of Critical Cyber Assets is developed and maintained in accordance with the procedure for the *Identification of Critical Cyber Assets.* The information contained therein is considered

classified pursuant to CIP-003, R4 and will be disseminated according to the (Utility) ***Administrative Policy - Public Disclosure of Documents*** and the ***CCA Information Classification and Protection Program.***

CCA Annual Review and Approval

Annual reviews of Critical Cyber Asset policies, risk-based assessment methodology, lists, and programs are performed as specified in NERC standard CIP-002 and the associated (Utility) programs. All annual reviews will be performed as detailed in the individual procedures. Final annual approval of the risk-based assessment methodology, the Critical Asset List and the Critical Cyber Asset List will be completed by the Senior Manager or delegate(s).

Personnel Risk Assessment and Access

Essential to the protection of Critical Cyber Assets is the careful control of access to those assets. It is the policy of the (Utility) that all persons granted unescorted physical or authorized cyber access to (Utility) Critical Cyber Assets undergo a Personnel Risk Assessment prior to being granted unescorted physical or authorized cyber access to a defined Critical Cyber Asset except in specified circumstances such as an emergency. Risk Assessments shall be conducted in accordance with the (Utility)'s ***Personnel Risk Assessment Program.*** It is the responsibility of the Director - Security Division to complete personnel risk assessments. It is the responsibility of the Regulatory Compliance and Policy Development Manager to manage the ***Personnel Risk Assessment Program*** in accordance with applicable NERC standards.

Access to Critical Cyber Assets shall be carefully managed. Revocation of Access shall happen within 7-days for personnel changes. For employees terminated for cause access shall be revoked within 24-hours. Access lists shall be reviewed quarterly to ensure appropriate access rights for employees.

Awareness and Training

The protection of Critical Cyber Assets can be fostered through proper education and security awareness. Both training and awareness activities should emphasize the importance of protecting and securing Critical Cyber Assets.

The (Utility)'s *CIP Cyber Security Awareness Program* shall serve as a mechanism to ensure that personnel having authorized cyber or unescorted physical access to Critical Cyber Assets or the associated information receive on-going reinforcement in sound security practices. The *CIP Cyber Security Awareness Program* serves as the first layer of cyber security education.

Persons granted unescorted physical access and/or authorized cyber access to Critical Cyber Assets (including non-(Utility) personnel) are required to complete annual training

on applicable cyber security policies and procedures, physical and electronic access controls, proper use and handling, and recovery action plans. Training will be customized based on the need of the individual and will be conducted in accordance with the *CIP Cyber Security Training Program.*

Information Protection and Control

The (Utility) identifies, classifies, and protects sensitive information associated with Critical Cyber Assets. Protected information includes, but is not limited to, certain operational procedures, asset lists, control network data, floor plans of areas containing critical cyber assets, and disaster recovery plans. Information is classified in accordance with the *CCA Information Classification and Protection Program* and disseminated pursuant to that Program.

Electronic Security

The electronic security perimeter surrounding critical assets shall be identified, protected and secured as directed in NERC standards CIP-002 through CIP-009.

Change Control

Careful control and implementation of changes made to critical systems is a key component of the reliability of those systems. The CSE Group is responsible for change control and configuration management for development, deployment, modifying, replacing, or removal of critical cyber asset hardware or software. The CSE Group develops, documents, and implements the processes which are used to identify, and control most (Utility) or vendor related changes to hardware or software components of (Utility) Critical Cyber Assets. Change control associated with systems used in the access control and monitoring of the Physical Security Perimeter is the responsibility of the Director - Security Division. Change control associated with Intelligent Electronic Devices (IED) is the responsibility of the CM Tech Shop Department Superintendent.

Electronic Security Perimeters

Electronic Security Perimeters are designed as a critical layer of protection around Critical Cyber Assets. All Critical Cyber Assets shall reside within an Electronic Security Perimeter. Electronic Security Perimeters are designed by the CSE Group in accordance with CIP-005 Rl requirements and the procedure for *ESP Identification and Documentation.*

It is important to the (Utility) that appropriate access controls and processes are developed to ensure proper protection of Critical Cyber Assets within electronic security perimeters. Technical and procedural mechanisms are used to control electronic access at all electronic access points to the electronic security perimeter. Specific direction is provided in a group of (Utility) procedures titled *Electronic Perimeter Access Controls.*

All non-Critical Cyber Assets residing within a defined electronic security perimeter shall be identified and protected pursuant to CIP-005 and the applicable (Utility) procedures. All Cyber Assets used in the access control and monitoring of the electronic security perimeters are also protected pursuant to the requirements specific to monitoring systems in NERC CIP standards 002-009.

No dial-up access is permitted to any (Utility) Critical Cyber Asset, or Electronic Security Perimeter access point.

Cyber Vulnerability Assessment

The CSE Group shall annually perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s). These assessments shall be conducted in accordance with (Utility) established *CIP Vulnerability Assessment Procedures.* The process, as well as results of the annual assessment, shall be documented appropriately.

Documentation Review and Maintenance

The Operations Reliability Manager shall direct the review, updating, and maintenance of all documentation which support the Electronic Security Perimeter(s) to ensure the processes and documentation reflect current configurations and practices. All modifications to the Electronic Security Perimeter(s), control system network, and cyber access monitoring controls shall be updated within ninety (90) calendar days of the change being completed.

Systems Security Management

It is essential that all Critical Cyber Assets as well as identified non-Critical Cyber Assets within the (Utility)'s defined Electronic Security Perimeter(s) be protected and secured.

Testing of new or modified Cyber Assets

Proper cyber security management practices include appropriate testing to ensure that new Cyber Assets or changes to existing Cyber Assets within the Electronic Security Perimeter(s), do not adversely affect existing cyber security controls. Testing shall be completed in accordance with the *(Utility) CIP Cyber Security Testing Procedures.*

Ports and Services

To facilitate the protection of the Critical Cyber Assets, only those ports and services that are required for normal and emergency operations shall be enabled. All other ports and services, including those used for testing purposes, shall be disabled prior to production use of all cyber assets. Ports and services are managed by the CSE Group and performed in accordance with (Utility) *CIP Cyber Assets Ports & Services Procedures.*

Security Patches

All work performed on (Utility) Critical Cyber Assets is performed by trained (Utility) staff. This includes the installation of security software patches. Cyber security related software patches are applied and administered by the CSE Group in accordance with (Utility) *CIP Security Patching Procedures.*

Malicious Software Prevention

It is the policy of the (Utility) to isolate the Critical Cyber Assets from external access whenever possible. The Operations Reliability Manager or equivalent directs the use of anti-virus software and other malware protection tools to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of viruses and malware on all Cyber Assets within the electronic security perimeters. Proper implementation and use is outlined in (Utility) *CIP Malicious Software Prevention Procedures.*

Account Management

The Operations Reliability Manager or equivalent is responsible for establishing appropriate procedural controls to implement and enforce access authentication. The (Utility) carefully maintains account privileges for system administration, network administration, CSE Group use, shared, generic and default accounts. The (Utility) requires the removal, disabling, or renaming of shared and default accounts where technically feasible to help maintain cyber security in accordance with standard CIP-007 and (Utility) *CIP Account Management Procedures.*

Security Status Monitoring

All system activity on Critical or non-Critical Cyber Assets within an Electronic Security Perimeter shall be monitored and logged with manual or automatic alerts for detected cyber security incidents. Security status monitoring shall be conducted in accordance with (Utility) *CIP Cyber Security Monitoring Procedures.* Incident logs shall be maintained in accordance with CIP-008 and all other information shall be maintained for ninety-days.

Disposal and Redeployment

It is (Utility) policy to exercise appropriate care and prudence in the destruction or redeployment of Cyber Assets within defined Electronic Security Perimeters. It is the responsibility of the CSE Group to handle the disposal or redeployment in accordance with (Utility) CIP *Media Disposal and Redeployment Procedures* to ensure that sensitive data is not compromised.

Cyber Vulnerability Assessment

The CSE Group shall annually perform a cyber vulnerability assessment of all Cyber Assets within Electronic Security Perimeter(s). The assessment shall be conducted in accordance with (Utility) established *CIP Vulnerability Assessment Procedures.* The process, as well as results of the annual assessment, shall be documented appropriately.

Documentation Review and Maintenance

The Operations Reliability Manager shall direct the review, updating, and maintenance of all documentation which support the Cyber Assets within the Electronic Security Perimeter(s) to ensure the processes and documentation reflect current configurations and practices. All modifications to the systems or controls shall be updated within thirty (30) calendar days of the change being completed.

Incident Reporting and Response

The accurate identification, classification and reporting of cyber security incidents facilitates the protection of Critical Cyber Assets. It is the responsibility of the Operations Reliability Manager to develop and maintain a *CIP Cyber Security Incident Response Plan* and implement the plan to ensure that response to cyber security incidents occurs within an incident appropriate timeframe. All reportable cyber security incidents shall be appropriately documented and kept for three (3) calendar years. Incidents will be managed in accordance with the (Utility)'s established *CIP Cyber Security Incident Response Plan.* The Plan shall be reviewed and updated at least annually.

Critical Cyber Asset Recovery

The ability to restore normal operations following an incident, that damages or destroys Critical Cyber Assets, is of paramount importance to the (Utility). It is the responsibility of the Operations Reliability Manager to ensure that prudent disaster recovery and business continuity planning is developed, maintained, and reviewed. Annual exercises, storage and backup of information, and testing will be conducted as outlined in the *(Utility) Recovery Plans for Critical Cyber Assets.* Recovery and testing of IED devices shall be the responsibility of the CM Tech Shop Department Superintendent and restoration shall be coordinated with the CSE Group.

Physical and Environmental Security

It is the policy of the (Utility) to locate Critical Cyber Assets within secure areas. Where a completely enclosed ("six-wall") border cannot be established, alternative measures to control physical access to the Critical Cyber Assets shall be established. Such areas are protected by a defined Physical Security Perimeter consisting of "six-wall" physical security with controlled access creating a physical barrier around the asset. The environment within which the Critical Cyber Assets reside shall be controlled to protect against environmental hazards, to reduce risk of loss and damage to the assets.

Physical Security Plan

It is the responsibility of the Director - Security Division to document, implement and maintain a *Physical Security Plan* for the protection of Critical Cyber Assets. The Physical Security Plan shall consider the technical and procedural controls necessary for the protection of Critical Cyber Assets as well as the requirements

of NERC Standard CIP-006. It shall be annually reviewed, updated, and approved by the Senior Manager or delegate(s).

Access Controls

It is the responsibility of the Director - Security Division to maintain strong Physical Access Controls Systems (PACS) in order to properly maintain the Physical Security Perimeters (PSP) protecting the Critical Cyber Assets. Electronic card readers provide a computerized monitoring and logging record of physical access through the physical security perimeter to Critical Cyber Assets. Physical intrusion detection, which alarms the system control center when the physical perimeter is accessed, affords additional protections. The Critical Asset Manager who oversees the Critical Assets and the associated Critical Cyber Assets is responsible for determining the operational parameters of these systems and controls as well as granting and revoking physical access to (Utility) Critical Assets.

The devices that authorize and/or log access to the PSP, exclusive of hardware at the PSP access point such as electronic lock control mechanisms and badge readers, shall be protected from unauthorized physical access. It is the responsibility of the Director- Security Division to ensure that PACS are afforded all of the protections detailed in CIP006 R2. Protection and maintenance will be done in accordance with established procedures detailed in the (Utility)'s *Physical Security Plan.*

It is the responsibility of the Director - Security Division, the Operations Reliability Manager and the Critical Asset Manager to ensure Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeters(s) reside within an identified Physical Security Perimeter.

Access Monitoring

It is the policy of the (Utility) to continually monitor physical access through PSP locations the protect Critical Cyber Assets. Unauthorized access attempts will be reviewed, investigated and processed in accordance with the (Utility) *Physical Security Procedure PSP-6R1.3.* Physical access records and records of PACS shall be maintained for ninety (90) calendar days. Reportable incident logs shall be maintained in accordance with CIP-008.

Maintenance, Testing and Documentation

Physical Access Control Systems (PACS) used to monitor access through the Physical Security Perimeter (PSP) shall be tested and maintained in a prudent manner to ensure proper protection of Critical Cyber Assets. All Physical Security Perimeters shall be identified and documented along with access points through and within those perimeters and PACS. This information shall be classified in accordance with the (Utility)'s *CCA Information Classification and Protection Program* and disseminated pursuant to classification. Testing shall be done in

accordance with (Utility) *Physical Access Control System Testing and Maintenance Procedures.*

Exceptions

Any instance where the (Utility) is unable to conform to its CIP Cyber Security Policy shall be documented as an exception and authorized by the Senior Manager. Authorized exceptions to the CIP Cyber Security Policy shall be reviewed and approved annually by the Senior Manager to ensure the ongoing validity of any exception.

Emergency Provision

An emergency is defined as an unforeseen event or occurrence that poses an imminent threat to: the safety and health of persons, (Utility) facilities, or the reliability of the (Utility)'s Bulk Electric System. In an emergency situation it may be necessary to temporarily suspend the CIP Cyber Security Policy. The priorities in an emergency are the safety and protection of persons first, and the protection and security of the (Utility)'s physical and cyber assets second. In order to protect both persons and property it may be necessary to temporarily disable access controls and other system protections.

If an emergency situation arises, (Utility) staff is directed to call the Security Division as soon as it is safe to do so. The Security personnel who receive the call will alert the General Manager or his designee. The General Manager or his designee will assess the situation and make a determination regarding an emergency declaration. If an emergency is declared, the General Manager or designee will notify system operations. System operations personnel will document the emergency declaration (including start time) in the log. When the (Utility) has returned to normal operations, the General Manager or designee will again alert system operations who will record the emergency ending time in the log. The CIP Cyber Security Policy will be suspended during the emergency declaration period.

Documentation

Documentation will be maintained in accordance with existing (Utility) practices pursuant to NERC standards CIP-002 through CIP-009 and related policies and procedures. Where there are conflicts, retention periods outlined in NERC Reliability Standards will supersede all other guidelines.

This Policy makes references to various (Utility) CIP programs and procedures that are not included as links in the policy. For information regarding these documents, contact the Regulatory Compliance and Policy Development Manager. Information is identified, classified and protected in accordance with ***Administrative Policy*** and the ***CCA Information Classification and Protection Program.*** Requests for information will be processed accordingly.

Reporting of Issues/Concerns

Employees are encouraged to report concerns regarding compliance issues and situations. Employees should feel free to report concerns to their supervisors, managers, directors, or executive managers. Employees may also report concerns to the (Utility)'s General Counsel/Chief Compliance Officer, General Manager, Compliance Manager or Internal Auditor. Retaliation against an employee reporting concerns or issues in good faith will not be tolerated.

Approval

This Policy is approved by the (Utility)'s General Manager and all Executive Managers. This Policy will be implemented in accordance with the NERC Implementation Plan for Cyber Security Standards.

Contact Information

Director - Security Division
Compliance Manager
Operations Reliability Manager
Regulatory Compliance and Policy Development Manager

References
NERC Reliability Standards CIP-002 through CIP-009
NERC Implementation Plan for Cyber Security Standards

Formerly:	**New**
Effective Date:	
Date of Amendments:	

Glossary

Critical Asset Manager - Specific (Utility) managers who oversee the operation of bulk electric system assets, critical assets, and the associated Critical Cyber Assets. The Critical Asset Manager is responsible for granting and revoking physical access to (Utility) critical assets containing Critical Cyber Assets.

Critical Assets - Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

Cyber Assets - Programmable electronic devices and communication networks including hardware, software, and data.

Critical Cyber Assets - Cyber Assets essential to the reliable operation of Critical Assets.

Cyber Security Incident - Any malicious act or suspicious event that: Compromises, or was an attempt to compromise, the Electronic Security Perimeter Physical Security Perimeter of a Critical Cyber Asset, or, Disrupts, or was an attempt to disrupt,

Electronic Security Perimeter - The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

Physical Security Perimeter - The physical, completely enclosed ("six-wall") borders surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

Six-wall Protection - Protection barrier surrounding an asset that includes above, below, and all four sides.

Section 14

TEMPORARY PROJECT CLOSURES:

Procedures have been placed into effect which eliminates the occurrence of any "temporary project closure".

- Labor Disputes - In the case of a bargaining unit strike, the (Utility) retains the right to employ a temporary workforce.

- Emergency Situations - The (Utility) recognizes that certain incidents and events (i.e. pandemic flu) may cause a reduction in the (Utility)'s workforce. Therefore, minimum staffing levels and essential functions have been identified to ensure the continued operation of each hydro project **(ATTACHED).**

ESSENTIAL SERVICES ASSESSMENT

NAME of person completing this form: Hydro Mgr Ext:

Department or Division Name: Hydro B

(UTILITY) H1N1 TEAM OBJECTIVES:
Maintain operation of critical business functions and delivery of essential services.
Protect the health & welfare of our employees.
Protect (Utility) assets.
Effectively communicate to our employees and our stakeholders.

Please keep these objectives in mind while proceeding through this sheet.

Essential Services* - List the services/activities that the (Utility) could not afford to abandon, even during an emergency. The list should include both *external services,* and *internal* functions. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service	Description	Is this Internal or External?
Protect plant integrity	Prevent dam overtopping and flooding	Internal
Manage river flows	Maintain FERC head level requirements and use flows as efficiently as possible	Internal
Generate electricity	Meet plant demand and voltage schedules	Internal
Provide basic hydro plant operations	Perform all above and keep plant systems operating	Internal
Provide emergency or urgent response to maintain electric generation	Respond to equipment failures and outages -restore generation as quickly as possible.	Internal
Maintain fish passage	Maintain a 1.1' differential in fishladder discharges	Internal
Provide emergency or urgent response to maintain fish passage	Respond to equipment failures and outages - restore fish passage criteria as quickly as possible.	Internal
Provide basic maintenance to generating and fish passage assets	Continue basic maintenance rounds and routines as conditions allow.	Internal
Provide organizational and supervisory support	Management duties: Assure safety and health services, payroll, CBA admin, site supervisory decisions, necessary communications and continuation of basic operational and business requirements	Internal

Minimum Staffing Levels -- Provide the minimum number of staff required to maintain essential services. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service (*see prior question)	Minimum# of Staff to maintain	Type/Description of position
Protect plant integrity	One operator in the control room	Hydro operator - Chief or chief relief
Manage river flows	Same	Same
Generate electricity	Same	Same
Provide basic hydro plant operations	Same	Same
Provide emergency or urgent response to maintain electric generation	One operator, one wireman, one technician and one mechanic	Chief or Chief relief trained Senior Operator Journeymen: tech, wire and mechanic
Maintain fish passage	One fishway attendant	Fishway attendant or qualified other
Provide emergency or urgent response to maintain fish passage	As required from crafts listed above	Same
Provide basic maintenance to generating and fish passage assets	As required from crafts listed above	Same
Provide organizational and supervisory support	One Duty Supervisor	Duty Supervisor: Superintendent, Director or temporary assigned staff support (Planner, Engineer)

Action Plans - Describe courses of action that will be taken to overcome the expected challenges. These will substantially be the strategies used to maintain delivery of essential services. ***Note: Action plans should directly support our objectives.*** *(Please feel free to provide/attach an additional sheet if needed).*

1. Provide a common area (lounge area) with food and bedding for employees asked to perform extended duty. Consider ways to support voluntary sequestration.
2. Supervision may support administrative tasks, (time entry, scheduling, etc)
3. Suspend large group meetings and non-essential meetings and limit/suspend (Utility) travel. Encourage social distancing techniques during meetings or tailgates that must occur.
4. Provide sufficient and accessible infection control supplies (e.g. hand-hygiene products, tissues and receptacles for their disposal) in all business locations. Step up surface cleaning in common areas.
5. Re-prioritize and suspend work when resources dwindle. Implement contingency plans for major projects or safely shut down major projects that cannot be supported.
6. Implement operational contingency plans if essential operations are threatened. Emergency assignments may be made to non-typical job classifications.

ESSENTIAL SERVICES ASSESSMENT

NAME of person completing this form: Hydro Mgr Ext:
Department or Division Name: Hydros A & C

(UTILITY) H1N1 TEAM OBJECTIVES:
Maintain operation of critical business functions and delivery of essential services. Protect the health & welfare of our employees. Protect (Utility) assets. Effectively communicate to our employees and our stakeholders.

Please keep these objectives in mind while proceeding through this sheet.

Essential Services* - List the services/activities that the (Utility) could not afford to abandon, even during an emergency. The list should include both *external* services, and *internal* functions. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service	Description	Is this Internal or External?
Operate/Monitor Hydro C	Operate hydro and diesel generators	Internal
Monitor Hydro C Powerplant	Monitor operating conditions	Internal
Support Hydro C Modernization	Tagging /equipment operations	Internal
Operate/Monitor/Adjust Hydro A generation	Operate/Monitor operating conditions	Internal
Operate/Monitor/Adjust Adult Fish Ladder	Operate/Monitor/Adjust Adult Fish Ladder	Internal
Complete C-7 Overhaul	Maintenance in progress	Internal

Minimum Staffing Levels -- Provide the minimum number of staff required to maintain essential services. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service (*see prior question)	Minimum* of Staff to maintain	Type/Description of position
Operate/Monitor Hydro C Powerplant	1	Hydro C Operator (days)
Monitor Hydro C Powerplant Support Hydro C Modernization	1	Operator (5 days/week)
Operate/Monitor/Adjust Hydro A generation	5	Chief Operator 24/7
Operate/Monitor/Adjust Adult Fish Ladder	1	Fishway Attendant (5 days/week)
Complete C-7 Overhaul	11	5 mechanics, 5 wiremen, 1 technician

<u>Action Plans</u> - Describe courses of action that will be taken to overcome the expected challenges. These will substantially be the strategies used to maintain delivery of essential services. ***Note: Action plans should directly support our objectives.*** *(Please feel free to provide/attach an additional sheet if needed).*

1. Provide food and bedding for employees asked to perform extended duty
2. All administrative tasks to be performed by supervision (time entry, scheduling, etc)
3. Close visitor center and museum if support personnel become absent
4. Re-prioritize and suspend work when resources dwindle
5. Cancel all standard meetings and replace with daily attendance checks and tail gates

***PLEASE ROUTE THIS COMPLETED FORM TO:

ESSENTIAL SERVICES ASSESSMENT

NAME of person completing this form: CM Superintendent Ext:

Department or Division Name: Central Maintenance

(UTILITY) H1N1 TEAM OBJECTIVES:
Maintain operation of critical business functions and delivery of essential services. Protect the health & welfare of our employees. Protect (Utility) assets. Effectively communicate to our employees and our stakeholders.

Please keep these objectives in mind while proceeding through this sheet.

Essential Services* - List the services/activities that the (Utility) could not afford to abandon, even during an emergency. The list should include both *external services,* and *internal* functions. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service	Description	Is this Internal or External?
Protect hydro plant integrity	Assist in maintaining physical hydro plant integrity - i.e. - spillway	Internal
Maintain reliability of the transmission yards, including emergency response	Provide basic transmission yard maintenance and emergency repair	Internal
Provide emergency or urgent response to maintain fish passage	Hydro plant fish ladder emergency repair	Internal
Provide emergency or urgent response to maintain electric generation	Hydro generating unit emergency repair	Internal
Emergency hatchery response	Emergency repair to mitigate possible hatchery fish loss	Internal

Minimum Staffing Levels - Provide the minimum number of staff required to maintain essential services. *(Please feel free to provide/attach an additional sheet if needed).*

Essential Service (*see prior question)	Minimum* of Staff to maintain	Type/Description of position
Protect hydro plant integrity	5 Mech. 4 Wiremen 2 Techs	All positions are maintenance oriented positions
Maintain reliability of the	4 Wiremen	All positions are maintenance

transmission yards, including emergency response	4 Technicians 1 Station Engineer 2 Materials Specialists	oriented positions
Provide emergency or urgent response to maintain fish pass	2 Wiremen 5 Mech. 2 Techs 2 Materials Specialists	All positions are maintenance oriented positions
Provide emergency or urgent response to maintain electric generation, Security equip, trunked radio/microwave, telephone, SCADA Systems, System Ops, telemetry, emergency power systems	7 Techs 6 Wiremen 5 Mechanics 2 Materials Specialists	All positions are maintenance oriented positions
Emergency hatchery response	1 Mech. 1 Wiremen 1 Tech 1 Materials Specialists	All positions are maintenance oriented positions

Action Plans - Describe courses of action that will be taken to overcome the expected challenges. These will substantially be the strategies used to maintain delivery of essential services. ***Note: Action plans should directly support our objectives.*** *(Please feel free to provide/attach an additional sheet if needed).*

1. Suspend performance of "non-essential" services.
2. Provide the minimum Supervisory presence for crew support and organization by location - 3
3. Practice social distancing practices with the crews - no large meetings, separate tailgates, etc...
4. Leverage administrative support (high-priority tasks) from internal resources.
5. Maintain special function personnel levels: CM specialists - (station crane mechanic,dive crew, mobile crane crew)
6. Provide overall minimum coverage for Mission Critical functions which would be:
   MCF jobs where coverage is required 24/7 for emergency continuance of core operations
   Hatchery response (1 Mech., 1 Wiremen, 1 Tech) Telecom, SCADA, Radio, Plant support (2 Wiremen, 4 Tech, 4 Mechs) Transmission/Distribution: (4) CM Switchyard Crew, (2) Technicians, (1) Station
   Engineer
   Materials Specialist (1 at each Hydro Warehouse)

   Total CM Wiremen - (6)
   Total CM Techs - (7)
   Total CM Mechanics - (5)
   Total CM Materials Specialists - (2)

'PLEASE ROUTE THIS COMPLETED FORM TO:

Section 15

COMMUNICATIONS:

The (Utility) recognizes the value of maintaining an effective communications system.

Telephones:

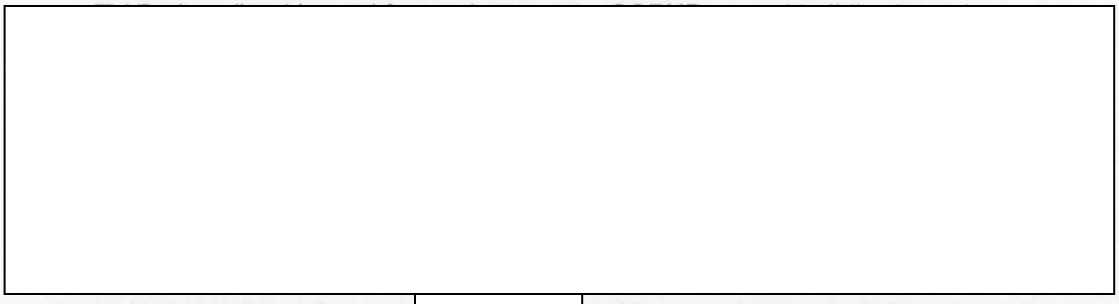
- Land-line telephones are located throughout the hydro projects.
- Cellular telephones are carried by most employees.
- Mobile satellite telephones are available within the (Utility).
- Government Emergency Telecommunications Service (GETS) cards are available within (Utility).

Radios:

- The (Utility) utilizes base station, mobile, and portable radios.
- Radio users include hydro project employees, contracted security guards, and (UTILITY) Security Division personnel.
- Radios are programmed to afford interoperability throughout the (Utility). Additionally, these radios provide interoperability with local First-Responder agencies.
- Radios normally operate with "wide area" (throughout (Utility)) coverage. If there is computer failure of the wide area coverage, then the individual project radios continue to operate with local repeaters. If the local repeaters fail, then radios can still be used in "talk around" mode (portable-to-portable, mobile-to-mobile, base station-to-base station). Base-station radios have battery back-up, in case of AC failure.

Background

- Seven (7) Mountain top repeater sites



- Local repeater sites at Hydros A&B with coverage enhancement
- Consoles at
- 290 mobiles, 402 portables
- 12 Microwave links interconnecting Co. facilities and mountain tops