

## Frequently Asked Questions (FAQs) for Cyber Security Standards CIP-003-1 — Cyber Security — Management Controls

Note that this document contains responses to general questions for CIP-002-1 through CIP-009-1 and specific questions for CIP-003-1. The questions and responses are **only** applicable to CIP-002-1 through CIP-009-1.

### General Questions for CIP-002-1 through CIP-009-1

1. **Question:** *What is meant by the term “where technically feasible?”*

**Answer:** Technical feasibility refers only to engineering possibility and is expected to be a “can/cannot” determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by the Responsible Entity. The Responsible Entity is not required to replace any equipment in order to achieve compliance with the Cyber Security Standards. When existing equipment is replaced, however, the Responsible Entity is expected to use reasonable business judgment to evaluate the need to upgrade the equipment so that the new equipment can perform a particular specified technical function in order to meet the requirements of these standards.

Although some standards do not require documentation and compensating measures when a determination of technical infeasibility has been made, Responsible Entities are free to do so in every such circumstance. Some standards do require such documentation and compensating measures because of the criticality of the specific requirement.

2. **Question:** *What is meant by the phrase “reasonable business judgment?”*

**Answer:** The phrase “reasonable business judgment” has an almost 200-year history in the business and corporation laws of America, Canada, and other Common Law nations. The phrase is in NERC Standards CIP-002 through CIP-009 to reflect — and to inform — any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards — that Responsible Entities have a significant degree of flexibility in implementing these Standards. Courts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances. A common formulation indicates the business judgment of an entity — even if incorrect in hindsight — should not be overturned as long as it was made (1) in good faith (not an abuse or indiscretion), (2) without improper favor or bias, (3) using reasonably complete (if imperfect) information as available at the time of the decision, (4) based on a rational belief that the decision is in the entity’s business interest. This principle, however, does not protect an entity from simply failing to make a decision.

3. **Question:** *What is meant by “data,” “documents,” “documentation,” “logs,” and “records?” What are the differences between them?*

**Answer:** As used in these Cyber Security Standards, these four terms are intended to be understood generally as follows (although these informal definitions do indicate some degree of overlap, depending upon the context in which the terms are used):

**DATA:** information in a “raw” form; facts which may be represented or symbolized in records.

**RECORDS:** Records typically provide evidence of data, such as a “snapshot” in time of actions and events. A record may be in paper or “electronic” format (either analog or digital, such as “on” videotape or DVD, or “on” or “in” a hard-drive). Typically, official records (such as “business records”) can only be modified or revised in compliance with proper and auditable trails, and thus can serve as objective, reliable evidence to demonstrate that a fact, situation or activity has occurred (thereby being usable, for instance, to demonstrate compliance with a requirement of these Cyber Security Standards).

**LOGS:** Generally, a log is a specific type or collection of recorded data (generally, as pertaining to a series of similar or related actions or events) that may be generated automatically or manually. At a minimum, logs identify the event, who or what caused the event, and when the event occurred (a “time-stamp”). A log, as a type of record, can be in paper or electronic format. A log may also, in some contexts, be referred to as a type of document, and several similar (or a “set” of) logs may be referred to as a type of documentation.

**DOCUMENTS:** A document is a record that generally is used to represent or demonstrate what an organization has done or expects to do (such as a “business record” in the legal sense). Documents may include but are not limited to policies, processes and procedures, specifications, drawings, maps, etc. As a type of record, a document can be in paper or electronic format.

**DOCUMENTATION:** A series or collection of related documents generally pertaining to a particular issue. Documentation can be records that demonstrate what an organization does, should do, or plans to do, including instructions to employees on how they should perform certain tasks. Documentation may also be records that represent, or can be used to demonstrate, what an organization has done or expects to do (such as a set of “business records”). Thus, the term “documentation” may be used to refer to any collection of documents (or “documentary” material) such as “business records,” a plan or set of plans, a policy with associated procedures, or “the log” or “all the logs” generated by a specific system or device over a specified period.

As with implementing all of the NERC Cyber Security Standards CIP-002 through CIP-009, Responsible Entities are to exercise reasonable business judgment in interpreting these terms. One important source to assist in such interpretation is the Responsible Entity's corporate document retention schedule. There are many additional useful sources for making such

interpretations. One comprehensive source, that itself refers to a number of other authoritative sources (including statutory and regulatory definitions), is:

Rutgers University Libraries Records Management Program Definitions  
[http://www.libraries.rutgers.edu/rul/libs/scua/ru\\_records/definitions.shtml](http://www.libraries.rutgers.edu/rul/libs/scua/ru_records/definitions.shtml)

## Standard CIP-003-1 — Cyber Security — Security Management Controls

1. **Question:** *Does the cyber security policy need to be a separate policy or can it be part of the Responsible Entity's overall security and best practices policies?*

**Answer:** The cyber security policy can be part of a larger corporate policy providing that the overall policy demonstrates management's commitment to addressing the requirements of these CIP standards and provides a framework for the governance of these standards.

2. **Question:** *What are some examples of classification levels?*

**Answer:** Information classification levels are used to indicate to personnel the sensitivity of information. Some classification levels could be Top Secret, Secret, Confidential and Unclassified. Other examples include Confidential, Sensitive, Nonpublic, and Public. The names that each entity gives its classification levels are up to each individual entity. Classification levels should be descriptive enough so that anyone looking at the information would be able to determine its relative sensitivity level by its classification. Different handling and protection activities are associated with each classification level.

3. **Question:** *In CIP-003 R1.1. you refer to "emergency situations." What is an emergency situation?*

**Answer:** Emergency situations include both traditional electric utility emergencies (when the operational reliability of the bulk electric system is threatened or restoration of critical service is required for example) as well as emergencies affecting Critical Cyber Assets (e.g. denial of service attacks). The Responsible Entity must take into account "emergency changes" to Critical Cyber Assets required during emergency situations within its change management procedures. Emergency change procedures should not only allow for rapid resolution but the steps taken to implement the change must be auditable. The Responsible Entity's policy must address these situations with consideration given to access control and monitoring requirements from CIP-004 (Personnel and Training), CIP-005 (Electronic Security Perimeters) and CIP-006 (Physical Security). Examples of unexpected occurrences include before, during or after storms, flood, fires, malicious acts or other similar special operating situations.