Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SAR posted for comment (March 20, 2008)
2. SC authorized moving the SAR forward to standard development (July 10, 2008)
3. CSO706 SDT appointed (August 7, 2008)
4. Version 1 of CIP-002 to CIP-009 approved by FERC (January 18, 2008)
5. Version 2 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
6. Version 3 of CIP-002 to CIP-009 approved by FERC (September 30, 2009)
7. Version 4 of CIP-002 to CIP-009 approved by NERC Board of Trustees (January 24, 2011) and filed with FERC (February 10, 2011)
8. Version 5 of CIP-002 to CIP-011 posted for formal comment and ballot (mm-dd-yy)

Description of Current Draft

This is the first posting of Version 5 of the CIP Cyber Security Standards for a 45-day formal comment period. An initial concept paper, Categorizing Cyber Systems — An Approach Based on BES Reliability Functions, was posted for public comment in July 2009. An early draft consolidating CIP-002 – CIP-009, numbered CIP-010-1 and CIP-011-1, was posted for public informal comment in May 2010. This version (Version 5) reverts to the original organization of the standards with some changes and addresses the balance of the FERC directives in its Order 706 approving Version 1 of the standards.

Anticipated Actions	Anticipated Date
45-day Formal Comment Period with Parallel Initial Ballot	11/03/2011
30-day Formal Comment Period with Parallel Successive Ballot	March 2012
Recirculation ballot	June 2012
BOT adoption	June 2012

Effective Dates

1. **18 Months Minimum** – The Version 5 CIP Cyber Security Standards shall become effective on the later of January 1, 2015, or the first calendar day of the seventh calendar quarter after the date of the order providing applicable regulatory approval. Notwithstanding any order to the contrary, CIP-002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this implementation plan.[1]
2. In those jurisdictions where no regulatory approval is required, the standards shall become effective on the first day of the seventh calendar quarter following Board of Trustees approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

[1] In jurisdictions where CIP-002-4 through CIP-009-4 have not yet become effective according to their implementation plan (even if approved by order), this implementation plan and the Version 5 CIP Cyber Security Standards supersede and replace the implementation plan and standards for CIP-002-4 through CIP-009-4.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center"	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3 In Requirement 1.6, deleted the sentence pertaining to removing component or system from service in order to perform testing, in response to FERC order issued September 30, 2009.	
3	12/16/09	Approved by the NERC Board of Trustees	Update
3	3/31/10	Approved by FERC	
4	12/30/10	Modified to add specific criteria for Critical Asset identification	Update
4	1/24/11	Approved by the NERC Board of Trustees	Update
5	TBD	Modified to coordinate with other CIP standards and to revise format to use RBS Template	

Definitions of Terms Used in the Standard

See the associated "Definitions of Terms Used in Version 5 CIP Cyber Security Standards," which consolidates and includes all newly defined or revised terms used in the proposed Version 5 CIP Cyber Security Standards.

When this standard has received ballot approval, the text boxes will be moved to the Application Guidelines Section of the Standard.

A. Introduction

1. Title: Cyber Security — Incident Reporting and Response Planning

2. Number: CIP-008-5

3. Purpose: Standard CIP-008-5 requires the identification, classification, response, and reporting of BES Cyber Security Incidents related to BES Cyber Assets and BES Cyber Systems.

4. Applicability:

4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of Functional Entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific Functional Entity or subset of Functional Entities are the applicable entity or entities, the Functional Entity or Entities are specified explicitly.

4.1.1 Balancing Authority

4.1.2 Distribution Provider that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator

4.1.6 Load-Serving Entity that owns Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.1.7 NERC

4.1.8 Regional Entity

4.1.9 Reliability Coordinator

4.1.10 Transmission Operator

4.1.11 Transmission Owner

4.2. Facilities:

4.2.1 Load Serving Entity: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard

4.2.2 Distribution Providers: One or more Facilities that are part of any of the following systems or programs designed, installed, and operated for the protection or restoration of the BES:

- A UFLS program required by a NERC or Regional Reliability Standard
- A UVLS program required by a NERC or Regional Reliability Standard
- A Special Protection System or Remedial Action Scheme required by a NERC or Regional Reliability Standard
- A Transmission Protection System required by a NERC or Regional Reliability Standard
- Its Transmission Operator's restoration plan

4.2.3 All other Responsible Entities: **All BES Facilities**

4.2.4 Exemptions: The following are exempt from Standard CIP-008-5

4.2.4.1 Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.4.2 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

4.2.4.3 In nuclear plants, the systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F. R. Section 73.54.

4.2.4.4 Responsible Entities that, in compliance with Standard CIP-002-5, identify that they have no BES Cyber Systems.

5. Background:

Standard CIP-008-5 exists as part of a suite of CIP Standards related to cyber security. CIP-002-5 requires the initial identification and categorization of BES Cyber Systems. CIP-003-5, CIP-004-5, CIP-005-5, CIP-006-5, CIP-007-5, CIP-008-5, CIP-009-5, CIP-010-1 and CIP-011-1 require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems. This suite of CIP Standards is referred to as the *Version 5 CIP Cyber Security Standards*.

Each requirement opens with "*Each Responsible Entity shall implement one or more documented processes that include the required items in [Table Reference].*" The referenced table requires the specific elements in the procedures for a common subject matter as applicable.

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show documentation and implementation of specific elements required in the documented processes. A numbered list in the measure means the evidence example includes all of the items in the list. In contrast, a bulleted list provides multiple options of acceptable evidence. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an inclusive list.

The term *documented processes* refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not infer any naming or approval structure beyond what is stated in the requirements. An entity should include as much as they feel necessary in their documented processes, but they must address the applicable requirements in the table.

The terms *program* and *plan* are sometimes used in place of *documented processes* where it makes sense and is commonly understood. For example, documented processes describing a response are typically referred to as *plans* (i.e. incident response plans and recovery plans). Likewise, a security plan can describe an approach involving multiple procedures to address a broad subject matter.

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans and procedures involving a subject matter. Examples in the Standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the Standards.

Applicability

Each table row has an applicability column to further define the scope to which a specific requirement row applies. The CSO706 SDT adapted this concept from the NIST Risk Management Framework as a way of applying requirements more appropriately based on impact and connectivity characteristics. The following conventions are used in the applicability column as described.

- **All Responsible Entities** – Applies to all Responsible Entities listed in the Applicability section of the Standard. This requirement applies at an organizational level rather than individually to each BES Cyber System. Requirements having this applicability comprise basic elements of an organizational CIP cyber security program.
- **High Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as High Impact according to the CIP-002-5 identification and categorization

processes. Responsible Entities can implement common controls that meet requirements for multiple High and Medium Impact BES Cyber Systems. For example, a single training program could meet the requirements for training personnel across multiple BES Cyber Systems.

- **Medium Impact BES Cyber Systems –** Applies to BES Cyber Systems categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers –** Only applies to BES Cyber Systems located at a Control Center and categorized as Medium Impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems with External Routable Connectivity –** Only applies to Medium Impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Low Impact BES Cyber Systems with External Routable Connectivity** – Applies to each Low Impact BES Cyber Systems with External Routable Connectivity according to the CIP-002-5 identification and categorization process, which includes all other BES Cyber Systems not categorized as High or Medium.
- **Associated Electronic Access Control or Monitoring Systems –** Applies to each Electronic Access Control or Monitoring System associated with a corresponding High or Medium Impact BES Cyber Systems. Examples include, but are not limited to firewalls, authentication servers, and log monitoring and alerting systems
- **Associated Physical Access Control Systems –** Applies to each Physical Access Control System associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Associated Protected Cyber Assets –** Applies to each Protected Cyber Asset associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Plans associated with High Impact BES Cyber Systems or Medium Impact BES Cyber Systems -a**pplies to any plan associated with a corresponding High or Medium Impact BES Cyber Systems.
- **Electronic Access Points –** Applies at Electronic Access Points (with External Routable Connectivity or dial-up connectivity) associated with a referenced BES Cyber System.
- **Electronic Access Points with External Routable Connectivity** – Applies at Electronic Access Points with External Routable Connectivity. This excludes those Electronic Access Points with dial-up connectivity.
- **Locally Mounted Hardware or Devices Associated with Defined Physical Boundaries** – Applies to the locally mounted hardware (e.g. such as motion sensors, electronic lock control mechanisms, and badge readers) associated with a

Defined Physical Boundary for High or Medium Impact BES Cyber Systems. These hardware and devices are excluded in the definition of Physical Access Control Systems.

B. Requirements and Measures

Rationale for R1: So that consistent responses to BES Cyber Security Incidents involving BES Cyber Assets and BES Cyber Systems occur. Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Once the number and severity of events rises to the level of becoming a reportable incident NERC EOP 4 directs further external reporting actions and timing requirements. When a requirement applies to All Responsible Entities, the drafting team proposes that an enterprise or single incident response plan for all BES Cyber Systems may be submitted. An organization may have a common plan for multiple registered entities it owns.

Summary of Changes: (FERC directives, most significant items, summary of smaller items)

R1. Each Responsible Entity shall have one or more BES Cyber Security Incident response plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*. *[Violation Risk Factor: Lower] [Time Horizon: Long Term Planning]*

M1. Evidence must include each of the documented plan(s) that collectively include each of the applicable items in *CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications*.

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.1	All Responsible Entities	Processes to identify, classify, and respond to BES Cyber Security Incidents.	Evidence may include, but is not limited to, dated copies of BES Cyber Security Incident response plan(s) that include how to identify, classify, and respond to BES Cyber Security Incidents targeting the Electronic Security Perimeter or Defined Physical Boundary of a BES Cyber System and covers incidents that impact the reliability of BES.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
1.2	All Responsible Entities	A process to determine if an identified BES Cyber Security Incident is a Reportable BES Cyber Security Incident.	Evidence may include, but is not limited to, dated documentation of process(es) that provide guidance or thresholds for determining which BES Cyber Security Incidents are also Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R1.1*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R1 – BES Cyber Security Incident Response Plan Specifications			
Part	**Applicability**	**Requirements**	**Measures**
1.3	All Responsible Entities	Define: 1.3.1. The roles and responsibilities of BES Cyber Security Incident response personnel; 1.3.2. The BES Cyber Security Incident handling procedures; 1.3.3. Internal staff and external organizations that should receive communication of the incident.	Evidence may include, but is not limited to, dated BES Cyber Security Incident response process(es) or procedure(s) that addresses roles and responsibilities of BES Cyber Security Incident response personnel, BES Cyber Security Incident handling processes or procedures, and communication processes or procedures.
Reference to prior version: *CIP-008 R1.2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R2: Added testing requirements to verify the REs response plan's effectiveness and consistent application in responding to a BES Cyber Security Incident(s) impacting a BES Cyber System.

R2. Each Responsible Entity shall implement its documented BES Cyber Security Incident response plan(s) to collectively include each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations]*

M2. Evidence must include, but is not limited to, documentation that collectively demonstrates implementation of each of the applicable items in *CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing*.

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.1	All Responsible Entities	When a BES Cyber Security Incident occurs, the incident response plans must be used when incidents occur and include recording of deviations taken from the plan during the incident or test.	Evidence may include, but is not limited to, incident reports, logs, and notes that were kept during the incident response process, and documentation that lists and justifies deviations taken from the plan during the incident.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged. Allows deviation from plan during actual events or testing if deviations are recorded for review.*	

CIP-008-5 Table R2 – BES Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicability**	**Requirements**	**Measures**
2.2	All Responsible Entities	Implement the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months between executions of the plan(s): • by responding to an actual incident, or • with a paper drill or table top exercise, or • with a full operational exercise.	Evidence may include, but is not limited to, dated evidence of implementing the BES Cyber Security Incident response plan(s) initially upon the effective date of the standard and at least once every calendar year thereafter, not to exceed 15 months, from response to an actual incident, or with a paper drill or table top exercise, or with a full operational exercise.
Reference to prior version: *CIP-008 R1.6*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	
2.3	All Responsible Entities	Retain relevant documentation related to Reportable BES Cyber Security Incidents for three calendar years.	Evidence may include, but is not limited to, dated documentation related to Reportable BES Cyber Security Incidents.
Reference to prior version: *CIP-008 R2*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

Rationale for R3: Conduct sufficient reviews, updates and communications to verify the REs response plan's effectiveness and consistent application in responding to a Cyber Security Incident(s) impacting a BES Cyber System.

Summary of Changes: Addressed BES Cyber Security Incident response plan review, update, and communication specifications to ensure that BES Cyber Security Incident response plans remain updated and individuals are aware of the updates.

R3. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication*. *[Violation Risk Factor: Lower] [Time Horizon: Operations Assessment and Real-Time Operations]*

M3. Evidence must include each of the applicable documented processes that include each of the applicable items in *CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update and Communication* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.1	All Responsible Entities	Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary.	Evidence may include, but is not limited to, dated documentation of a review of each BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 calendar months, and an updated BES Cyber Security Incident response plan if necessary.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Minor wording changes; essentially unchanged.*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Applicability**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan.	Evidence may include, but is not limited to dated documentation of a review of the BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, including dated documentation of any lessons learned associated with the response plan.
Reference to prior version: *CIP-008 R1.5*		**Change Description and Justification:** *Included requirement for review after testing or actual response based on review of DHS controls*	
3.3	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan based on any documented lessons learned within sixty calendar days of the completion of the review of that plan.	Evidence may include, but is not limited to dated, documented lessons learned from the results of the BES Cyber Security Incident response plan and the dated, revised plan.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	

CIP-008-5 Table R3 – BES Cyber Security Incident Response Plan Review, Update, and Communication			
Part	**Part**	**Part**	**Part**
3.4	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Update the BES Cyber Security Incident response plan(s) within thirty calendar days of any organizational, or technology changes that impact that plan.	Acceptable evidence may include, but is not limited to, updated documentation reflecting changes made to the BES Cyber Security Incident response plan in response to organizational or technology changes.
Reference to prior version: *CIP-008 R1.4*		**Change Description and Justification:** *Included additional specification on update of response plan Addresses FERC Requirement (686) to modify on lessons learned and aspects of the DHS Controls*	
3.5	High Impact BES Cyber Systems Medium Impact BES Cyber Systems	Communicate each update to the BES Cyber Security Incident response plan to each person with a defined role in the BES Cyber Security Incident response plan within thirty calendar days of the completion of the update of that plan.	Evidence of communication of updates may include, but is not limited to: • Emails • USPS or other mail service • Electronic distribution system • Training sign-in sheets.
Reference to prior version: *New Requirement*		**Change Description and Justification:** *Added specific timing requirement on communication of plan changes based on review of the DHS Controls*	

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

- Regional Entity
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.
- If the Responsible Entity is also a Regional Entity, the ERO or a Regional Entity approved by the ERO and FERC or other applicable governmental authorities shall serve as the Compliance Enforcement Authority.
- If the Responsible Entity is NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.

1.2. Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was complaint for the full time period since the last audit.

- Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audit

Self-Certification

Spot Checking

Compliance Investigation

Self-Reporting

Complaint

1.4. Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long Term Planning**	**Lower**	N/A	N/A	The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not define the roles and responsibilities of response personnel, or does not define incident handling procedures, or does not communicate the incident to appropriate organizations.	The Responsible Entity has not developed a BES Cyber Security Incident response plan to identify, classify, and respond to BES Cyber Security Incidents. OR The Responsible Entity has developed a BES Cyber Security Incident response plan, but the plan does not identify Reportable BES Cyber Security Incidents.
R2	**Operations Planning** **Real-time Operations**	**Lower**	N/A	N/A	N/A	The Responsible Entity does not use its BES Cyber Security Incident response plan when an incident occurs. OR The Responsible Entity

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						has not tested the execution of its BES Cyber Security Incident response plan once each calendar year, not to exceed 15 calendar months between executions of the plan.
R3	**Operations Assessment** **Real-time Operations**	**Lower**	N/A	N/A	The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans based on lessons learned within 30 calendar days of execution. OR The Responsible Entity has reviewed but not updated each of its BES Cyber Security Incident response plans within 30 calendar days of any	The Responsible Entity has not reviewed the results of each of its BES Cyber Security Incident response plan(s), test or actual incident response, within 30 calendar days of execution. OR The Responsible Entity has reviewed and updated each of its BES Cyber Security Incident response plans but has not communicated all

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					system, organizational, or technology change that impacts one of the response plans.	updates to all responsible personnel.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

FAQ, SP99, ISA, US-CERT, NIST Guidelines, etc. as a source of materials

Requirement R1:

A Reportable BES Cyber Security Incident is a BES Cyber Security Incident that results in a necessary response action. A response action can fall into one of two categories: necessary or elective. The distinguishing characteristic is whether or not action was taken in response to an event. Precautionary measures that are not in response to any persistent damage or effects may be designated as elective. All other response actions should be designated as necessary.