

## Agenda

# Critical Infrastructure Protection Committee Meeting

June 8, 2011 | 1 p.m. – 5 p.m.

June 9, 2011 | 8 a.m. – noon

Toronto Airport Marriott

901 Dixon Road

Toronto, Ontario, Canada

### Administrative Matters

### Antitrust Compliance Guidelines

### Consent Agenda – Approve

- |                    |               |
|--------------------|---------------|
| <b>1. Minutes*</b> | <b>30 min</b> |
| • March 9, 2011    |               |

### Regular Agenda

- |   |               |
|---|---------------|
| <b>2. CIPC Chair Report – Chuck Abell</b>                             | <b>30 min</b> |
| a. Board of Trustees Highlights – Chuck Abell                         |               |
| b. Executive Committee Activities                                     |               |
| c. Nomination and CIPC approval for Chair of Nominating Subcommittee* |               |
| <b>3. NERC / ES-ISAC Updates – Mark Weatherford &amp; NERC Staff</b>  | <b>90 min</b> |
| a. NERC / CSO Update  |               |
| b. Electricity Sub-Sector Coordinating Council and PCIS Update        |               |
| c. ISAC Update  |               |
| d. Alerts Update  |               |
| e. Cyber Security Standards Update                                    |               |
| i. CSO706 – Version 5   |               |
| ii. Survey  |               |
| iii. CIP-005 Urgent Action  |               |
| iv. Interpretation Team   |               |

f.	Security Summit	
g.	GridEx	
h.	Sufficiency Reviews	
i.	Adequate Level of Reliability Task Force (ALRTF) Approval*	
<b>4.</b>	<b>NASPI Update – Allison Silverstein</b>	<b>60 min</b>
<b>5.</b>	<b>CAN Process Update – Mike Moon</b>	<b>30 min</b>
<b>6.</b>	<b>DOE/NIST/NERC Risk Management Framework – Brian Harrell &amp; Matt Light</b>	<b>30 min</b>
<b>7.</b>	<b>Coordinated Action Plan Task Force Reports – Stuart Brindley</b>	<b>45 min</b>
a.	SIRTF – Tom Bowe	
b.	CATF – Mark Engels	
c.	GMDTF – Don Watkins	
d.	SEDTF – Dale Burmester	
<b>8.</b>	<b>CIPC Working Group / Task Force Updates – Chuck Abell</b>	<b>60 min</b>
a.	CSSWG – Mark Engels (15 min)	
b.	Substations Guideline Task Force – Allen Klassen (15 min)	
c.	Protecting Sensitive Information Guideline Task Force – Nathan Mitchell (15 min)	
d.	Business Continuity Guideline Task Force* – Darren Myers	
i.	Approve Guideline for Broad Industry Review*	
<b>9.</b>	<b>DSR Standards Drafting Team (Project 2009-01) Update – Bob Canada</b>	<b>10 min</b>
<b>10.</b>	<b>Energy Sector Roadmap to Secure Energy Delivery Systems –Jim Brenton</b>	<b>10 min</b>
<b>11.</b>	<b>Recent BPS Incidents – Scott Mix</b>	<b>10 min</b>
<b>12.</b>	<b>Washington, DC Legislative Activities Update – Dave Batz, EEI</b>	<b>30 min</b>
<b>13.</b>	<b>Round-table Discussion*</b>	<b>30 min</b>
a.	Communications – Exchanging Information About Emerging Threats	
	<b>Agency Reports</b>	<b>30 min</b>
<b>14.</b>	<b>Department of Homeland Security</b>	
a.	National Threat Advisory System (NTAS) – (requested)	

**15. Department of Energy**

- a. National Electric Sector Cybersecurity Organization (NESCO)
  - Rhonda Dunfee
- b. NLE-11 – Matt Light

**16. Public Safety Canada / Royal Canadian Mounted Police**

**17. Federal Energy Regulatory Commission**

**Closing**

**5 min**

**18. Follow-up Items and Future Actions – Chuck Abell**

**19. 2011 Future Meetings – Scott Mix**

- September 14–15, 2011 St. Louis, MO
- December 14–15, 2011 Atlanta, GA

\*Background material included

## Antitrust Compliance Guidelines

### I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

### II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.

- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

### **III. Activities That Are Permitted**

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

## Draft Minutes Critical Infrastructure Protection Committee

Phoenix Convention Center  
March 9-10, 2011  
Phoenix, AZ

Critical Infrastructure Protection Committee Vice-Chairman Chuck Abell called to order a duly noticed, regular meeting of the Critical Infrastructure Protection Committee (CIPC) on March 9, 2011 at 1:02 p.m., local time, and a quorum was declared present. The meeting announcement, agenda, and list of attendees are attached as **Exhibits A, B, and C**, respectively.

Vice-Chairman Chuck Abell, Ameren, and Vice-Chairman Bob Canada, Southern Company, both presided.

Secretary Scott Mix, NERC CIP Technical Manager, announced a quorum of 26 members and the following proxies:

1. Ed Goff for Joel Garman
2. Frank Dessuit for Ken Kujala
3. Joe Doetzel for John Breckenridge
4. Keith Overland for Allen Klassen
5. Scott Bordenkircher for Darren Nielsen
6. Brian Gardner for Robert Richhart

### **NERC Antitrust Compliance Guidelines**

Mr. Abell called attention to the NERC Antitrust Compliance Guidelines distributed with the agenda and read the statement concerning publicly announced meetings.

### **Introductions of Members, Alternates, Associates, and Others**

Mr. Abell called for introductions of members of the CIPC and other attendees.

### **Approval of Agenda**

Mr. Abell presented the agenda for approval and indicated that due to timing issues and scheduling constraints, the agenda order would be modified as necessary during the meeting. Upon **motion** by Mr. Robert McClanahan, seconded by Mr. Mark Engels, the agenda for the December meeting was adopted.

### **Approval of Minutes**

Mr. Abell presented the December 9-10, 2010 minutes for approval, and asked if there were any changes noted by the membership. One change was noted by Mr. Abell. Upon **motion** by Mr. Mark Engels, seconded by Mr. Jeff Fuller, the minutes for the December meeting, with the one noted change, were adopted.

**Note:** Slides from the presentations from this meeting are available at <http://www.nerc.com/filez/cipmin.html>.

### **CIPC Executive Committee Report**

Mr. Canada presented the CIPC Chair report prepared by Mr. Lawson, which consisted of an overview of the highlights of the meeting, a recap of recent CIPC Executive Committee meetings, and Electricity Sub-Sector Coordinating Council (ESCC) activities. Additionally, he reported on his CIPC report at the recent NERC Board of Trustees meeting. (**Presentation 1**)

### **Coordinated Action Plan Report**

Mr. Stuart Brindley, of SJBrindley Consulting, and NERC Consultant, provided an update on activities associated with the Coordinated Action Plan. (**Presentation 2**)

Mr. Dale Burmester, ATC, and chair of the Spare Equipment Database Task Force (SEDTF), provided an update on the Task Force's activities. (**Presentation 3**)

Mr. Mark Engels, Dominion, and chair of the Cyber Attack Task Force (CATF) provided an update on the Task Force's activities. (**Presentation 4**)

Mr. Tom Bowe, PJM, and chair of the Severe Impact Resiliency Task Force (SIRTF) provided an update on the Task Force's activities. (**Presentation 5**)

### **NERC ES-ISAC, CRPA, and Alerts Update**

Mr. Tim Roxey, NERC Director - Critical Infrastructure Risk Management and Technology Division, provided an update on recent activities at NERC concerning changes to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Cyber Risk Preparedness Program (CRPA), and recent alerts activities. (**Presentation 6**)

### **Technical Feasibility Exception (TFE) Update**

Mr. Tom Hofstetter, NERC CIP Compliance Specialist, provided an update on the Technical Feasibility Exception (TFE) program. (**Presentation 7**)

### **FERC Order 706 Drafting Team and Remote Access Update**

Mr. Scott Mix, NERC CIP Technical Manager, provided an update on the activities and status of the CSO 706 Standards Drafting Team, and the status of the activities for updating Standard CIP-005-3 to add remote access requirements. (**Presentation 8**)

### **CAN Process Update**

Ms. Valerie Agnew, NERC Manager of Compliance Standards Interface and Outreach, provided an update on the Compliance Application Notice (CAN) development and status. (**Presentation 9**)

## **DOE Roadmap Update**

Mr. Hank Kenchington, DOE Deputy Assistant Secretary R&D, Office of Electricity Delivery and Energy Reliability, provided a discussion and update on the status of the 2011 Roadmap to Secure Energy Delivery Systems. (**Presentation 10**)

The CIPC then adjourned for the day at 5:14 PM, and re-convened the following day at 8:05 AM.

## **NERC Security Summit Update**

Mr. Brian Harrell, NERC Manager of CIP Standards, Training, and Awareness, provided an update on the NERC Security Summit. That summit, also known as “GridSecCon”, will take place on Oct 18-19, 2011 with training provided by INL and SANS on the front and backside. Location will be the JW Marriott, New Orleans, LA. This summit will bring industry, law enforcement and homeland security officials, and regulators to one venue to discuss physical and cybersecurity. Official announcements and save the date brochures will be distributed in Toronto. NERC is planning on attendance of between 250 and 300 people. The summit will be focused on security, rather than on compliance.

## **2011 NERC Security Grid Exercise (GridEx) update**

Mr. Harrell then provided an update on the 2011 NERC Security Grid Exercise (GridEx). The statement of work has been finalized and NERC will be approaching a contractor to support a two day North American cybersecurity exercise. The proposed date for the exercise is November 16-17, 2011. The scenario will be developed in the coming months and NERC is targeting approximately 30 Registered Entities to volunteer and play. If you have some preliminary interest for your company to participate, please contact Brian Harrell (brian.harrell@nerc.net).

## **2011 NERC Sufficiency Review Program Update**

Due to the success of the 2010 Sufficiency Review Program (SRP), NERC has renewed the program for 2011 and is currently soliciting for volunteers. Mr. Ralph Anderson, NERC CIP Risk Specialist, and the project leader for the program provided a status report of the program. (**Presentation 11**)

## **DOE/NIST/NERC – Cyber Risk Management Guidelines update**

Mr. Harrell then provided an update on the Cyber Risk Management Guideline project, a joint effort between DOE, NERC and NIST. Industry representatives likely saw the DOE press release announcing the creation of a DOE/NIST/NERC risk management guideline working group. This group has met a small handful of times and has started the discussion on scoping and objectives. Representatives include industry reps (as coordinated through trade associations and NERC), NIST, DOE, NERC, FERC, DHS, Control Systems Working Group (SGIP-CSWG). The core group will use the NIST 800-39 document as a baseline and will marry it up to needs required in the electrical sector. The working group is currently working to put associated risks into tiers. This risk management guideline is not intended to replace the CIP standards but instead address risks found beyond the standards.

## **Control Systems Security Working Group (CSSWG) Report**

Mr. Mark Engels, Dominion, and chair of the Control Systems Security Working Group provided a report of recent Working Group activities. (**Presentation 12**)

### **Substation Guideline Task Force (SUBGTF) Report**

A brief verbal report was provided by Mr. Canada: a few members have started to review the existing document, and the new template format. Mr. Canada will be reaching out to the chair, Mr. Allen Klassen, next week to determine if he is able to continue as chair.

### **Protecting Sensitive Information Task Force (PSIGTF) Report**

Mr. Nathan Mitchell, APPA, and chair of the Protecting Sensitive Information Task Force (PSIGTF) provided a report of recent Task Force activities, which was presented by Mr. Mix. (**Presentation 13**)

### **Business Continuity Guideline Task Force (BCGTF) Report**

Mr. Darren Nielson, Progress Energy and chair of the Business Continuity Guideline Task Force (BCGTF), provided an update of recent Task Force activities, and discussed a revised schedule for the development of the guideline. (**Presentation 14**)

### **Roundtable Discussion**

Mr. Canada led the CIPC in a brief roundtable discussion on the topic of “What physical and cyber security schemes do you have in place at your 200kV and above substations?”

Following the roundtable, Mr. Canada polled the CIPC as to whether the Physical Security members of the CIPC would be interested in a further discussion on topics of interest. CIPC members were requested to email their topical suggestions to Mr. Canada.

### **Disturbance and Sabotage Reporting Standard Drafting Team Status Report**

Mr. Canada, Chair of the Disturbance and Sabotage Reporting SDT, provided an update of that team’s activities. The Standard was posted for comment on March 8. The SDT continues to coordinate its activities with the Events Analysis Working Group (EAWG). CIPC members were encouraged to review and comment on the posted standard, paying specific attention to any discrepancies or holes between the standard and the revised EAWG postings. Discussions are also underway with DOE to determine how a single reporting form can be developed for both EOP-004 and DOE-417 needs.

### **BPS Events Update**

Mr. Mix provided a report on BPS events that occurred in the preceding 3 months.

### **Washington, DC Legislative Activities Update**

Mr. Dave Batz, Manager, Cyber & Infrastructure Security for the Edison Electric Institute, provided an update on recent and ongoing activities happening in Washington, DC, in particular in Congress. (**Presentation 15**)

### **Department of Homeland Security**

Although Ms. Cathy Eade, DHS, was unable to attend the CIPC meeting, Mr. Matthew Light, DOE provided several reminders sent to him by Ms Eade. Those were:

- Industry members with security clearances through DHS must complete their annual training on time; else they face revocation of their clearance.
- Industry members who have requested clearances, and have started the process should know that the E-QUIP (on line forms) process for submitting information required before a clearance can be granted is a

very time consuming process, and has a short and defined window for entering data into the forms. They should gather all the information necessary to complete the form (7 to 10 years of living and travel information, and family history) prior to starting the process.

- Industry members with security clearances who change jobs must inform DHS as soon as possible with updated contact information and company names / responsibilities.

## **DOE**

Mr. Matthew Light then continued with his DOE report. He provided three reports:

- Update on DOE activities (**Presentation 16**)
- Update on NLE-11 (**Presentation 17**)
- Overview on a new Reliability, Survivability and Resiliency Self Assessment tool (**Presentation 18**)

## **Public Safety Canada Presentation**

Mr. Dave Baumken, of Public Safety Canada (PS Canada) provided brief update on Canadian infrastructure initiatives. These initiatives include an information sharing and protection protocol for industry to government information sharing, and the startup of a web-based system for submitting incident reports, that is being developed in coordination with PS Canada, the RCMP, and National Resources Canada. He reminded the members that the new initiatives were started less than one year ago, and that most observable progress tends to happen in the second year of such programs.

## **FERC**

No report.

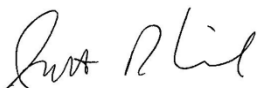
## **Recap**

Chair Lawson and Mr. Mix provided a recap of the committee actions and reminded the CIPC that the next meeting will be held June 9-9, 2011 in Toronto, Ontario, Canada.

## **Adjourn**

There being no further business, and upon **motion** by Mr. Carl Eng, seconded by Mr. Marc Child, the CIPC meeting was adjourned at 11:02 AM.

Submitted by,



Scott Mix  
Secretary

## **CIPC Nominations Subcommittee Chair**

### **Action Required**

Approve nomination for Nomination Subcommittee Chair.

### **Background**

The CIPC Charter provides that the term for officers is two years. It is now time to start the process to elect (or re-elect) officers for the next two-year term.

The relevant section of the CIPC Charter is:

2. Nominating Subcommittee.
  - a. At the last regular meeting (normally the June meeting) before the selection of a new Committee Chair (normally the September meeting), the incumbent Chair will nominate, for the Committee's approval, a Chair of the nominating subcommittee. The subcommittee will recommend candidates for the Committee's Chair, two Vice Chairs, and four SME EC members.
  - b. The subcommittee Chair will then assemble the nominating subcommittee of five Committee members.
  - c. The subcommittee will solicit nominations from the Committee for the Officer and SME EC positions.
  - d. The subcommittee will review the nominations received and develop a slate of seven candidates: one for the Committee Chair, two for the Committee Vice-Chairs, and four SME members of the EC.
  - e. The subcommittee will present its slate of officers at the Committee's September meeting and SME EC members at the Committee's December meeting.

CIPC Chair Barry Lawson will provide his nomination to Chair the Nominating Subcommittee for approval at the meeting.

## **Adequate Level of Reliability Task Force**

### **Action Required**

Approve Scope and solicit volunteers.

### **Background**

In response to the January 18, 2007 Order on Compliance Filing, NERC was directed to develop a plan for defining the term “Adequate Level of Reliability”. In response to that order, NERC filed with FERC on May 5, 2008 the current Adequate Level of Reliability document for informational purposes.

Subsequent to that filing, additional characteristics of Adequate Level of Protection are needed, specifically, critical infrastructure protection components, and system resilience, among others. Additionally, the existing characteristics may need to be revised.

The Technical Committees have been asked to approve the scope of a new task force, the “Adequate Level of Reliability Task Force (ALRTF)”, which is attached, and to solicit from their memberships a small number of volunteers to serve on the task force.

The ALRTF is being presented on the joint PC/OC/CIPC Webinar on May 31.

## DRAFT Scope: Adequate Level of Reliability Task Force (ALRTF)

### Scope

To address the changing landscape of reliability, the ALRTF will review and determine if the existing definition and characteristics of “adequate level of reliability” (ALR) needs enhancement in coordination with the MRC’s BES/ALR Policy Group addressing ALR. The goal is to have a definition of ALR that encompasses NERC’s responsibility to ensure reliability, and to define objectives and characteristics that are measurable, enabling the ERO enterprise to focus on and align its activities with specific characteristics of ALR that have the greatest impact on bulk power system reliability.

### Purpose

Deliver, for use by the ERO enterprise, a document which includes a definition of ALR and associated characteristics with demonstrated ability to measure the relative state of ALR on an ongoing basis. The definition and associated characteristics may be identical to those previously approved or may be enhanced if necessary. Further, these measurable objectives and characteristics should focus on support for the ERO’s key activities, including Reliability Standards and Compliance and Certification functions.

### Background

In its January 18, 2007 Order on Compliance Filing, the Federal Energy Regulatory Commission directed NERC to file a plan for defining the term “adequate level of reliability.”<sup>1</sup> The Commission explained that it intended to use this definition when judging the merits of NERC’s Reliability Standards against the requirements of Section 215 (c) of the Federal Power Act. The Act requires Reliability Standards “that provide for an *adequate level of reliability* of the bulk power system” [emphasis added].<sup>2</sup>

The Commission required NERC’s plan to include two broad objectives and address several questions:

<sup>1</sup> *Order on Compliance Filing*, 118 FERC ¶61,030, paragraph 16.

<sup>2</sup> The definition of Bulk-Power System, as it appears in Section 215(a)(1) is: “the facilities and control systems necessary for operating an interconnected electric energy transmission network or any portion thereof; and the electric energy from generation facilities needed to maintain transmission system reliability.”

- First, the plan needed to develop a definition of adequate level of reliability using a stakeholder process. The Commission asked whether the proposed definition be applied to all Reliability Standards, certain sets of standards, or, in some cases, be tailored for each standard. The Commission also asked NERC to consider opportunities to develop and apply metrics that can form the basis for broadly defining an adequate level of reliability.
- Second, the plan needed to “propose a continuing improvement process to consider ‘adequate level of reliability’ when developing new or modified Reliability Standards.”

In its March 19, 2007 response to the order, NERC explained that it directed its Operating Committee and Planning Committee to develop the definition of adequate level of reliability through a stakeholder process and provide that definition to the NERC Board of Trustees.<sup>3</sup> NERC also explained that it would “integrate the approved definition into its three-year standards work plan and standards development process, as well as its compliance monitoring and enforcement program as appropriate.”

A document, prepared by the NERC Operating Committee and Planning Committee, was submitted for information on May 5, 2008<sup>4</sup> in part to fulfill NERC’s commitment to provide a definition of adequate level of reliability.

At the time of filing, the Bulk-Power System (“System”) was defined to achieve an adequate level of reliability when it possesses following six characteristics:

1. The System is controlled to stay within acceptable limits during normal conditions;
2. The System performs acceptably after credible Contingencies;
3. The System limits the impact and scope of instability and Cascading Outages when they occur;
4. The System’s Facilities are protected from unacceptable damage by operating them within Facility Ratings;
5. The System’s integrity can be restored promptly if it is lost; and
6. The System has the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components

It has become apparent that additional characteristics may need to be added (e.g. critical infrastructure protection components, system resilience, etc.), the descriptions of the characteristics may need to be revised, and revisions may be required to enable objective measurability.

Further, these ALR characteristics and NERC’s Reliability Standards Objectives<sup>5</sup> may require harmonization to ensure consistency across the ERO Enterprise. These Objectives are:

1. **Reliability Planning and Operating Performance** — Bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions.

<sup>3</sup> *Compliance Filing of the North American Reliability Corporation in Response to January 18, 2007 Order and March 9, 2007 Order*, March 19, 2007, Docket Nos. RR06-01-003 and RR06-01-005, pp. 4-7.

<sup>4</sup> [http://www.nerc.com/files/Adequate\\_Level\\_of\\_Reliability\\_Definition\\_05052008.pdf](http://www.nerc.com/files/Adequate_Level_of_Reliability_Definition_05052008.pdf)

<sup>5</sup> See *Rules of Procedure* [http://www.nerc.com/files/NERC\\_Rules\\_of\\_Procedure\\_EFFECTIVE\\_20110101.pdf](http://www.nerc.com/files/NERC_Rules_of_Procedure_EFFECTIVE_20110101.pdf), Section 302.

2. **Frequency and Voltage Performance** — The frequency and voltage of bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
3. **Reliability Information** — Information necessary for the planning and operation of reliable bulk power systems shall be made available to those entities responsible for planning and operating bulk power systems.
4. **Emergency Preparation** — Plans for emergency operation and system restoration of bulk power systems shall be developed, coordinated, maintained, and implemented.
5. **Communications and Control** — Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of bulk power systems.
6. **Personnel** — Personnel responsible for planning and operating bulk power systems shall be trained and qualified, and shall have the responsibility and authority to implement actions.
7. **Wide-area View** — The reliability of the bulk power systems shall be assessed, monitored, and maintained on a wide-area basis.
8. **Security** — Bulk power systems shall be protected from malicious physical or cyber attacks.

The goal of this task force, with direction of the MRC BES/ALR Policy Group and the standing committees, is to develop an integrated set of measurable ALR characteristics for use in evaluating the current state of bulk power system reliability with a single set of reliability principles and characteristics. The work must be coordinated with the MRC's BES/ALR Policy Group working on policy issues that shape the boundaries of an adequate level of reliability, with appropriate sequencing of activities.

### **Assumptions and Limitations**

The following assumptions and limitations have been identified at the outset of this activity:

- The ALR of the bulk power system reliability must be measurable enabling industry to focus on the current status and support improvements.
- Developing metrics that objectively measure bulk power system performance is feasible and the data is available.
- Registered entities will assist the ERO in measuring ALR.
- The work of the task force will be coordinated with the MRC's BES/ALR Policy Group, and the final work product will be shaped by the final definition of Bulk Electric System.

### **Membership**

This is a joint task force reporting to the MRC's BES/ALR Policy Group with membership from the standing committees. The standing committee chairs (who are members of MRC's BES/ALR Policy Group) will appoint the ALRTF chair and vice chair and a maximum of three members to the task force from each committee.

Given the challenging nature of this work, efforts will be made to reach out to include the contribution of experts beyond the scope of the technical committees. The task force is comprised of the following:

- Chair and vice chair (appointed by the standing committee chairs/vice chairs)
- Industry representatives and experts (including NERC member entities, equipment suppliers and manufacturers)
- Government partners (including Federal Energy Regulatory Commission, U.S. Department of Energy, Natural Energy Board and Natural Resources Canada, etc.)
- NERC staff

### **Monitoring and Directing Progress**

The task force shall report progress to the MRC BES/ALR Policy Group on a monthly basis.

### **Resources**

An initial, face-to-face, kickoff meeting will be held. During that meeting, the task force will develop a work plan to meet the deliverables within the specified deadlines. The task force is expected to be very active, with face-to-face meetings held at least once a quarter and two conference calls per month (two hours each) with additional work done by sub-teams between meetings and calls.

### **Deliverables**

Deliver a document to the SCCG, which outlines a definition and characteristics with demonstrated ability to measure the relative state of ALR on an ongoing basis.

### **Work Plan**

#### **2011**

- **2<sup>nd</sup> Quarter**
  - April 2011 – Draft ALRTF Scope approved, chair/vice chair appointed, and NERC staff assigned.
  - May 2011 – Kickoff meeting held; detailed project schedule developed. Initial review of current ALR definition and characteristics as well as the Standards Reliability Objectives is completed.
  - June 2011 – ALRTF Scope shared with standing committees along with preliminary assessment identifying whether there are potential areas for improvement, addition, and harmonization and if there are areas for improvement, identifying how improved definition and characteristics can be used by each standing committee, Region, and NERC Program.
- **3<sup>rd</sup> Quarter**
  - July 2011 – Identify metrics or measurements that could be used to assess ALR.

- August 2011 – Pilot characteristic measurements. Report progress to Board of Trustees.
- September 2011 – Update Regions and NERC program areas and seek guidance on the identified characteristics and measurement methods.
- September 2011 – Present initial results and outline of expected final report for concurrence.
- **4<sup>th</sup> Quarter**
  - October 2011 – Continue piloting and, if necessary, refining ALR characteristics and measurements. Begin drafting of final report.  
November 2011 – Complete draft final report, along with results from piloting and recommendations for next steps. Share initial findings with Board of Trustees.
  - December 2011 – Present draft final report to the standing committees and, and seek approval of revised definition of ALR and input on draft report.

## **2012**

- **1<sup>st</sup> Quarter**

- January 2012 – Incorporate the input from the standing committees.
- February 2012 – Present final results to NERC's MRC and BoT for approval

## **Business Continuity Guideline Task Force**

### **Action Required**

Approve guideline for posting for broad industry comment.

### **Background**

The Business Continuity Guideline Task Force (BCGTF) has completed the review and update of all comments received during the initial 30-day CIPC posting of the document. A total of 6 commenters provided comments. All comments were reviewed, responded to, and the guideline was updated based on the comments received.

A redline and clean version of the guideline are included in the agenda package. The complete record of the comments and responses is posted on the SGWG web page (at <http://www.nerc.com/filez/sgwg.html>).

CIPC is requested to approve the guideline document to be sent for a 45-day broad industry review, after which the BCGTF will again review, respond to comments, and update the guideline. Following that review and update period, CIPC will be requested to approve the final guideline as a CIPC guideline.

## 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<sup>1</sup> 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.

<sup>1</sup> 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"

10 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  
15 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.*

20 **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.

25 **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  
30 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  
35 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  
40 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.

45 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  
50 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.

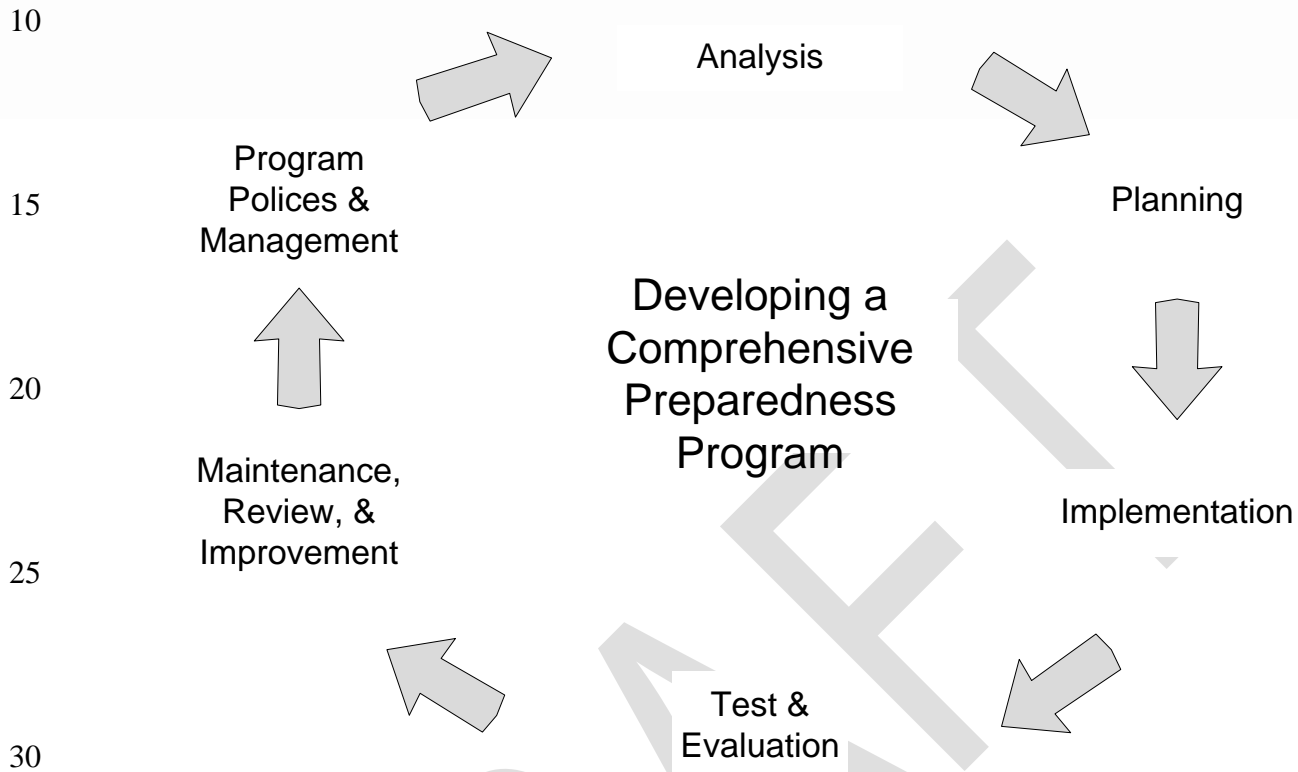


Figure 1: Business Continuity Life Cycle

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**

10 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**

15 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**

20 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**

25 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:**

30 *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001,  
[http://www.esisac.com/publicdocs/ApproachforAction\\_June2001.pdf](http://www.esisac.com/publicdocs/ApproachforAction_June2001.pdf)

35 Business Continuity Institute Good Practices Guidelines:  
<http://www.thebci.org/gpg.htm>

40 DRI International (DRII), Business Continuity Management Program;  
<https://www.drii.org/professionalprac/index.php>

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

10 PS-Prep Framework Guide: Electric Sector Voluntary Private Sector Preparedness  
Accreditation and Certification Program,  
Available on HSIN

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

## PS-PREP: 3 Adopted Standards

20 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.

25 ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and  
Continuity Management Systems, Copyright 2010, American National Standards  
Institute. Used with permission.  
<https://www.asisonline.org/guidelines/published.htm>

30 BS25999-2:2007, Specification for Business Continuity Management, Copyright  
2007, British Standards Institution. Used with permission.  
[www.bsi-emea.com/BCM/Overview/index.xalter](http://www.bsi-emea.com/BCM/Overview/index.xalter)

35 NFPA 1600-2010, Disaster/Emergency Management and Business Continuity  
Programs, Copyright 2010, National Fire Protection Association. Used with  
permission.  
[www.nfpa.org/assets/files/PDF/NFPA16002010.pdf](http://www.nfpa.org/assets/files/PDF/NFPA16002010.pdf)

## Additional Resources:

### 40 Security:

National Strategy for Homeland Security; Homeland Security Council; October 2007;  
[http://www.dhs.gov/xlibrary/assets/nat\\_strat\\_homelandsecurity\\_2007.pdf](http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf)

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

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

10 *Threat Alert System and Cyber Response Guidelines for the Electricity Sector v2.0*,  
NERC, October 2002,  
<http://esisac.com/library-guidelines.htm>

## **Business Continuity:**

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

20 ASIS, International; *Business Continuity Guideline: A Practical Approach for  
Emergency Preparedness, Crisis Management, and Disaster Recovery*; 2005;  
<http://www.asisonline.org/guidelines/published.htm>

25 Electricity Sector Influenza Pandemic Planning, Preparation, and Response  
Reference Guide; NERC; February 2006;  
<http://esisac.com/library-cip-doc.htm>

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

35 “Business Continuity Guideline: A Practical Approach for Emergency Preparedness,  
Crisis Management, and Disaster Recovery,” Copyright (c) 2005 by ASIS  
International. Used by permission. The complete guideline is available from ASIS  
International, 1625 Prince Street, Alexandria, Virginia 22314  
<http://www.asisonline.org/guidelines/published.htm>.

Business Continuity Institute Good Practices Guidelines:  
<http://www.thebci.org/gpg.htm>

## **Emergency Management:**

45 Federal Emergency Management Administration (FEMA); *Emergency Management  
Guide for Business and Industry*; FEMA Document 141, October 1993; Washington,  
D.C.;  
<http://www.fema.gov/business/guide/index.shtm>

50 Federal Emergency Management Administration (FEMA), *Standard Checklist  
Criteria for Business Recovery*; October 1993; Washington, D.C.,  
<http://www.fema.gov/business/bc3.shtm>.

10

**Revision History:**

<b>Date</b>	<b>Version Number</b>	<b>Reason/Comments</b>
6/14/2002	1.0	Initial Version – <i>Continuity of Business Processes Security Guideline</i>
7/1/2007	2.0	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.
4/3/11	2.1	Completely revised and posted for initial CIPC Comment
4/5	2.15	Correction of formatting and typographical errors in initial posting
5/9	2.16	Updated based on comments received
5/12	2.17	Posting for industry Comment

15

20

25

30

35

40

45

50

55

DRAFT

## 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, for 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 essential/critical<sup>1</sup> 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.

<sup>1</sup> 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 operational-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.

### **Definitions:**

~~The following terms are defined in the NERC Glossary of Terms<sup>2</sup>:~~

~~Critical Assets~~

~~Critical Cyber Assets~~

~~Cyber Security Incident~~

~~Disturbance~~

~~The following definitions apply in this guideline:~~

~~**Alternate Worksite**<sup>4</sup> — A work location other than the primary location, to be used when the primary location is not accessible or is incapable of normal operations.~~

~~**Business Continuity**<sup>4</sup> — A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.~~

~~**Business Continuity Plan**<sup>4</sup> — A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level.~~

~~**Crisis**<sup>4</sup> — Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization’s financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization’s reputation, products, or officers, and therefore negatively impacting its future.~~

~~**Crisis Management Team**<sup>4</sup> — A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.~~

**Critical Function**<sup>4</sup> — Business activity or process that cannot be interrupted or rendered unavailable for several business days without causing a significant negative impact to the organization.

**Disaster**<sup>4</sup> — An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths, or loss of essential resources or services.

**Disaster Recovery**<sup>4</sup> — Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

**Emergency**<sup>4</sup> — An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability.

**Mitigation Strategies**<sup>4</sup> — Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.

**Pandemic**<sup>3</sup> — An epidemic outbreak of an infectious disease that spreads worldwide, or at least across a large region. The worldwide outbreak of a disease in humans in numbers clearly in excess of normal.

**Prevention**<sup>4</sup> — Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring. The tasks included in prevention should include compliance with corporate policy, mitigation strategies, and behavior and programs to support avoidance and deterrence and detection.

**Readiness**<sup>4</sup> — The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.

**Recovery/Resumption**<sup>4</sup> — Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.

**Response**<sup>4</sup> — Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.

**Risk Assessment**<sup>4</sup> — Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or

~~vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.~~

### Scope of Application:

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

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

~~A Risk Assessment would be made for each resource and function 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.~~

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

~~Essential resources and facilities support the essential business processes ability to operate, and replacements/alternatives are needed in order to effectively recover the process following a disruption.~~

~~Ultimately, the critical business processes support the company's core missions, which include:~~

- ~~• Serve its customers with a reliable source of electric energy to maintain a normal quality of life,~~
- ~~• 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.~~

### 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 essential/critical to minimize the impact from natural and man-made disasters.

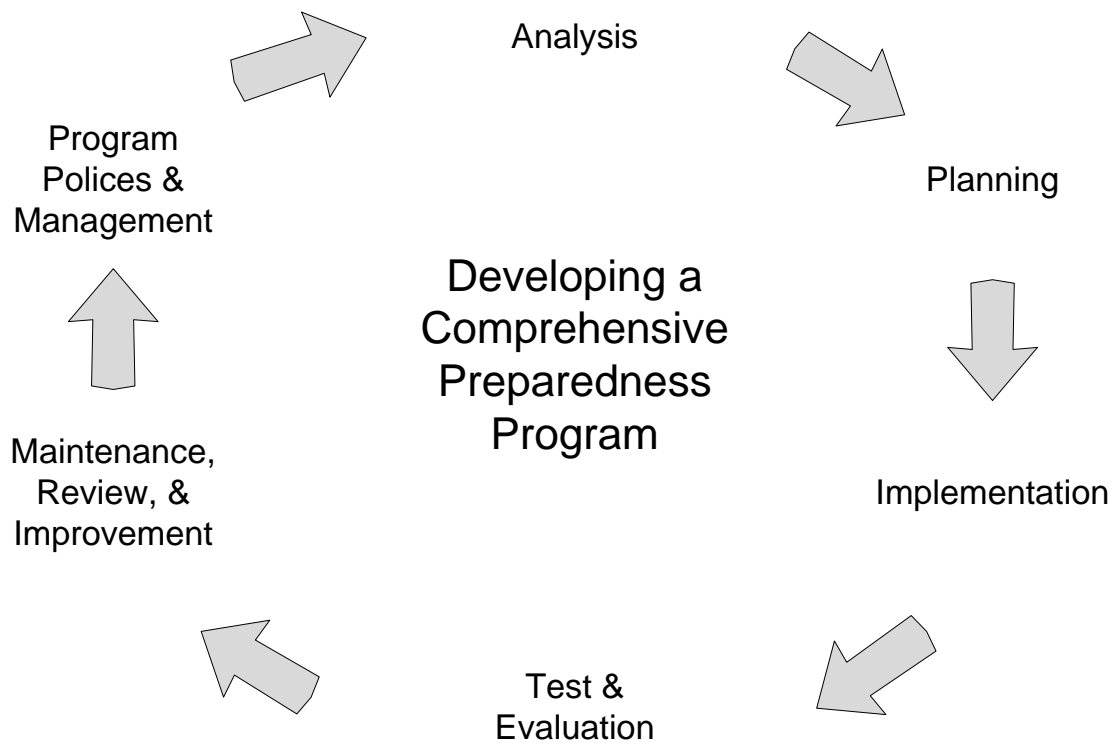


Figure 1: Business Continuity Life Cycle

| [Based on the PS-PREP program documentation, aA](#) 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:

*An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001,

[http://www.esisac.com/publicdocs/ApproachforAction\\_June2001.pdf](http://www.esisac.com/publicdocs/ApproachforAction_June2001.pdf)

Business Continuity Institute Good Practices Guidelines:

<http://www.thebci.org/gpg.htm>

DRI International (DRII), Business Continuity Management Program;

<https://www.drii.org/professionalprac/index.php>

Disaster Recovery Journal (DRJ); Glossary v2.0: DRJ and DRII;

<http://www.drj.com/tools/tools/glossary-2.html>

PS-Prep Framework Guide: Electric Sector Voluntary Private Sector Preparedness Accreditation and Certification Program,

~~Date TBD; Link TBD~~ Available on HSIN

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

~~Links TBD~~ 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.

ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems, Copyright 2010, American National Standards Institute. Used with permission.

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

BS25999-2:2007, Specification for Business Continuity Management, Copyright 2007, British Standards Institution. Used with permission.

[www.bsi-emea.com/BCM/Overview/index.xalter](http://www.bsi-emea.com/BCM/Overview/index.xalter)

[NFPA 1600-2010, Disaster/Emergency Management and Business Continuity Programs, Copyright 2010, National Fire Protection Association. Used with permission.](http://www.nfpa.org/assets/files/PDF/NFPA16002010.pdf)  
[www.nfpa.org/assets/files/PDF/NFPA16002010.pdf](http://www.nfpa.org/assets/files/PDF/NFPA16002010.pdf)

## **Additional Resources:**

### **Security:**

[National Strategy for Homeland Security; Homeland Security Council; October 2007;](http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf)  
[http://www.dhs.gov/xlibrary/assets/nat\\_strat\\_homelandsecurity\\_2007.pdf](http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf)

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>

*Threat Alert System and Cyber Response Guidelines for the Electricity Sector v2.0*,  
NERC, October 2002,

<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>

ASIS, International; *Business Continuity Guideline: A Practical Approach for  
Emergency Preparedness, Crisis Management, and Disaster Recovery*; 2005;

<http://www.asisonline.org/guidelines/published.htm>

[Electricity Sector Influenza Pandemic Planning, Preparation, and Response  
Reference Guide](http://www.nerc.com/ess/inf/pandemic/); NERC; February 2006;

<http://esisac.com/library-cip-doc.htm>

Purpose of Standard Checklist Criteria for Business Recovery;

<http://www.fema.gov/business/bc.shtm>

[“Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery,” Copyright \(c\) 2005 by ASIS International. Used by permission. The complete guideline is available from ASIS International, 1625 Prince Street, Alexandria, Virginia 22314  
http://www.asisonline.org/guidelines/published.htm.](http://www.asisonline.org/guidelines/published.htm)

[Business Continuity Institute Good Practices Guidelines:  
http://www.thebci.org/gpg.htm](http://www.thebci.org/gpg.htm)

## **Emergency Management:**

Federal Emergency Management Administration (FEMA); *Emergency Management Guide for Business and Industry*; FEMA Document 141, October 1993; Washington, D.C.;

<http://www.fema.gov/business/guide/index.shtm>

Federal Emergency Management Administration (FEMA), *Standard Checklist Criteria for Business Recovery*; October 1993; Washington, D.C.,

<http://www.fema.gov/business/bc3.shtm>.

## **Endnotes**

~~1. “Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery,” Copyright (c) 2005 by ASIS International. Used by permission. The complete guideline is available from ASIS International, 1625 Prince Street, Alexandria, Virginia 22314  
<http://www.asisonline.org/guidelines/published.htm>.~~

~~2. “Glossary of Terms Used in Reliability Standards;” NERC; April 20, 2010;  
[http://www.nerc.com/docs/standards/rs/Glossary\\_of\\_Terms\\_2010April20.pdf](http://www.nerc.com/docs/standards/rs/Glossary_of_Terms_2010April20.pdf)~~

~~3. Definition summarized from numerous sources. The central definition is that obtained from the US Center for Disease Control: “Pandemic: The worldwide outbreak of a disease in humans in numbers clearly in excess of normal.”  
<http://www.pandemicflu.gov/glossary/#P>~~

~~4. [Business Continuity Institute Good Practices Guidelines:  
http://www.thebci.org/gpg.htm](http://www.thebci.org/gpg.htm)~~

## Revision History:

Date	Version Number	Reason/Comments
6/14/2002	1.0	Initial Version – <i>Continuity of Business Processes Security Guideline</i>
7/1/2007	2.0	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.
<u>4/3/11</u>	<u>2.1</u>	<u>Completely revised and posted for initial CIPC Comment</u>
<u>4/5</u>	<u>2.15</u>	<u>Correction of formatting and typographical errors in initial posting</u>
<u>5/9</u>	<u>2.16</u>	<u>Updated based on comments received</u>

## **CIPC Membership Roundtable**

### **Action Required**

Discussion.

### **Background**

The CIPC, at its December 2010 meeting provided a list of suggestions for future meetings. One of those items was to have roundtable discussions of topics of interest to CIPC members at each CIPC meeting.

The roundtable discussion topic for the June 2011 CIPC meeting is “Communications – Exchanging information about emerging threats”.

CIPC members are requested to prepare thoughts on how information is, could be, or should be communicated amongst members of their region, or between members between regions concerning emerging threats. In particular,

- What mechanisms exist, or should be established ahead of time so that they can be rapidly initiated when a threat emerges?
- What kinds of information sharing protocols should be established?
- Should there be “triggering actions” that initiate the exchanging of information?
- What technologies should be used? What happens if the chosen technology is unavailable due to the threat?
- Can or should NERC be involved in the facilitation of the information sharing? If so, how?