NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Frequently Asked Questions (FAQs)
Cyber Security Standards CIP–002–1 through CIP–009–1

General CIP-002 through CIP-009

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

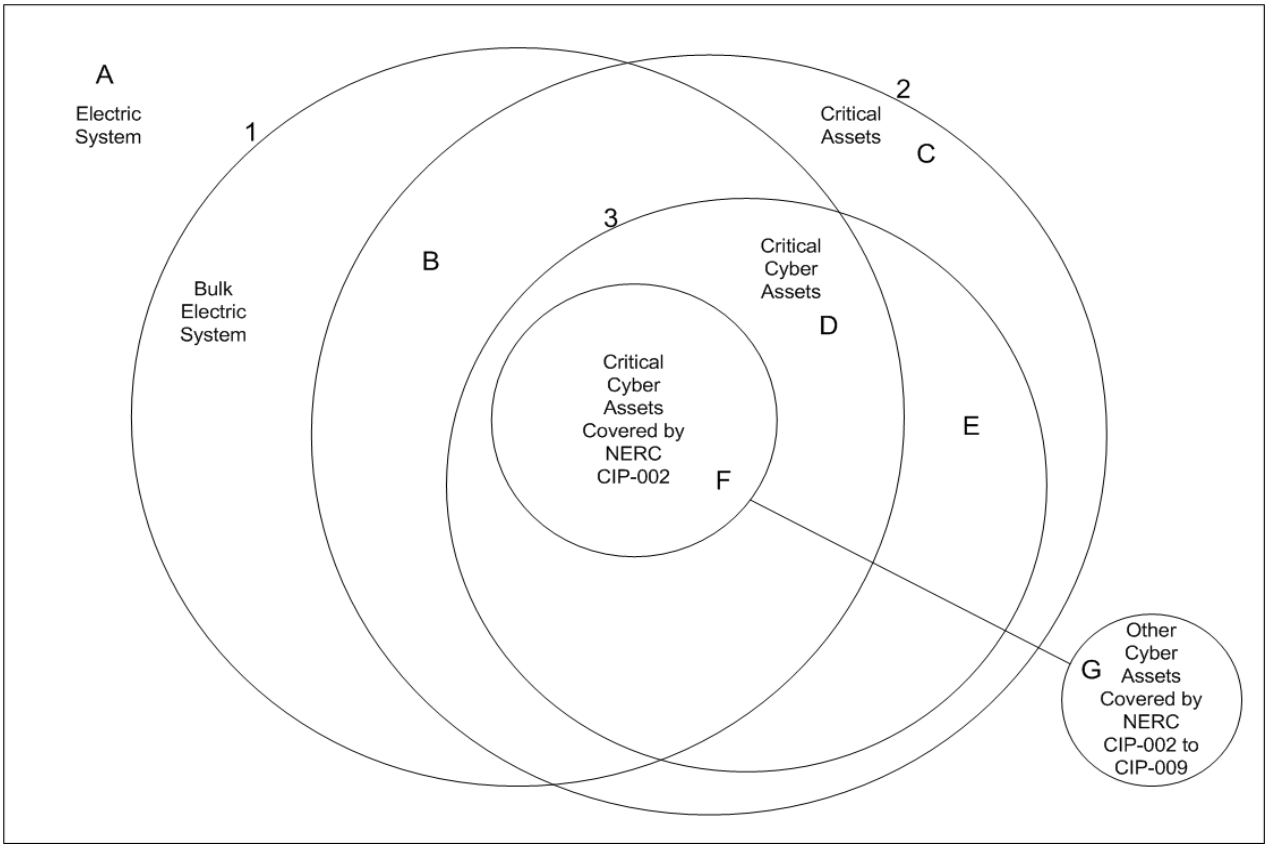
interpretations. One comprehensive source, that itself refers to a number of other authoritative sources (including statutory and regulatory definitions), is:

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

Standard CIP–002–1 — Cyber Security — Critical Cyber Assets

1. **Question:** *Can the overall relationship be shown between Critical Assets, Cyber Assets, and the Bulk Electric System?*

   Answer: The following Venn diagram and explanation shows the necessary relationships related to the NERC Cyber Security Standards (CIP–002 through CIP–009).



Explanation:

Area A — The entire Electric System including Transmission, Distribution, *Bulk Electric System*, Generation, and Market Systems.

Circle 1 — *Bulk Electric System,* as defined by NERC.

Circle 2 — *Critical Assets*, as identified by the Responsible Entity. Many *Critical Assets* are also part of the *Bulk Electric System* (Areas B, D, F), but not all (Areas C, E).

Circle 3 **—** *Critical Cyber Assets* supporting all the *Critical Assets* as identified by the Responsible Entity. Shown are *Critical Cyber Assets* supporting the *Bulk Electric System* (Areas D, F) and *Critical Cyber Assets* not supporting the *Bulk Electric System* (Area E).

Area F — Indicates *Critical Cyber Assets* that support the *Bulk Electric System* within the scope of the NERC Cyber Security Standards.

Area G — *Cyber Assets* covered by the NERC Cyber Security Standard CIP–007 because of their network connectivity with *Critical Cyber Assets* that support the *Bulk Electric System.*

2. **Question:** *Why aren't all Cyber Assets associated with the Bulk Electric System required to be secured and protected under the Cyber Security Standards?*

   Answer: The implementation of the Cyber Security Standard is limited, allowing for a more reasonable implementation timeline, by focusing on Critical Assets, as identified in CIP–002, that are essential to the operation of the bulk electric system and Critical Cyber Assets that use routable protocols or are dial-up accessible. The Critical Cyber Assets that use non-routable protocols have a limited attack scope; hence, they are less vulnerable than Critical Cyber Assets using routable protocols.

   To identify Critical Assets and Critical Cyber Assets, the Responsible Entity should consider using a cross-functional team and other methods that are appropriate for its organization.

3. **Question:** *Which Blackstart units have to comply with the CIP Standards?*

   Answer: NERC is only concerned about blackstart units that are designated for use in system restoration plans. While many units may be able to blackstart, the CIP standards only apply to blackstart units identified under EOP-007-0: *Establish, Maintain, and Document a Regional Blackstart Capability Plan*. These generators are sometimes referred to as "critical blackstart units."

4. **Question:** *Why are the Critical Asset criteria for automatic load shedding under control of a common system set at 300 MW?*

   Answer: The DOE EIA-417 report form required filing a report after an "uncontrolled loss of 300 MW or more of firm system loads for more than 15 minutes from a single incident."

5. **Question:** *Does redundancy of a Critical Asset or a Critical Cyber Asset change the criticality of these assets?*

   Answer: No, in NERC's Cyber Security Standards, redundancy does not affect the criticality of any asset. Redundancy will only affect availability and reliability while not improving integrity or information confidentiality and may in fact increase the Cyber Asset's exposure to a cyber attack. For the purpose of security, each Critical Cyber Asset and redundant Critical Cyber Asset must be protected under the Cyber Security Standards as Critical Cyber Assets.

6. **Question:** *In the Cyber Security Standard CIP-002, what is considered a routable protocol?*

   Answer: In this standard, routable protocols are those that provide switching and routing as described by the Open System Interconnection (OSI) model Layer 3 or higher.

   The OSI is a standard description or "reference model" that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the

application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. The OSI model is valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

Layer 3 provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control, and packet sequencing. The most common layer 3 protocol is IP, and it is usually associated with TCP/IP.

Frame relay is a Layer 2 protocol, and is, therefore, not a routing protocol. Routable protocols such as IP may use frame relay.

Some commonly used protocols, such as Profibus, DNP, Modbus, and Fieldbus do not make use of an OSI Layer 3; rather, they interface the OSI Application layer (Layer 7) directly to the OSI Data Link layer (Layer 2). Because these protocols do not make use of an explicit Layer 3 protocol, they are not considered "routable" for purposes of this standard. (However, if they are run over IP, such as DNP over IP or Modbus over IP, they are routable per this standard.)

The OSI model guides product implementers so that their products will work consistently with other products. Although OSI is not always adhered to strictly in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe them in relation to the OSI model.

For details regarding telecommunications and networking protocols, see http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci523729,00.html, http://www.linuxports.com/howto/intro_to_networking/book1.htm, and http://images.techiehq.net/faqs/osi.gif.

7. **Question:** *What is dial-up accessible access under CIP–002?*

   Answer: Dial-up accessible access in CIP–002 refers to any temporary (non-permanent), interruptible, or not continuously connected communication access to a Critical Cyber Asset from any remote site. Using a modem over a land line, wireless technology, or VPN using a routable protocol to connect to a Critical Cyber Asset from one or more locations or by one or more users are examples of dial-up accessible access. Access to a Critical Cyber Asset via a permanent communication connection from a specific computer over a dedicated communication circuit would not be considered dial-up accessible access.

8. **Question:** *If a dial-up connection exists on a Critical Cyber Asset that does not use a routable protocol, can the dial-up access be secured without a Physical Security Perimeter?*

   Answer: Critical Cyber Assets with dial-up access not using a routable protocol must meet the Electronic Security Perimeter requirements for the remote access to that device but does not require a Physical Security Perimeter or local Electronic Security Perimeter for the actual Critical Cyber Asset. Secure remote access meets the intent of the Cyber Security Standards to provide a minimum level of security. Please refer to CIP-006.

9. **Question:** *Are Cyber Assets for a control center or generation control center with monitoring only and no direct remote control required to be protected and secured under the Cyber Security Standards?*

   Answer: Cyber Assets within an Electronic Security Perimeter at a control center or generation control center that provides critical operating functions and tasks as identified in CIP–002 must be protected per the requirements of the Cyber Security Standard. The monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction.

   An example of monitoring without direct control that is subject to the Cyber Security Standards is a Reliability Authority that receives data from Critical Cyber Assets to a state estimator.

10. **Question:** *What are the requirements for protecting and securing jointly owned Critical Cyber Assets under the Cyber Security Standards?*

    Answer: All Responsible Entities having such joint assets are expected to ensure compliance with the Cyber Security Standards. Responsibility for carrying out the actions necessary to comply with the standards can be determined by specific agreements and contracts between the parties. In cases where assets are operated by a non-owner, responsibility for carrying out the actions necessary to comply with the standards also can be determined by specific agreements and contracts between the parties.

11. **Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the Cyber Security Standards?*

    Answer: Communications is not covered under this standard because communications are often leased by the Responsible Entities and the technologies for existing Cyber Assets do not always support encryption or other possible security alternatives. Asset owners are encouraged, whenever possible, to provide communications or communication systems with the same protection as their associated Critical Cyber Asset.

12. **Question:** *Are environmental or support systems, such as HVAC or UPS, for Critical Cyber Assets required to be protected in a manner similar to their associated Critical Cyber Asset?*

    Answer: Environmental or support systems for Critical Cyber Assets do not require the same protection as the associated Critical Cyber Asset because compliance to all sections of the Cyber Security Standard would affect only availability and reliability while not improving the integrity or information confidentiality of the Critical Cyber Asset. Asset owners are encouraged, whenever possible, to provide environmental or support systems with the same protection as their associated Critical Cyber Asset. Similar protections should be given to voice systems and PBX systems as

appropriate. If the support systems are network-connected to the Critical Cyber Assets, they must be afforded the same protection given Critical Cyber Assets as required in other Cyber Security Standards.

13. **Question:** *Are alarm systems or alarm control centers that support Critical Assets, which do not themselves directly provide any operating functions or tasks alarming, required to be protected as a Critical Cyber Asset*?

    Answer: Alarm systems or alarm control centers for Critical Assets do not require protection as a Critical Cyber Asset unless they also provide critical operating functions or tasks under Cyber Security Standard CIP-002, or unless they are identified in other Cyber Security Standards as requiring the same protection given Critical Cyber Assets. Examples of alarm systems not requiring protection as a Critical Cyber Asset would be providing for functions such as environmental or support systems, or communication alarming. Asset owners are encouraged, whenever possible, to provide alarm systems or alarm control centers with the same level of protection as other Critical Cyber Assets.

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.

Standard CIP–004–1 — Cyber Security — Personnel & Training

1. **Question:** *What is meant by "authorized cyber access?"*

   Answer: The phrase "authorized cyber access" is similar in intent to "authorized unescorted physical access" (see Standard CIP-006, Requirement R1.6). In other words, the phrase refers to permitting ("authorizing") someone to have "trusted," unsupervised access in a cyber environment. Other than in emergency situations, some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training. Procedures covering cyber access under emergency circumstances must be covered in the Responsible Entity's cyber security policy as required by Standard CIP-003.

2. **Question:** *Are any employees, contractors, or service providers going to be "grandfathered" under the personnel risk assessment requirement in this standard?*

   Answer: Employees, contractors, or service providers who have had a personnel risk assessment within the previous 7 years from the implementation date of the Standard do not need to be reassessed until 7 years after the date of their last assessment. All others will have to have either an updated assessment or initial assessment conducted as required by the standard.

3. **Question:** *What are the Personnel Risk Assessment requirements for this standard?*

   Answer: The assessment should be conducted in accordance with all applicable laws and agreements, and leaves the specific components of the assessment process to those entities subject to the Standard. As a minimum, identity verification and a seven-year criminal check are required. However, it is recommended that additional checks such as employment history, education verification, professional certifications, etc., be reviewed where warranted and where applicable to the position. Further guidance on the administration of personnel risk assessment programs can be found in reference documents such as "LPA Background Check Protocol" published by the Labor Policy Association (ISBN 0-9667568-8-6), and the Fair Credit Reporting Act, where applicable.

4. **Question:** *What sort of "awareness" program is required and what sort of proof will we have to provide that it's been conducted?*

   Answer: An awareness program is intended to reinforce sound security practices, but is expected to be less detailed or rigorous than a training program. The content of an awareness program is left to the discretion of each Responsible Entity and can take the form of memos, e-mail, computer based training, posters, meetings, etc. The proof of reinforcement can be copies of posters, e-mails or notices, etc., or meeting logs, etc.

5. **Question:** *Who is responsible for conducting the personnel risk assessments of contractors and service vendors?*

   Answer: The Responsible Entity is accountable for ensuring that personnel risk assessments are

conducted per this standard for contractors and service vendors. Whether that is done through an audit process to ensure that it is being properly conducted, or by directly administering the process, or by some other method, the Responsible Entity must confirm that a program exists and meets the requirements of this standard.

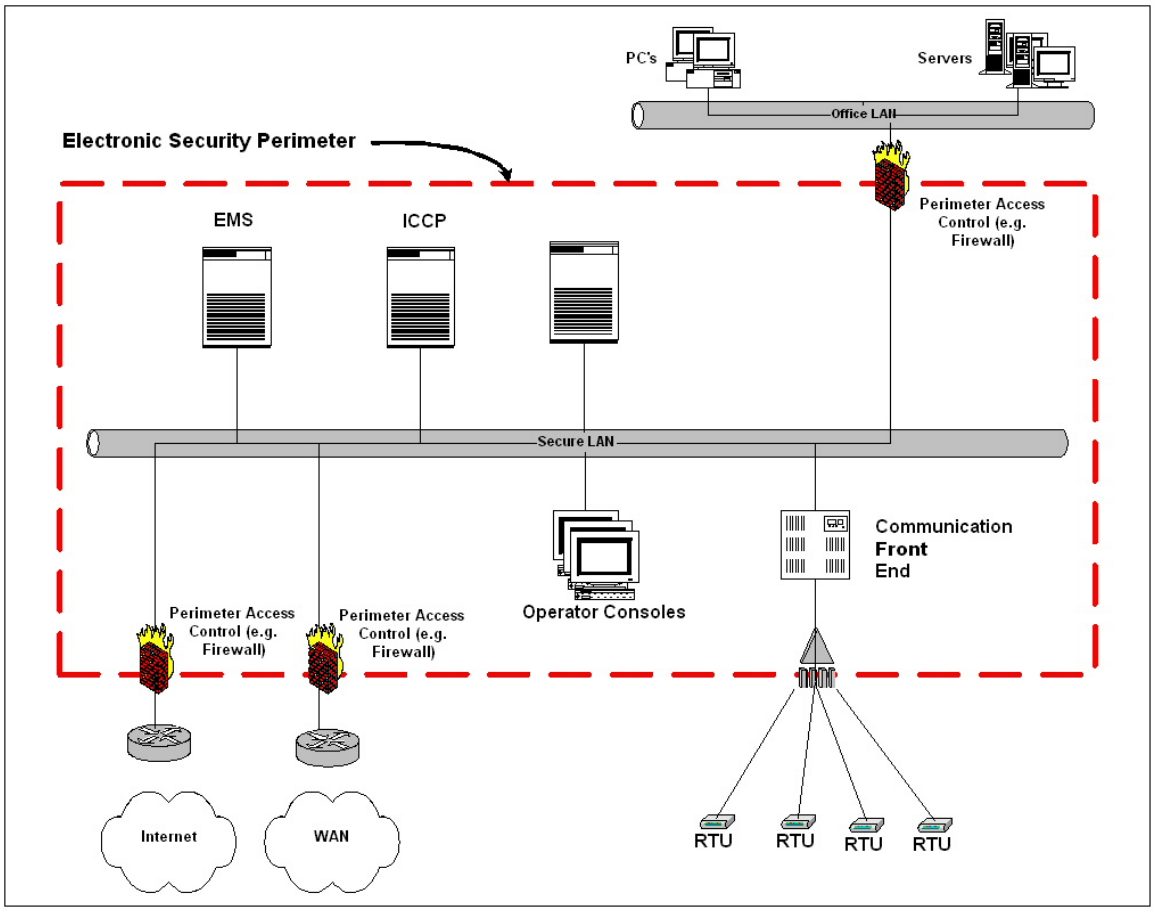
6. **Question:** *What if our existing labor agreement does not address or allow personnel risk assessments of bargaining unit employees? How can we meet the standard?*

   Answer: Standard CIP–004 acknowledges limitations in labor agreements by indicating that application of the risk assessment section is subject to "existing collective bargaining unit agreements." In those cases where a Responsible Entity cannot implement a program due to a labor agreement, it can write an exception to its cyber security policies. However, the Responsible Entity is expected to address the assessment issue as a bargaining item in their next contract negotiation.

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.



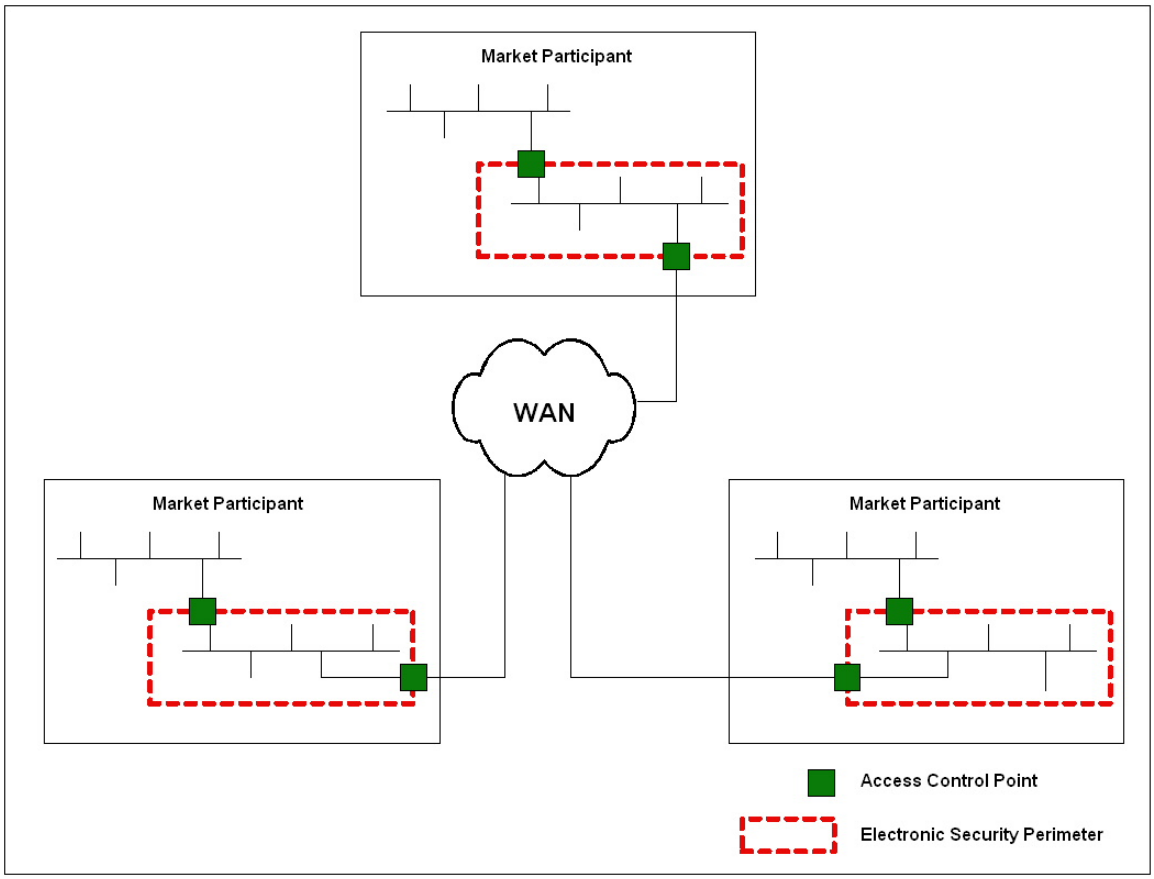
   The RTUs may need an Electronic Security Perimeter if they use a routable protocol and meet the definition of a Critical Cyber Asset. Also a single computer may need an Electronic Security Perimeter if it meets the definition of a Critical Cyber Asset.

   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).

Standard CIP–006–1 — Cyber Security — Physical Security

1. **Question**: *What is a "six-wall" border?*

   Answer: This refers to a physical, completely enclosed border, such as a room, cage, safe, or metal cabinet. Raised floors and drop ceilings may not constitute part of a border because they could create potentially uncontrolled access points. Fences do not constitute a completely enclosed border. The intent is to clearly define a security boundary that applies the same level of security over its entire area.

2. **Question:** *How does the Physical Security Perimeter relate to the Electronic Security Perimeter?*

   Answer: The requirement in CIP-006 mandates that all Cyber Assets required to be protected or access points to the Electronic Security Perimeter reside within a Physical Security Perimeter.

3. **Question**: *What are access points to a Physical Security Perimeter?*

   Answer: The access points are any places a person may pass through the perimeter; e.g. door, window, or portal.

4. **Question:** *If a remote device accesses a Critical Cyber Asset through a controlled electronic access point, does the Physical Security Perimeter need to be expanded to include that remote device?*

   Answer: No. If the electronic access point meets the electronic security requirements of CIP 002–009, then the remote device does not need to reside within the Physical Security Perimeter.

5. **Question**: *Our backup EMS system resides in a shared facility. We have implemented a caged enclosure to control access to our equipment. Does this suffice?*

   Answer: Yes, a security cage meets the requirements for a Physical Security Perimeter as long as all equipment resides within the cage or other completely enclosed ("six-wall") border, and the cage provides a door with a lock to control access. Note that you must also meet the access control, monitoring, and logging requirements of the standard.

6. **Question**: *Can a Responsible Entity identify zones or levels of access to various Critical Cyber Assets based upon pre-defined levels of criticality?*

   Answer: The standard requires that all Critical Cyber Assets meet the physical security requirements of the standard. A Responsible Entity may go beyond the required minimum and establish higher levels of security as it deems necessary.

7. **Question**: *Does a Responsible Entity's design of physical access controls and monitoring require the prevention of tailgating?*

Answer: It is very difficult to prevent tailgating in most unmanned physical security implementations. To address this issue, the Responsible Entity should consider covering tailgating in the physical security policies and procedures, and communicating these policies in its annual security awareness program.

8. **Question**: *What constitutes compliance for monitoring physical access 24 hours a day, 7 days a week?*

   Answer: The use of an electronic access system (cardkey, keypad, biometric, etc.) that supports logging is an acceptable method of monitoring. Similarly, an access point manned by a 24x7 security guard, or monitored from a manned central monitoring station would suffice. Additionally, the recording of video sufficiently meets the intent of the standard; "Real Time" human monitoring is not a requirement, but serves as an option to meeting the requirement.

9. **Question**: *Our company uses both video recording and electronic cardkey logs to log physical access through the physical perimeter. Do we need to keep both logs for 90 days?*

   Answer: Yes, if both are designated as logging methods in the physical security plan. Please note, in the event that a security incident involving physical access is detected within the 90-day period, the specific logs related to that incident must be retained for three years.

10. **Question**: *If the only method used for logging physical access is video, wouldn't it be difficult to meet the 90-day retention with digital video systems because of storage costs?*

    Answer: While this may be true, it is possible to maintain these records. One method that would be acceptable would be to use motion or sound detection devices to limit the amount of dead time recording.

11. **Question**: *Does CIP-006 intend that access points with physical access controls (e.g.: card key control) also need "CCTV" or "Alarm Systems"?*

    Answer: Modern physical access control systems usually provide alarm monitoring and would, therefore, qualify as monitoring systems. No separate systems are required unless the criticality of the access point dictates it.

12. **Question**: *What is a monitoring station?*

    Answer: A monitoring station or stations can be a commercial service, a security central station, or an operations dispatch desk. The main criterion is human monitoring, 24 hours per day.

13. **Question**: *In the case of a room containing Critical Cyber Asset(s) that is staffed at all times, escorted personnel who enter these rooms would be exempt from a Responsible Entity's cyber*

security policy requirements for personnel risk assessment, training, and physical access logging. Is this a correct interpretation?

Answer: Yes, except that logging still applies. People who are escorted "at all times" are exempt from all but logging physical access.

14. **Question**: *Requirement R1 appears to assume there is one central security plan for the whole company vs. a security program. If this standard requires a CIP 002-009 security plan, then that is what it should say. Otherwise, it should just state, "the company shall have a documented implementation plan approved by the senior manager responsible for the implementation of NERC CIP 002–009."*

    Answer: A separate CIP 002–009 security plan is not contemplated in this standard. Rather, any existing security plans or programs should align with the CIP 002–009 standards. If no security plans or programs exist, the Responsible Entity must create one in accordance with the provisions of CIP-002–009.

15. **Question**: *Are Critical Cyber Assets that do not use routable networking protocols and are controllable through dial-up facilities covered by CIP-006?*

    Answer: No. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity is not required to comply with Standard CIP-006 for that single access point at the dial-up device.

16. **Question**: *What is a restricted key-way or key system?*

    Answer: A restricted key-way or key system is a set of controls to manage a key system; i.e. signature accountability, receipts maintenance, periodic inventories, securing unused keys by using a locked security container, stamping "Do Not Duplicate" marking, are often numbered, etc.

17. **Question**: *Is an entity required to implement a card key system, special locks, or use security personnel to meet the provisions of R2?*

    Answer: Yes. The standard permits flexibility, and an entity may choose to implement or apply another device. However, any alternative devices must be equivalent to those proposed in the standard and defined in the Responsible Entity's physical security plan.

18. **Question**: *R1.7 requires entities to update their "physical security plan" within 90 days of any physical security system redesign or reconfiguration. Is this a "hard and fast" requirement?*

    Answer: Yes, when a physical security system redesign or reconfiguration is made the plan must be updated. Examples include adding video recording, applying card access to additional doors, removing a security officer and replacing that individual with an applied technology, or a major change in operating procedures for the location. Redesign or reconfiguration can also be changes to

procedures including modifying escort or locking procedures. Replacing "in kind" does not require a change in the physical security plan.

19. **Question**: *We have determined that using a human to manually log access at a remote site containing Critical Cyber Assets is not cost effective and we are considering just having a log placed at the location for personnel to use on an honor system. Does this meet the intent of R4.3?*

    Answer: A manual log is effective in locations that are staffed 24x7 such as system control centers or generating stations; however, manual logs alone may not be effective at remote, unmanned substations containing Critical Cyber Assets**.** The Responsible Entity must ensure that the requirements of R2 and R3 are met when determining the logging procedure to use.

20. **Question**: *Does the standard require entities to protect telecommunications services and facilities that serve physical security system assets?*

    Answer: CIP-002 through CIP-009 do not address telecommunications.

21. **Question**: *To what extent is system maintenance and functional testing required?*

    Answer: The extent of functional testing is typically recommended by manufacturers.

22. **Question**: *What type of testing and maintenance schedule is required by CIP-006?*

    Answer: Entities may set their own schedules as long as all physical security systems are tested and maintained within a 3-year period.

23. **Question:** *Please explain the percentages in the Levels of Noncompliance pertaining to controlling, monitoring, and logging Physical Security Perimeters.*

    Answer: The percentages were added in the Levels of Noncompliance to acknowledge concerns of Responsible Entities who may have a large number of Physical Security Perimeters.

    This part of CIP-006 assumes that the Responsible Entity has multiple security perimeters. The percentage refers to the number of uncontrolled, unmonitored, or non-logged Physical Security Perimeters divided by the total number of Physical Security Perimeters. It does not refer to some percentage of any single Physical Security Perimeter that may be uncontrolled, unmonitored, or not logged. If any portion of a Physical Security Perimeter is uncontrolled, unmonitored, or not logged, then all the Cyber Assets within that Physical Security Perimeter are considered unprotected.

    An example may help explain this better. An entity is responsible for four Physical Security Perimeters. If one of those Physical Security Perimeters is uncontrolled, unmonitored, or not logged, then the applicable percentage is 25% and the Responsible Entity is Level Two noncompliant. If the Responsible Entity has only one Physical Security Perimeter and, for example, one door is not

controlled, then 100% of that Responsible Entity's Physical Security Perimeters are inadequate and that Responsible Entity is Level Four noncompliant.

Standard CIP-007–1 — Cyber Security — Systems Security Management

1. **Question:** *Why are non-critical Cyber Assets subject to the requirements of this standard?*

   Answer: Non-critical Cyber Assets within the Electronic Security Perimeter are subject to the requirements of CIP-007 because if not protected, they can provide an open door into your network and Critical Cyber Assets. Non-critical Cyber Assets that are within the Physical Security Perimeter but not within the Electronic Security Perimeter are not subject to the requirements of CIP-007.

2. **Question:** *Is an isolated test environment required?*

   Answer: Electronic isolation is not required; the test environment is not required to be outside the Electronic Security Perimeter. A controlled non-production system can be used. The standard requires that the test environment not introduce additional risk to production operations.

3. **Question:** *Can a redundant system be used for testing?*

   Answer: The Responsible Entity must determine the non-production systems in its environment. It is possible, depending on the Responsible Entity's environment, that a redundant system can be used for testing if it can be configured such that it does not introduce additional risk to production operations.

4. **Question:** *What are some sample security test procedures?*

   Answer:

   - Basic "port scans" to identify open/available services,
   - File integrity checking to identify change in size of certain files,
   - Review of active user accounts subsequent to changes to the system,
   - Validate security-related functions: access controls, audit functions, file protection,
   - Test for malicious logic in source code,
   - Review technical documentation to determine security features, and
   - Review source code if available for application security.

5. **Question:** *To what extent is testing an application that requires real-time data inputs allowed?*

   Answer: Testing should not compromise or put a production system at risk of failure or compromise. The more the test simulates real life operation the better.

6. **Question:** *If testing yields a failure of a "Critical Cyber Asset" is that a reportable Cyber Security Incident?*

Answer: No, even if it impacts the production environment.

7. **Question:** *To what extent are common system administration modifications (changes) considered applicable to this standard. i.e., what constitutes a "significant change?*"

   Answer: The phrase "significant change" is subject to interpretation by the Responsible Entity using reasonable business judgment, but clearly includes any change that might introduce vulnerabilities into the production environment.

8. **Question:** *What is an appropriate process for managing individual user, administrator, shared, and other generic accounts*?

   Answer: Documentation of accounts should identify all personnel having access permission to use them and policies should provide clear guidance concerning acceptable use. Logging procedures must be established that create audit trails of all commands issued from an administrative account, including failed privileged command execution.

   Where possible, system administrators should log in using individually assigned accounts and switch user to obtain administrator privileges so that accountability is maintained. Direct logins as root/administrator should be limited and should provide a mechanism even if manual to track usage.

   Concerning generic or shared account usage auditing: Where a generic or shared account must be used, a named individual must be identified as being responsible for ensuring appropriate use, tracking who has access to the account at all times, and changing the password when someone leaves the group.

   On frequency of password changes: Generally, the more powerful the account privileges the more frequently the account password should be changed. For guidance on hardening passwords, refer to DOE or NIST SP–800 Series Standards.

9. **Question:** *Are all patches required to be installed?*

   Answer: The standard addresses only security patches and requires that a process must be in place to manage the implementation of those patches. It is acceptable to make a conscious decision not to implement a security patch, as long as you document your reasons and compensating measures. The process should include investigation, testing, implementation, back-out plans, and appropriate decisions made throughout the process. This process can be a component of the documented configuration management process described in CIP-003 Requirement R6.

10. **Question:** *What if an application vendor recommends that you do not apply a certain security patch?*

    Answer: The Responsible Entity should work with the application vendor to determine when the patch should be applied. Compensating measures or acceptance of risk should be documented.

11. **Question:** *What is "malware?"*

    Answer: Malware generally means malicious software such as viruses, worms, time-bombs, and Trojan horses. This software may be distributed through email attachments, unsecured remote procedure calls, Internet downloads, and opening infected files. Malware may delete or modify files, attempt to crack passwords, capture keystrokes, present unwanted pop-ups on screen, fill-up disc space, or other malicious and destructive activity, without the authorization or knowledge of the person using the infected computer.

12. **Question:** *What is the concept of "need to know" with respect to work functions performed?*

    Answer: The authorized requirement of a person to know, access, or possess information that is necessary for the performance of an authorized, assigned job responsibility.

13. **Question:** *What is the difference between the ports and services requirement in CIP-005 and the one in CIP-007?*

    Answer: The requirement in CIP-005 is for Critical Cyber Assets on the Electronic Security Perimeter. CIP-007 refers to Cyber Assets within the Electronic Security Perimeter.

14. **Question:** *Is a live port scan required as part of the cyber vulnerability assessment?*

    Answer: CIP-007 does not require a live scan of the ports inside the perimeter. The requirement is to perform a review of the ports on an annual basis to verify that only those ports required for production operation are open. The review can be performed in any manner determined by the Responsible Entity.

15. **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 and verification 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. An automated review may automate the comparison using scripts or such automated tools as port scanners. 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 should ensure that automated tools are adequately tested.

16. **Question:** *What is meant by compensating measures for ports and services that cannot be shutdown?*

    Answer: A system's services typically use ports to communicate externally. Computer ports are

essentially doorways through which information comes into and goes out. You should disable all services and ports that are not required. In the event you are unable to disable unused ports and services, compensating measures should be applied. Examples of compensating measures are the use of firewalls, routers, and monitoring software to protect communications to and from those Critical Cyber Assets. Firewalls and routers can be configured to allow or disallow communications to specific ports. Monitoring software can be deployed to monitor not only communications to and from those Critical Cyber Assets but also monitor specific services. Furthermore, a host-based firewall can be used to control communications to or from a particular asset.

Standard CIP-008-1 — Incident Reporting and Response Planning

1. **Question:** *The standard does not provide procedures to characterize and classify incidents or events as reportable. Is guidance available?*

   Answer: Yes. NERC's Indications, Analysis and Warning (IAW) Standard Operating Procedure (SOP) defines criteria and thresholds for event reporting purposes. The Department of Energy's 417 report can be referenced as well. State, provincial, and regional entities may also provide guidance.

   Recall, CIP-008 only applies to cyber incidents and those physical incidents that are directly related to Critical Cyber Assets.

2. **Question:** *How is the information submitted by a Responsible Entity to the ES ISAC protected from disclosure?*

   Answer: NERC manages the ES ISAC. NERC employees are held accountable to a Code of Conduct that requires them to maintain the confidentiality of (1) any confidential or proprietary NERC information disclosed or available to the employee; (2) any confidential or proprietary information of NERC members, members of NERC members, or market participants to which the employee has access by virtue of his or her position with NERC; and (3) any confidential or proprietary information of others that has been provided to NERC on condition of confidentiality.

   Furthermore, if the ES ISAC receives information from a Responsible Entity that warrants an industry-wide warning, sensitive information provided by the Responsible Entity will be anonymized before being disseminated.

   NERC will consider the use of non-disclosure agreements in future revisions of the IAW Program.

3. **Question:** *What references are available to assist in developing an incident response plan?*

   Answer:

   a. Indications, Analysis, & Warning Program (IAW) Standard Operating Procedure (SOP): http://www.esisac.com/IAW.htm

   b. National Institute of Standard and Technology Special Publication 800-61, Computer Security Incident Handling Guideline: http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

   c. In addition, there are many publications available from sites such as SANS and CERT that can provide additional material.

4. **Question:** *Is the Responsible Entity accountable for reporting to the ES ISAC when an intermediary is involved?*

   Answer: Yes. The Responsible Entity can submit the cyber security incident through an intermediary such as a RTO/ISO, but the Responsible Entity must establish procedures with the intermediary to ensure that the ES ISAC receives the report.

Regardless of whether an intermediary is used to submit a report, the Responsible Entity is accountable for meeting the data retention requirements.

5. **Question:** *Please describe the relationship between CIP-008 and CIP-001.*

   Answer: The scope of CIP-008, Cyber Security — Incident Reporting and Response Planning, applies to Critical Cyber Assets only. CIP-001, Sabotage Reporting, applies to a broader scope of critical infrastructure but a narrower group of applicable entities.

6. **Question:** *The term "suspicious event" is too broad. Why is this term included?*

   Answer: CIP-008 requires the Responsible Entity to define procedures to characterize and classify events as Cyber Security Incidents. A suspicious event by itself may not result in a Cyber Security Incident, but excluding suspicious events from consideration may lead to overlooking malicious activity. For example, a single failed login attempt on a single system may not be considered suspicious, but multiple failed logins across multiple accounts or systems could be an indication of malicious activity. The Responsible Entity must consider suspicious events when creating its incident classification procedure.

   The requirements of this standard are not intended to apply to security events that have not been characterized as Cyber Security Incidents. For example, an IDS system may identify events such as port scans; the Responsible Entity should then apply its categorization and classification procedures to determine if these events are Cyber Security Incidents that should be responded to and reported on. For those events that are not determined to be Cyber Security Incidents, the standard does not require any further action.

7. **Question:** *As a Canadian entity, does the information reported to the ES ISAC go to a Canadian agency as well?*

   Answer: Critical Infrastructure Protection Information System messages posted using the IAW form will be sent to both the Department of Homeland Security and Public and Safety Emergency Preparedness Canada.

Standard CIP–009–1 — Cyber Security — Recovery Planning

1. **Question:** *Must we have a documented recovery plan for Critical Cyber Assets in every substation?*

   Answer: No. The short-term recovery plan for Critical Cyber Assets in a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency and remedial action, and outage scheduling. One recovery plan for Critical Cyber Assets should suffice for several similar facilities such as substations or power plant control centers.

2. **Question:** *How often and to what level do we need to drill our recovery plans?*

   Answer: Depending on the risk of loss associated with a particular asset, a "table top" drill that is performed once a year may be sufficient. If the consequences of losing a particular asset are extreme, a monthly drill that lasts an entire operations shift may not be excessive. Each Responsible Entity should perform a risk assessment of its Critical Assets and develop Recovery Plans and exercise those plans to a degree consistent with the consequences of loss. The minimum Recovery Plan testing period is one year.

3. **Question:** *What level of security would I need for my backup location or system?*

   Answer: The recovery site and/or system must adhere to the Cyber Security Standard, as it will require access to the same Critical Cyber Assets as the primary system.

4. **Question:** *How complex should the drills be?*

   Answer: The drills have to effectively exercise all the major elements of the Recovery Plan. The Recovery Plan exercise should test, at a minimum, roles and responsibilities. Document lessons learned and integrate and communicate any updates to the plan.

   The periodicity of drills should be consistent with the duration, severity, and probability associated with each type of event. For example, a higher probability event with a short duration may not require a Recovery Plan drill at all since the Responsible Entity exercises its response regularly. However, the Recovery Plan for a lower probability event with severe consequences must have a drill associated with it that is conducted, at minimum, annually.

5. Question: *Do we have to drill recovery plans for all Critical Cyber Assets?*

   Answer: No, not every Critical Cyber Asset requires a recovery plan drill. Facilities and infrastructure that are numerous and distributed, such as substations, may not require an individual recovery plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area that requires a redundant or backup facility. Because of these differences, the recovery plans associated with control centers will differ a great deal from those associated with

power plants and substations. There is no requirement for recovery plans for substations and generation plants that have no Critical Cyber Assets.