

Frequently Asked Questions (FAQs) for Cyber Security Standards CIP-005-1 — Cyber Security — Electronic Security

Note that this document contains responses to general questions for CIP-002-1 through CIP-009-1 and specific questions for CIP-005-1. 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

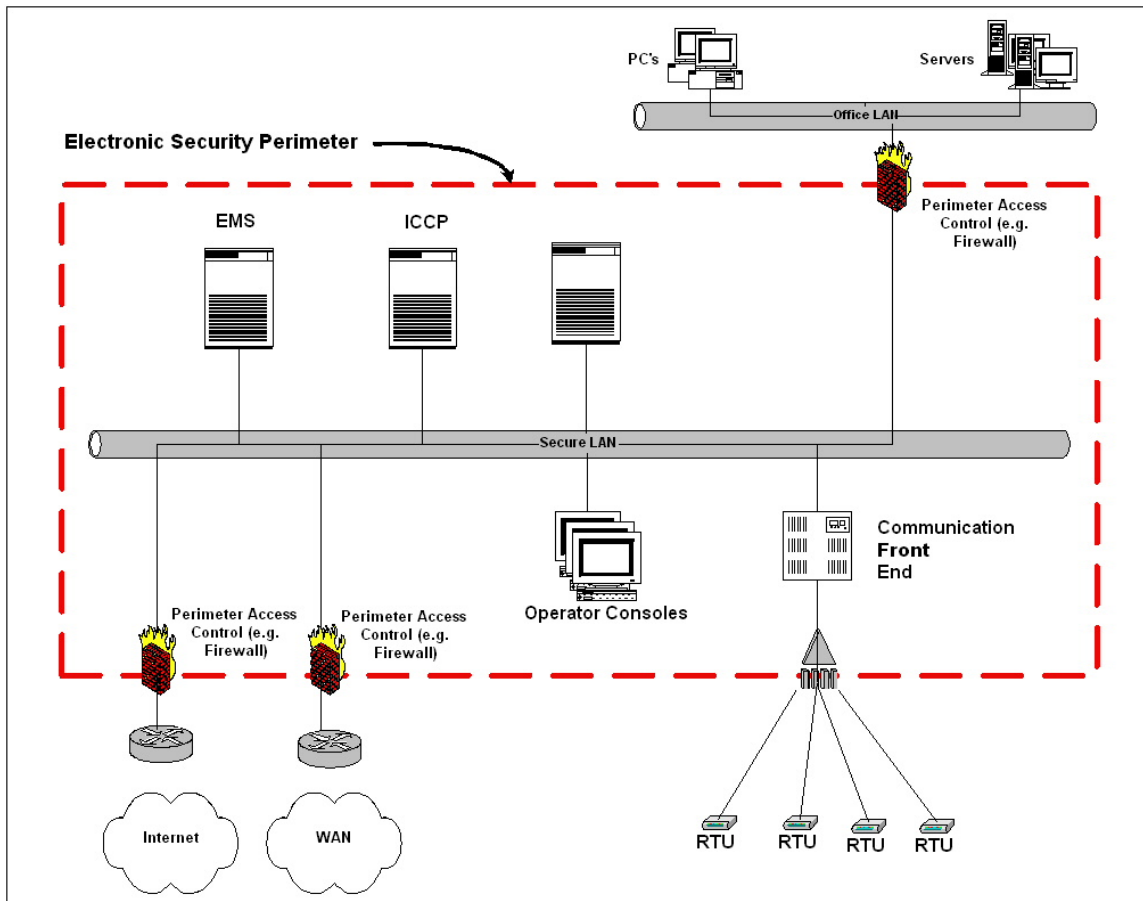
interpretations. One comprehensive source, that itself refers to a number of other authoritative sources (including statutory and regulatory definitions), is:

Rutgers University Libraries Records Management Program Definitions
http://www.libraries.rutgers.edu/rul/libs/scua/ru_records/definitions.shtml

Standard CIP-005-1 — Cyber Security - Electronic Security

1. **Question:** *How do you define the Electronic Security Perimeter?*

Answer: The following schematic illustrates a typical case of how the Electronic Security Perimeter is defined.

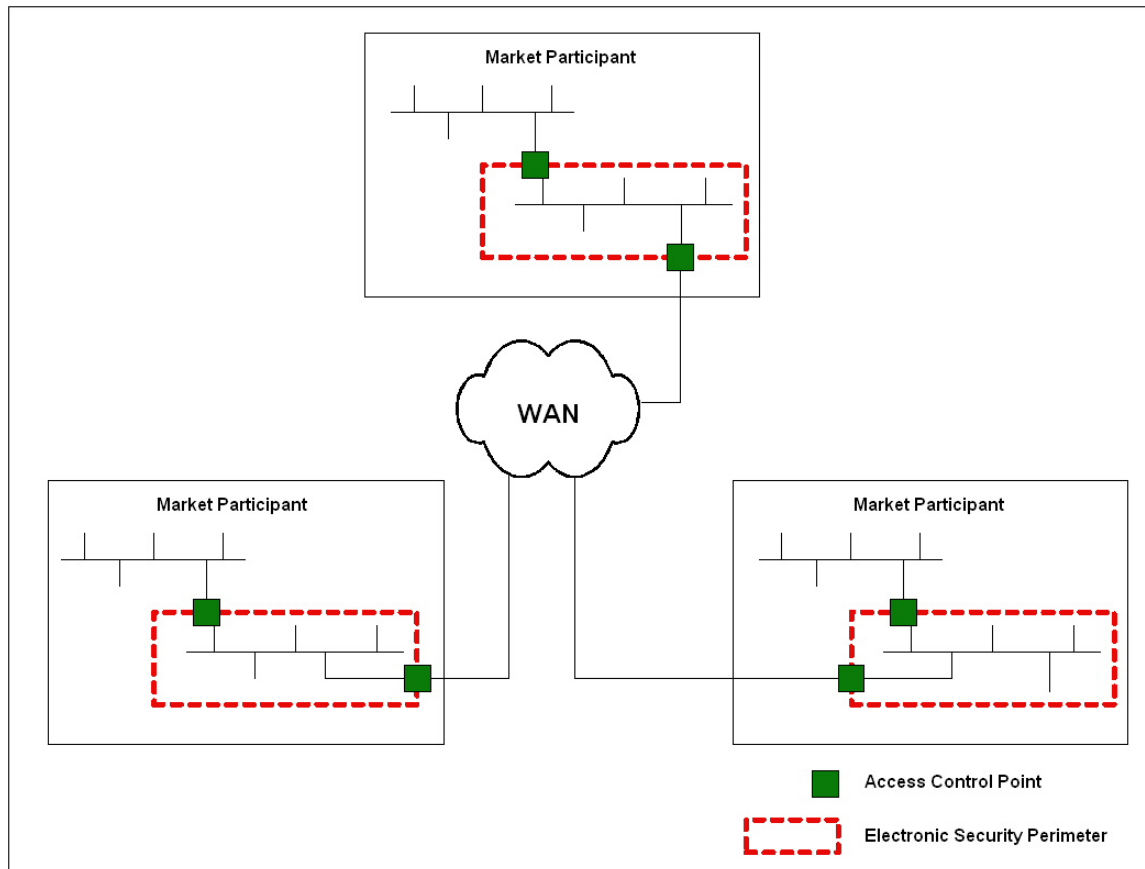


The RTUs may need an Electronic Security Perimeter if they use a routable protocol and meet the definition of a Critical Cyber Asset. Also a single computer may need an Electronic Security Perimeter if it meets the definition of a Critical Cyber Asset.

This standard deals with the security of the electronic perimeter. In a defense in depth approach, appropriate protection measures must also be implemented, as addressed in the requirements for CIP-003 Security Management Controls and CIP-007 Systems Security Management.

2. **Question:** *I am connected to other partners' Electronic Security Perimeters through a Wide Area Network (WAN) connection. What is now included in the Electronic Security Perimeter? Is the connection to the partner included?*

Answer: The standard states that where discrete Electronic Security Perimeters are connected by communication lines, the communication lines are not included in the Electronic Security Perimeter. The following schematic illustrates this point.



3. **Question:** *I have a single RTU that controls a critical bulk electric asset in a substation, connected through a modem to my EMS communication front-end. What is the Electronic Security Perimeter in this case? There is no LAN in the substation.*

Answer: An Electronic Security Perimeter is required at the master station front-end. If the modem is not dial-up accessible and the RTU does not use a routable protocol then an Electronic Security Perimeter is not necessary.

RTUs that use a non-routable protocol with a master/slave synchronous polling method that cannot access anything on the EMS, and use SBO (select before operate) command to control devices at the RTU end, do not require an Electronic Security Perimeter.

If a dialup modem on a critical bulk electric asset is used for configuration or polling it must be in an Electronic Security Perimeter that is just around the dialup access point (e.g., SCADA-controlled, dial-back, or other technologies that give proper access controls and logging).

4. **Question:** *What is an access point to the Electronic Security Perimeter?*

Answer: An access point is any place where electronic traffic crosses the Electronic Security Perimeter. Examples include routers, firewalls, and dial-up, Radio Frequency (RF) and Infrared (IR) devices.

5. **Question:** *What are dial-up accessible access points?*

Answer: For the access point to be considered dial-up accessible, it must be reachable through the regular telephone network and excludes leased lines. Dial-up accessible access points are those that can be dialed up from the public switched telephone network (“POTS”) or other land-based dial-up such as ISDN. For a standalone Critical Cyber Asset with a single attached dial-up accessible device such as a modem or ISDN CSU/DSU, the Electronic Security Perimeter consists of that single device with the access point at the modem. The requirements apply to that single access point.

6. **Question:** *What is meant by discovery of access points?*

Answer: Discovery is a process by which Responsible Entities validate that they have properly identified all the access points to the Electronic Security Perimeter. The discovery process can be performed automatically (e.g. war-dialing), manually (e.g. physical inspection to detect dial-up modems and antennas present), or both.

7. **Question:** *Must I have a firewall to secure the Electronic Security Perimeter?*

Answer: A firewall is any device that provides access control between a more secure and a less secure zone and usually provides electronic logging. The standard does not specifically require the use of a firewall. However, it does require that all access points to the Electronic Security Perimeter be secured with adequate access control and monitoring measures. Any measure that meets the requirements of the standard is sufficient. A firewall device can satisfy many of the requirements in the standard including access control, electronic logging and alerting, and strong authentication.

8. **Question:** *What do the terms “organizational processes, and technical and procedural mechanisms for control of electronic access” and “strong procedural and technical controls” mean in CIP-005?*

Answer: In order to properly implement the standard, all the following elements of electronic access control must be considered:

- Organizational processes mean those parts of the controls that deal with the different interactions and relationships between organizational entities necessary for making the controls work.
- Technical mechanisms are those implemented through technology: equipment, software and systems.

- Procedural mechanisms are those manual processes and procedures that must be implemented for the electronic access controls to be effective. Procedural controls are often used to compensate for deficiencies in technical controls. For example, these may include procedures which require a phone call to a control center with appropriate authentication before access is granted, or additional manual logging.

Strong technical and procedural controls normally require use of at least two of the following three factors: (1) something the person knows, (2) something the person has, and (3) something the person is. “What a person knows” is typically a password, pass phrase or some personal identification number (PIN). “What a person has” is typically a physical device such as an electronic authentication token or smart card, and “what a person is” is usually some biometric characteristic such as a fingerprint or iris pattern.

The most common implementation today requires the knowledge of a PIN and some dynamic sequence of numbers or digital certificate stored on a physical device. Such mechanisms can also include:

- Out-of-band authentication procedures to augment static user identification and password access. (For example, access will not be enabled via static user identification and password authentication unless a telephone call is received from the party requesting access. On receipt of the telephone call and after successful procedural authentication of the calling party, an administrator will enable access allowing the party to use his or her static user identification and password).
- One-time use passwords.
- In dial-up access, automatic number identification (ANI) or caller identification to augment static user identification and password authentication.
- In dial-up access, call back to augment static user identification and password authentication.
- Where remote activation of dial-up connectivity via Supervisory Control and Data Acquisition system (SCADA)-activated relays from the security or control center is technically feasible, dial-up equipment can be physically deactivated when not in approved use and remotely activated upon approval of activation.

9. **Question:** *Am I required to implement an intrusion detection/prevention device?*

Answer: This standard does not specifically require installation of intrusion detection systems on your network or in the Cyber Assets. It does require that you have some intrusion detection processes that allow you to monitor accesses to or attempts to access your Electronic Security Perimeter and to be alerted so that you can respond. These do not have to be reported by a network or host intrusion device, but may be processes which you have implemented to review your access logs in a timely fashion or to automatically scan your logs for intrusions or attempted intrusions. However, network and host intrusion detection systems are specifically designed for this purpose and automatically provide these functions.

10. **Question:** *I have a dial-up access point where I cannot technically implement 24x7 monitoring, nor is full logging available. How can I satisfy Requirement R3 for monitoring?*

Answer: R3.1 does not require 24x7 monitoring or logging where it is not technically feasible. Refer to FAQ #1 under the General heading.

11. **Question:** *I have a Virtual Private Network (VPN) that allows some external computers to connect to a VPN server on my security perimeter. Have I extended my security perimeter?*

Answer: No. The VPN server is your access point into your perimeter and you must implement the appropriate control measures at the VPN server, such as restricting access ports and appropriate authentication measures, and at the remote end, such as virus monitoring.

12. **Question:** *What is an appropriate use banner?*

Answer: An appropriate use banner is a notification presented to the user when accessing a system.

There are usually at least two different banners used: one for access devices used at the edge of networks, when it is desirable to minimize the information about the systems, and one used in internal networks. The first is intended for authorized and unauthorized users. The second emphasizes corporate policy on appropriate use of technology systems.

A sample of a typical banner on an edge system follows:

This system is for the use of authorized users only. Individuals using this system are subject to having their activities monitored and recorded by authorized company personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, company personnel may provide the evidence of such monitoring to law enforcement officials.

A sample of a banner used on an internal system follows:

ABC Corporation, Inc.

This computer system is to be used only by authorized individuals. Anyone using this system expressly consents to having his/her activities monitored and recorded by authorized Company personnel. Any use of Company technology systems in conflict with Company policies, procedures, or values is prohibited and may lead to severe penalties. Use of this system for illegal purposes may also lead to civil or criminal liability. See Corporate Policy XXX-XX,YYY-Y, and Sect. N of the Corporate Code of Conduct.

13. **Question:** *Why must non-critical Cyber Assets within a defined Electronic Security Perimeter be subject to the requirements of CIP-005?*

Answer: The intent of the requirements of CIP-005 is to define an Electronic Security Perimeter around Critical Cyber Assets and to protect the Critical Cyber Assets by defining a set of requirements to control and monitor access through the perimeter at each access point. The standard defines a minimum set of requirements to adequately protect access through the perimeter to the Critical Cyber Assets inside them. If the same requirements are not applied *at these access points* for access to the non-critical Cyber Assets within the same Electronic Security Perimeter, then the level of protection for access through the perimeter at these access points is weakened. Non-critical Cyber Assets provide a jumping-off point for attack to any asset within the perimeter.

14. **Question:** *What does “review to verify” ports and services mean?*

Answer: A “review to verify” means that Responsible Entities must examine their systems to assure that only the ports and services required for operations are enabled. The review may be manual or automated. A manual review is typically conducted by looking at the running configuration of the controls at the access points and comparing it to the documented desired or designed configuration of the system. Scripts or tools such as port scanners can be used to automate the review. NOTE: extreme caution must be used when using automated scanning tools because there are cases where they have caused instabilities on the scanned targets. Responsible Entities should ensure that automated tools are adequately tested before deploying in a production environment.

Responsible Entities may also want to verify that the automated tools are providing accurate information by comparing the results to those obtained from a manual review.

15. **Question:** *Is a physically isolated and dedicated network required for connections between Electronic Security Perimeters?*

Answer: No, physical isolation is not required, nor is a dedicated link required. The standard does not specify any requirement for communication between discrete Electronic Security Perimeters, since this is currently beyond the scope of these standards. It is possible for the data between discrete perimeters to be carried over a shared infrastructure such as a shared WAN, or to be carried over dedicated links. However, the Responsible Entity must ensure that the access control devices (such as firewalls) at the access points to the Electronic Security Perimeters do not permit unauthorized access to the Electronic Security Perimeters and the Cyber Assets within them. When data is carried over a shared infrastructure, the Responsible Entity should ensure as well that the data has not been changed in transit. Logical or virtual separation of the data in a shared infrastructure can be accomplished by using existing technologies such as virtual circuits and communication tunnels. Encryption or other data integrity checking technologies can also ensure that data is not changed in

transit, provided performance and latency requirements for the applications are satisfied.

16. **Question:** *Where can I find additional information on network security and practices on securing a network perimeter?*

Answer: The National Institute of Standards and Technology (NIST) has some publications which deal with this issue. The following site provides a listing of NIST publications on computer security <http://csrc.nist.gov/publications> (SP-800 series).