Security Guideline for the Electricity Sector:
Business Processes and Operations Continuity

Preamble:
It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the Bulk Electric System. Guidelines provide suggested guidance on a particular topic for use by Bulk Electric System entities according to each entity’s facts and circumstances and not to provide binding norms, establish mandatory reliability standards, or be used to monitor or enforce compliance.

Introduction:
This Guideline addresses potential risks that can apply to some Electricity Sector Organizations and identifies practices that can help mitigate these risks. Each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.

This Guideline is to provide all electricity sector organizations, regardless of their NERC registration, with concepts that should be considered when developing business continuity plans, which strive to assure continuity of business processes and operations. Such plans represent one approach for enabling the organization to take an all-hazards approach to prepare itself for natural or man-made disasters, prevent or reduce an incident’s adverse impact, and to assure effective coordinated response and recovery efforts.

Facilities and functions critical\(^1\) to operations should be identified by the impact analysis and risk assessments each organization develops to support its operational continuity plans.

The critical business processes that support the company’s core missions include:

- Serve its customers with a reliable source of electric energy,
- Provide services that ensure the reliable operation of the energy grid and interconnection,
- Avoid losses that would create a significant risk to public health and safety.

\(^1\) Note that the use of the term “critical” in this guideline does not imply any relation to the CIP-002 definition of a “Critical Asset”
This guideline provides a framework for identifying the concepts and steps associated with an effective operations continuity plan. While the DHS Private Sector Preparedness (PS-PREP) program was used as the primary source for this guideline, other methodologies are equally applicable. The “Additional Resources” section of this guideline contains a list of other methodologies.

**NOTE:** Companies that are NERC Registered Entities may have additional obligations under the NERC Reliability Standards.

**Scope of Application:**
This guideline applies to business processes (or operations / functions), resources and facilities which are considered critical to the individual organization in fulfilling its mission of producing and/or delivering electric energy.

**Guideline Details:**
This guideline describes steps that an electricity sector organization should consider in developing plans that will strive to ensure continuity of operations during and after an incident or crisis. Continuity of operations could include efforts for resiliency, incident response, crisis communication, and resumption.

In developing its continuity of operations plan each organization should define critical processes and assets, and identify those resources and functions that support these processes and assets.

A Risk Assessment should be performed for each critical process and asset to establish priorities, and to identify mitigation strategies to lower risks. For situations where risks cannot be reduced to an acceptable level, the organization should consider alternate or redundant capabilities.

Critical business processes (or operations / functions) cannot be unavailable without jeopardizing safety, regulatory, operational or financial performance of the company.

Critical resources and facilities support the critical business processes' ability to operate, and replacements/alternatives are needed in order to effectively recover the process following a disruption. Utilities historically have extensive plans and contracts/agreements in place for the restoration of electric service to customers in response to natural disasters such as earthquakes, floods, and other weather-related emergencies. Continuity of operations plans should be developed for business processes and are critical to minimize the impact from natural and man-made disasters.
Based on the PS-PREP program documentation, a comprehensive continuity of operations plan typically addresses the following process elements:

**Program Policies and Management**
Top level authorization, support and commitment should be given to the preparedness program. An organization should take the following actions: Develop policy, vision and mission statements; devote appropriate personnel and financial resources; and, assign an individual or committee in larger organizations, with appropriate authority to lead the preparedness efforts.

**Analysis**
The following activities are critical for the organization to develop appropriate program goals related to incident prevention and mitigation and incident management and continuity: Evaluate legal, statutory, regulatory, and industry best practices as well as other requirements; define and document the scope of the preparedness program; and, conduct a risk assessment and impact analysis.
Planning
The organization should develop multiple plans, each of which should have clearly defined end products, a specific schedule, and assigned responsibilities and resources. Primary plans should exist for the following activities: Prevention and mitigation and incident management. Supporting plans should exist for the following activities; resource management and logistics; training; testing and evaluation; and, records management.

Implementation
Successful implementation of preparedness program requires the development and maintenance of a comprehensive project management and control system which includes the following: Each of the specified projects carried out according to the plan, adhering to completion dates; assurance of program-level coordination; and, periodic program reviews and internal audits.

Testing and Evaluation
For the purpose of quality control, a testing and evaluation plan should incorporate the following elements: Specify a series of evaluations to examine various elements of the implementation process; use dry runs to evaluate the program overall; and, review findings from these processes to revise plans as needed.

Maintenance, Review and Improvement
The preparedness program requires routine maintenance, review, feedback, and continuous improvements. Programs can achieve these goals by taking the following actions: Implementing periodic formal reviews to verify adherence to program requirements and discover areas of improvement; using any post-incident evaluations, such as special analysis and reports, lessons learned and performance evaluations; and, identifying program areas that require periodic maintenance, and regularly scheduling that maintenance.

Related Documents and Links:


Disaster Recovery Journal (DRJ); Glossary v2.0: DRJ and DRII; http://www.dri.com/tools/tools/glossary-2.html

Electric Sector Data Set - Companion to the PS-Prep Framework Guide
Available on HSIN

**PS-PREP: 3 Adopted Standards**

Note. Each adopted standard has a worksheet designed to assist any entity performing a preliminary self-assessment. The worksheets align key subject areas of a comprehensive preparedness program with specific elements of the three adopted preparedness standards.

https://www.asisonline.org/guidelines/published.htm

www.bsi-emea.com/BCM/Overview/index.xalter

www.nfpa.org/assets/files/PDF/NFPA16002010.pdf

**Additional Resources:**

**Security:**


NERC Security Guidelines for the Electricity Sector;
http://esisac.com/library-guidelines.htm

*Security Guideline for the Electricity Sector — Physical Response v3.0, NERC,* November 2005,
http://esisac.com/library-guidelines.htm

Business Continuity:

American Red Cross; Preparing Your Business for the Unthinkable; Washington, D.C.; http://www.redcross.org/services/disaster/beprepared/unthinkable2.pdf


Purpose of Standard Checklist Criteria for Business Recovery; http://www.fema.gov/business/bc.shtm


Emergency Management:


## Revision History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Version Number</th>
<th>Reason/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/14/2002</td>
<td>1.0</td>
<td>Initial Version – <em>Continuity of Business Processes Security Guideline</em></td>
</tr>
<tr>
<td>7/1/2007</td>
<td>2.0</td>
<td>Title and content revised to Continuity of Business Operations Security Guideline. Extensive updates and edits to make the text current and incorporated the 2006 CIPC approved format for all guidelines.</td>
</tr>
<tr>
<td>4/3/11</td>
<td>2.1</td>
<td>Completely revised and posted for initial CIPC Comment</td>
</tr>
<tr>
<td>4/5</td>
<td>2.15</td>
<td>Correction of formatting and typographical errors in initial posting</td>
</tr>
<tr>
<td>5/9</td>
<td>2.16</td>
<td>Updated based on comments received</td>
</tr>
<tr>
<td>5/12</td>
<td>2.17</td>
<td>Posting for industry Comment</td>
</tr>
</tbody>
</table>