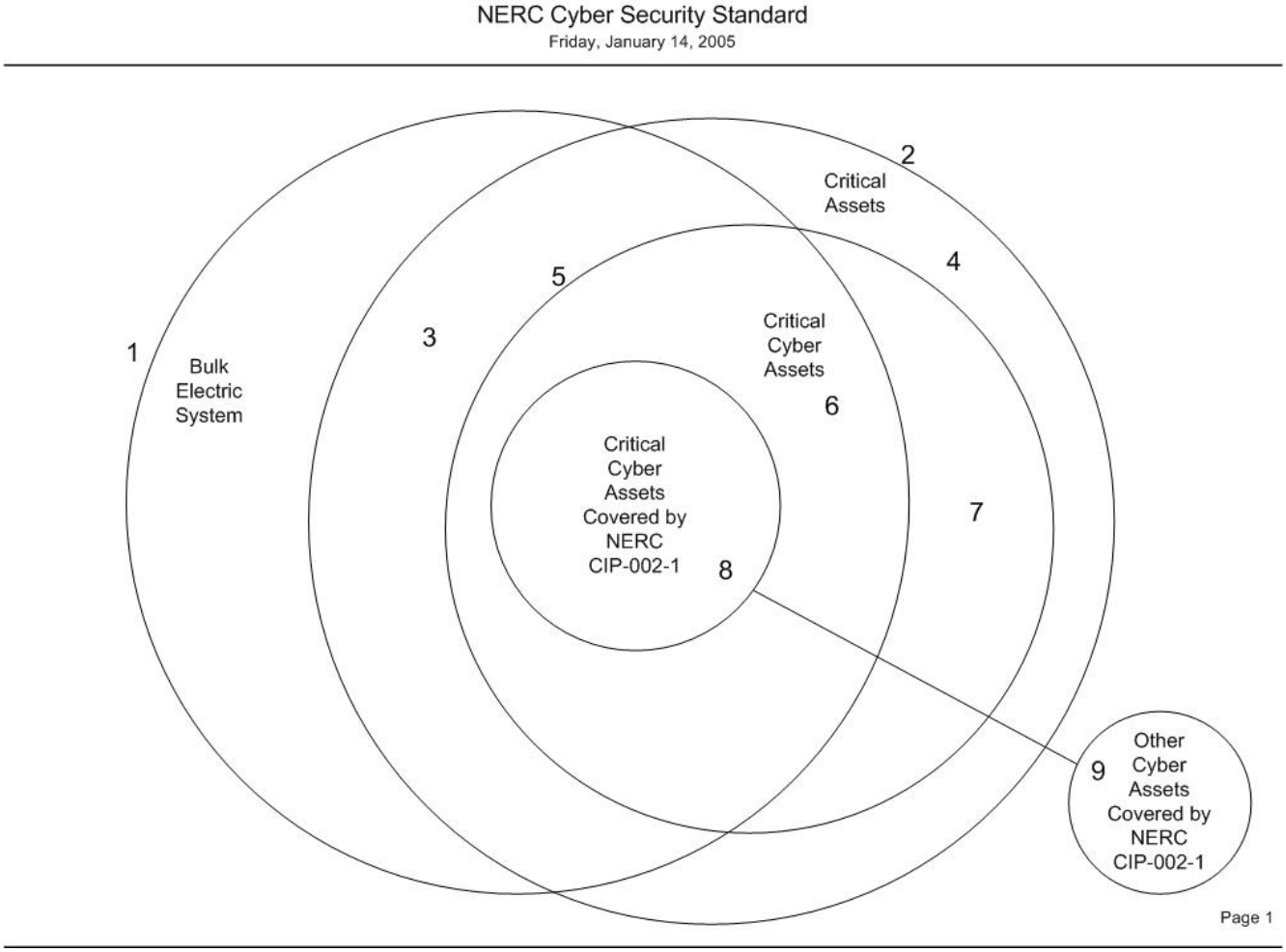
Frequently Asked Questions (FAQ's)
for
Cyber Security Standards CIP–002–1 thru CIP–009–1

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

1. **Question:** *Can the overall relationship between critical assets, Cyber Assets and the bulk electric system be shown visually?*

   Answer: The following Venn diagram and explanation shows the necessary relationships related to the NERC cyber security standards (CIP–002–1 through CIP–009–1).



Critical Cyber Asset Drawing Explanation

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* (Area 3), but not all (Area 4).

Circle 5 **—** *Critical Cyber Assets* supporting all the *Critical Assets* as identified by the Responsible Entity. Shown are *Critical Cyber Assets* supporting the *Bulk Electric System* (Area 6) and *Critical Cyber Assets* not supporting the *Bulk Electric System* (Area 7).

Area 8 — Indicates *Critical Cyber Assets* which support the *Bulk Electric System* within the scope of the NERC cyber security standard.

Area 9 — *Cyber Assets* covered by the NERC cyber security standard CIP–002–1 Requirement R3 ONLY because of their network connectivity with *Critical Cyber Assets* which 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 standard?*

   Answer: The implementation of the cyber security standard is limited, allowing for a more reasonable implementation timeline, by focusing on critical assets and Critical Cyber Assets that use routable protocols. The critical assets, as identified in CIP–002–1, are important to the operation of the interconnected bulk electric system. The Critical Cyber Assets using non-routable protocols have a very limited attack scope; hence they are less vulnerable than Critical Cyber Assets using routable protocols. Critical Cyber Assets using routable protocols within, and not leaving, the Electronic Security Perimeter still require protection under the cyber security standard as part of the intended current implementation of the cyber security standard.

3. **Question:** *Why is the term generation used instead of generator to determine critical bulk electric system assets?*

   Answer: Cyber Assets providing generator monitoring, control, or protection could be a common mode of failure for multiple units. Any such cyber asset must be considered a Critical Cyber Asset if the total potential generation affected is equal to or greater than the generation limit in the cyber security standards.

4. **Question:** *What is an IROL?*

   Answer: Interconnection Reliability Operating Limit (IROL) is a system-operating limit, which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk electric system. *(See NERC under-development standard 200 and standard 600; IROL was not used in previous NERC policies or standards.)*

   Related definitions from standard 200 are as follows:
   Bulk Electric System: A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 35 kV or as approved in a tariff filed with FERC).

   Cascading Outages: The uncontrolled successive loss of system elements triggered by an incident at any location that results in the loss of 300 MW or more of networked system load for a minimum of 15 minutes.

   Instability: The inability of the transmission system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

Interconnection Reliability Operating Limit Event: An instance of exceeding an Interconnection Reliability Operating Limit for any length of time.

Interconnection Reliability Operating Limit Event Duration: The length of time an Interconnection Reliability Operating Limit is exceeded. The duration is measured from the point where the limit is first exceeded and ends when the value drops below the limit and remains below the limit for at least 30 seconds.

Uncontrolled Separation: The unplanned break-up of an interconnection, or portion of an interconnection, that is not the result of automatic action by a special protection system or remedial action scheme operating correctly.

Wide-Area Impact: The impact of a single incident resulting in the uncontrolled loss of 300 MW or more of networked system load for a minimum of 15 minutes.

5. **Question:** *Does redundancy of a critical bulk electric system asset or a Critical Cyber Asset change the criticality of these assets?*

   Answer: In NERC's cyber security standards No, 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 exposure to a cyber attack. For the purpose of security, each critical asset and redundant critical asset(s) must be protected under the cyber security standards as a Critical Cyber Asset.

6. **Question:** *Why have the following objectives from the definition of critical bulk electric system in the cyber security standard 1300 SAR been left out of the specific criteria used to identify critical bulk electric system assets in the proposed cyber security standards: "…would have a significant impact on the ability to serve customers for an extended period of time, ...or would cause significant risk to public health and safety"?*

   Answer: In keeping with the NERC mission, the cyber security standards criteria for identifying critical bulk electric system assets is focused only on reliability criteria. The identification of critical assets which "…would have a significant impact on the ability to serve customers for an extended period of time...or would cause significant risk to public health and safety" should be performed by the asset owner in collaboration with federal, provincial, state governments, and local authorities as appropriate. The Responsible Entities using a risk-based assessment must define the additional necessary criteria for identifying critical bulk electric assets.

7. **Question:** *In the cyber security standard, what is considered a routable protocol?*

   Answer: Routable protocols in the cyber security standard 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. Examples of protocols, which could be working at layer 3, are as follows: TCP/IP, Token Ring, DNP 3.0 (network mode only), etc.

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.

8. **Question:** *What is a dial-up accessible access under cyber security standard CIP–002–1?*

   Answer: Dial-up accessible access in the cyber security standard CIP–002–1 refers to any temporary (non-permanent) or not continuously connected communication access to a Critical Cyber Asset from any remote site. Using a modem to connect to a Critical Cyber Asset from one or more locations or by one of 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.

9. **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 Perimeters requirements for the remote access to that device but does not require a Physical Security Perimeter requirements 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.

10. **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 standard?*

    Answer: A control center or generation control center that provides critical operating functions and tasks as identified in Cyber Security Standard CIP–002–1 must be protected under the cyber security standard. The monitoring and operating control function includes controls performed automatically, remotely, manually or by voice instruction.

11. **Question:** *What are the requirements for protecting and securing jointly owned Critical Cyber Assets under the cyber security standard?*

    Answer: Jointly owned Critical Cyber Assets of Responsible Entities must be protected and secured as if the asset was not jointly owned. The nameplate value of the jointly owned critical assets will be used to identify critical assets as per Cyber Security Standard CIP–002–1

Requirement R1. All Responsible Entities having such joint assets are expected to ensure proper treatment according to the cyber security standard.

12. **Question:** *Do communication-related Cyber Assets for Critical Cyber Assets require protection under the cyber security standard?*

    Answer: Communications or communication systems between Electronic Security Perimeters for Critical Cyber Assets do not require the same protection as their associated Critical Cyber Asset. 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.

13. **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.

14. **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-002-1 Requirement R1, or unless they are identified under section Cyber Security Standard CIP-002-1 Requirement R3 as other Cyber Assets. Examples of alarm systems not requiring protection as a critical asset would be providing for functions such as security, environmental or support systems, or communication alarming. Asset owners are encouraged, whenever possible, to include alarm systems or alarm centers in their preferred risk-based assessment to identify additional critical assets under Cyber Security Standard CIP-002-1 Requirement R7 or 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 this Cyber Security Policy need to be a separate policy or can it be part of the corporations 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 this standard and provides a framework for the governance of these policies.

2. **Question:** *What types of information are to be considered critical?*

   Answer: Each Responsible Entity will need to conduct risk assessments to determine what information, were it to be released to unauthorized individuals, would put the reliable operation of that portion of the grid under its control at risk. Some examples of critical information would be the entity's grid maps, network connectivity diagrams, operating procedures, floor plans for facilities housing critical assets, and disaster recovery plans.

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

   Answer: Information classification levels indicate the sensitivity level of the information for personnel. The U. S. Government uses classifications such as Top Secret, Secret, Classified and Unclassified. Private industry can follow this type of classification hierarchy with classifications such as 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.

4. **Question:** *What is meant by documenting any deviation or exception from policy?*

   Answer: In order to properly determine risk on an ongoing basis, Responsible Entities need to understand areas where they may not be able to fully meet the requirements of this standard due to technology limitations or other mitigating circumstances. By having a separate person or persons responsible to review and approve these deviations or exceptions provides a set of responsible controls over any inability to fully address the requirements of this standard. Furthermore, by reviewing these deviations or exceptions, at least annually, ensures that each entity is continually aware of the potential risks to itself and the reliability of the electric grid for which it is responsible. Where it may be unclear to a compliance auditor whether a compensating control exists to meet the standard, it is recommended that the entity document a questionable deviation or exception in order to be able to ensure compliance to this standard.

5. **Question:** *Would the roles and responsibilities for critical asset owner, custodians, and users be the same for the access, use, and handling of critical information?*

   Answer: Identifying individuals within the entity who are responsible for the critical asset (logical or physical) assigns accountability for the security of that asset. Owners of critical assets are responsible for determining its classification level (logical asset) and restrictions on access (logical and physical). For example, an Operations Center Manager would be responsible for determining the areas within the facility that should be restricted to authorized personnel. He or she would also determine the types of information that should be restricted in the areas for which he or she is responsible. The manager would be responsible for assigning classification levels to the information.

6. **Question:** *Can you further explain the Governance section and what you mean by the appropriate level of accountability?*

   Answer: Corporate Governance provides for the following:

- A method to examine controls to evaluate whether each process is adequately monitored and reported to ensure that the process is performing as required by the business' needs.
- A method to help organize the process of assessing controls.
- Methods to measure the effectiveness of controls.
- Help to continuously identify opportunities to improve the security of the entities operations.

Additionally, a structure of corporate governance provides for the following activities:

Control Environment — The internal control component (commonly referred to as "tone at the top") that represents the overall environment in day-to-day activities. This is set at the executive level and demonstrates management's commitment to internal policies as well as this standard.

Risk Assessment — The internal control component that deals with awareness, identification, and analysis of relevant risks to each process area and how these risks are managed. This area needs to be addressed within each business unit responsible for a critical asset or assets.

Control Activities — The internal control component that examines policies and procedures and activities performed to meet objectives of the company. These control activities can be performed as often as daily or infrequently as annually depending of the needs of the process owner. All personnel are responsible to examine business processes and point out improvements.

Information and Communication — The internal control component that looks at how information is identified, captured, processed, and exchanged.

Monitoring — the internal control component that includes supervisory and managerial oversight, as well as monitoring of risks and recommended process changes.

If no one is responsible for the information, processes and activities that occur within a business unit and especially where they impact a critical asset or assets, then no one can be held accountable to maintain the overall security and reliability of those assets.

7. **Question:** *Do I have to validate existing employees/contractors who already have access?*

Answer: By validating existing employees you ensure that they are granted the appropriate levels of access as required by their job responsibilities. This is an ongoing activity. By validating existing personnel, you ensure that no person has additional levels of access that they do not require (transferred or promoted personnel) or have elevated privileges that they should not have in order to perform their job functions.

8. **Question:** *Who should be reviewing access privileges (physical and logical)?*

Answer: This is where "Separation of Duties" becomes important. The term "Separation of Duties" is professional security and audit terminology meaning that the same personnel who authorize, grant, or revoke access privileges should not be the ones who conduct the review of

personnel access privileges. Typically, Security or Audit departments can conduct the review. The functional managers of the area being reviewed would also have to be involved in the review process in order to identify any person that should not have access to that area or information.

9. **Question:** *Why do I need to have someone designated to validate that systems have successfully passed a testing process?*

   Answer: Again, this is part of governance. It is considered a best practice by many auditors that the person who validates the system is not the same person who developed the software or runs the system. It is recommended that you assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that the requirements of this standard are being properly addressed. This further provides another set of eyes on the process that is not influenced by daily operations or the way it "should" work. This, of course, does not mean that the operator, etc. cannot provide input into the testing process. It simply separates the duties of daily operations from the testing protocols. Separation of duties is considered a standard of due care by many professional security and audit organizations.

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

1. **Question:** Are any employees, contractors or service providers going to be "grandfathered" under the background-screening requirement in this section?

   Answer: Only employees, contractors or service providers who have had a background screening check within the previous 5 years from the implementation date of the Standard will be "grandfathered" for the purposes of this section. All others will have to have either an update screening or initial screening conducted, depending upon the length of time since the last screening or the current unrestricted access to Critical Cyber Assets.

2. **Question:** What are the Background Screening requirements for this section?

   Answer: As indicated, the screen should be conducted in accordance with all applicable laws and agreements, and leaves the specific components of the screening 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 background screening 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.

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

   Answer: Awareness training is left to the discretion of the Responsible Entities and can take the form of memos, e-mail, computer based training, posters, meetings, etc. The proof of reinforcement can be copies of the media, employee training records, meeting logs, etc. This training can be combined with training on the cyber security standard itself.

4. **Question:** What does "access" mean?

Answer: Employees, contractors or service vendors who are deemed to be trustworthy enough for access (cyber or physical) to critical cyber security assets, as defined by the standard. They will have been trained and screened per this section of the standard. All others should be escorted or otherwise supervised when being provided access to critical cyber security assets.

5. **Question:** What does "for cause" mean in under Background Screening?

   Answer: "For cause" means any situation that comes to management's attention that would void an employee's, contractor's, or services vendor's right to access, either on or off the job. Typically, this is gross misconduct such as a misdemeanor or felony conviction, but it can include disciplinary action that impugns the reliability of the employee.

6. **Question:** What are "adverse employment actions" referred to under Background Screening?

   Answer: Adverse employment actions could include rescinding of a job offer or transfer due to derogatory information that surfaces as part of the screening process, such as a criminal conviction, violent tendencies, dishonesty, unethical behavior, etc. Criminal convictions themselves are not necessarily a bar to employment, but the non-disclosure of conviction may be. Other factors include the length of time since the infraction, the nature of the infraction, the applicant's employment record since the infraction, etc. Further guidance is contained in publications such as the "LPA Background Check Protocol" previously referenced.

7. **Question:** Who is responsible for conducting the screening of contractors and service vendors?

   Answer: The Responsible Entity is accountable for ensuring that background screening is conducted per this section 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, the Responsible Entity must be prepared to confirm that a program exists and meets the intent of this section.

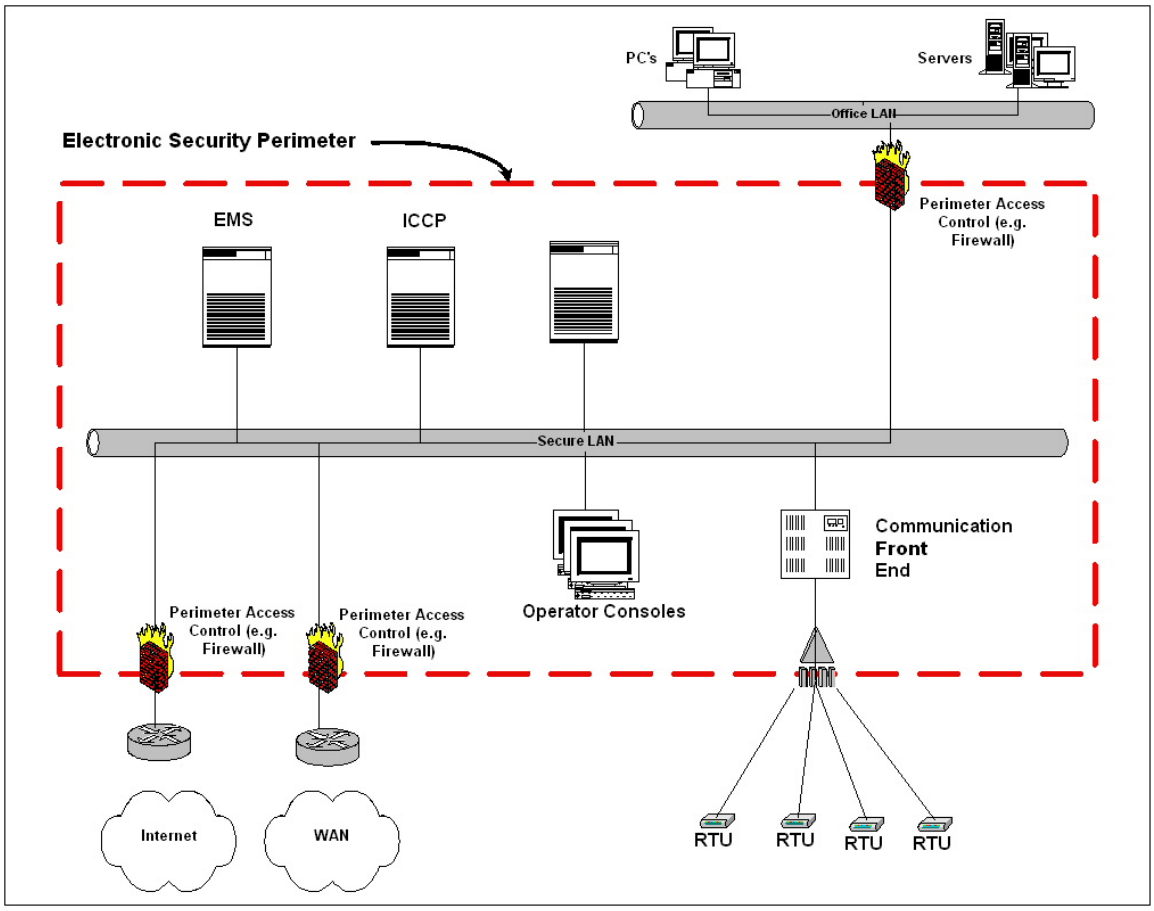
8. **Question:** What if our existing labor agreement does not address or allow background screening of bargaining unit employees? How can we meet the standard?

   Answer: Standard CIP–004–1 acknowledges limitations in labor agreements by indicating that application of the screening section is subject to "existing collective bargaining unit agreements". In those cases where a company cannot implement a program due to a labor agreement, they can apply for a case-by-case waiver, and provide a copy of the labor agreement if it is in force during a compliance audit. However, those companies are expected to address the screening issue as a bargaining item in their next contract negotiation to attempt to attain full compliance under the standard.

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.

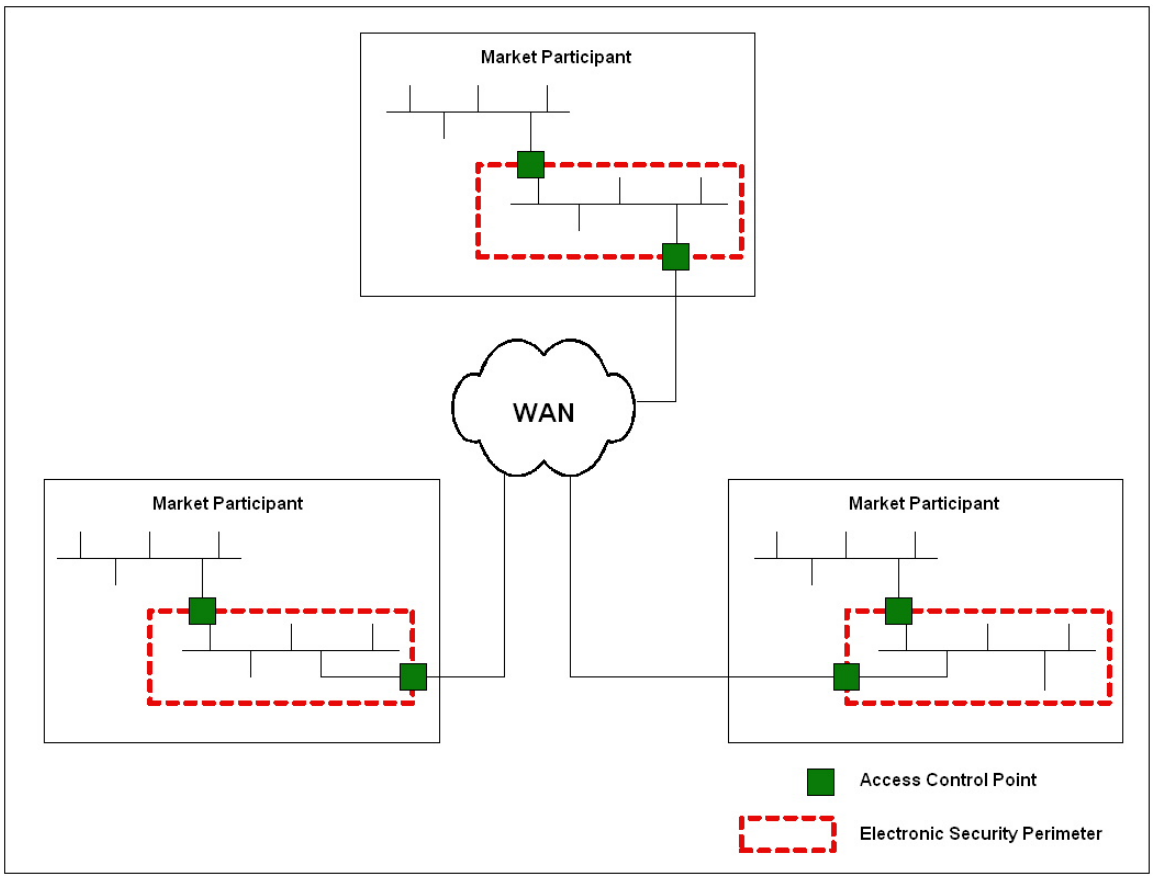


The RTUs may need an Electronic Security Perimeter if they use a routable protocol and meet the definition of a Critical Cyber Asset. Also, a single computer may need an Electronic Security Perimeter if it meets the definition of a Critical Cyber Asset.

This section of the standard deals with the security of the electronic perimeter. In a defense in depth approach, appropriate protection measures must also be implemented at the device level: these measures are addressed in the requirements for Standard CIP–003–1 Cyber Security — Security Management Controls and standard CIP–007–1 Cyber Security — 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 clearly states that where discrete Electronic Security Perimeters are connected by communication lines, the communication lines are not included in the security perimeter. The following schematic illustrates this point.



3. **Question:** *I have a single RTU, which 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. An Electronic Security Perimeter is not required for the RTU if it uses a non-routable protocol. The RTUs using routable protocols employ a master/slave synchronous polling method that cannot be used to access anything on the EMS. They also use SBO (select before operate) command to control devices at the RTU end.

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

4. **Question:** *Must I have a firewall to secure the electronic perimeter?*

   Answer: A firewall is any device that provides access control between a more secure and a less secure zone and has electronic logging. The standard does not specifically require the use of a commercial firewall. However, it does require that all access points to the perimeter be secured with adequate access control and monitoring measures. Any measure, which meets the requirements of the standard, is sufficient. However, in the case of a network with multiple devices connected and containing one or more Critical Cyber Assets as defined in the standard, a firewall device provides many functions, which satisfy many of the requirements in the

standard. These include, among others, access control, electronic logging and alerting and strong authentication capabilities.

5. **Question:** *What is strong authentication?*

   Answer: A requirement of the standard requires that strong authentication be implemented for interactive access to an Electronic Security Perimeter. Often, trusted employees and contractors/vendors outside of the electronic perimeter, require access inside the Electronic Security Perimeter to support or maintain Cyber Assets there. These trusted employees or contractors/vendors are required to authenticate before access is granted.

   Authentication measures can require any combination of three factors: something the person knows, something the person has, and 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. A strong authentication scheme is usually defined as one, which requires at least two of these factors. 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. Other ways to implement enhanced authentication is by a procedural verification (such as requiring a telephone call with verification of some characteristic of the person) before the person is activated and allowed to authenticate using a password.

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

   Answer: The standard does not specifically require that you install intrusion detection systems on your network or in the Cyber Assets. It requires that you have some intrusion detection processes, which 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 systems specifically designed for this purpose and provide an easier way to automatically provide these functions.

7. **Question:** *I have a Virtual Private Network (VPN) which 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 access control measures at the VPN server (such as restricting access ports and appropriate authentication measures) to the entity you are authorizing access to.

8. **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 intended for

authorized users as well as unauthorized users, and one used in internal networks, when emphasis is on corporate policy on appropriate use of technology systems.

A sample of a typical banner on an edge system may be as 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 enforcement officials.

==========

A sample of a banner used on an internal system may be as 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.

==========

9. **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

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

1. **Question:** *What is the Physical Security Perimeter?*

Answer: The Physical Security Perimeter is the physically secured area within which the Critical Cyber Assets reside. It is defined as the nearest four-wall boundary that can be physically secured to control and monitor physical access to the assets.

2. **Question:** *Can each utility define the Physical Security Perimeter as they see fit, or are there some minimal requirement for the Physical Security Perimeter as it relates to the Electronic Security Perimeter?*

   Answer: The only minimal requirement is that all Cyber Assets or access points (for example network connections, firewalls, VPN devices, routers) to the Electronic Security Perimeter must reside within the Physical Security Perimeter.

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

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

4. **Question:** *Can an organization identify zones or levels of access to various Critical Cyber Assets based upon predefined levels of criticality?*

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

5. **Question:** *Does an organization'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 organization should consider covering tailgating in the physical security policies and procedures, and communicating these policies in the annual awareness training.

6. **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.

7. **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 under the CIP 002–009 standard for physical security?*

   Answer: Yes, a security cage can meet the requirements for a security perimeter as long as all equipment resides within the cage, and the cage provides a door with lock to control access. Note that you must also meet the access control, monitoring, and logging requirements of the standard.

8. **Question:** *Our company utilizes 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: No, retention of one log of physical access for 90 days is sufficient. However, in the event that a security incident involving physical access is detected within the 90-day period, the specific log related to that incident must be retained for three years.

9. **Question:** *What are some examples of " government or industry generally accepted risk assessment methodologies"?*

   Answer: Examples are:
   i. Vulnerability & Risk Assessment Program (VRAP) …. Source: US DOE or Argonne National Laboratory, and the basis of the first NERC risk assessment guideline.
   ii. Risk Assessment Methodology (RAM-T)…. Source: Sandia National Laboratory or US DOE.
   iii. Carver Methodology…. Source: US Department of Defense.

10. **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.

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 central monitoring station?

    Answer: Can be a commercial service or a dispatch desk. The main criterion is human monitoring 24 hours per day.

13. **Question:** It seems that monitoring a gate at a fenced facility such as a power plant would be sufficient to secure a four-walled boundary.

    Answer: The suggestion would not meet the intent of CIP–006 though it could contribute to an improved security strategy. Cyber Assets are generally housed inside walled facilities and these are to be secured according to the standard.

14. **Question:** If the only method used for logging physical access is video, it could be difficult to meet the 90-day retention with digital video systems because of storage costs.

    Answer: While this is 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.

15. **Question:** In the case of a room containing Critical Cyber Asset(s) which is staffed at all times, escorted personnel who enter these rooms are escorted and would be exempt from the requirements for background checking, training, and logging physical access. Is this a correct interpretation?

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

16. **Question:** Give me an example of a six-wall boundary.

    Answer: In a building, the tendency is to secure the perimeter walls and access points. The standard requires that the floor and ceiling be secured to the same standard as the perimeter. For example, raised floors and drop ceilings create vulnerabilities. In the case where the Critical Cyber Asset is small and located in an area where one would want to give less restricted access, one may secure the asset with a Physical Security Perimeter such as a cage, safe or metal cabinet that has had security measures applied to it. The intent is to clearly define a security boundary, which applies the same level of security over its entire area.

17. **Question:** *Section CIP-006, requirement (1) appears to assume that 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 be aligned with the CIP 002–009 standard. If none exists, one should be created in accordance with the provisions of NERC CIP 002–009

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

1. **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.

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

   Answer: The entity is responsible for determining the non-production systems in its environment. It is possible depending on the 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.

3. **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
   - Performance testing to assure system stability under load conditions

- Validate security-related functions: access controls, audit functions, file protection
- Test for malicious logic
- Review technical documentation to determine security features
- Review source code if available for application security

4. **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.

5. **Question:** *If said test yields a failure of a "Critical Cyber Asset" is that a reportable incident?*

   Answer: No

6. **Question:** *What is meant by "document the test environment"?*

   Answer: The testing environment should be documented to verify that it adequately represents the production environment and security testing. Documentation should also verify that the testing environment is on a controlled non-production test environment.

7. **Question:** *Does the test environment specification need to be included with each test conducted?*

   Answer: If the test environment does not change, it can be documented once and referenced in each subsequent test.

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

   Answer: Common system administration modifications (changes) should be reviewed to verify they do not introduce vulnerabilities to the system. The tests are intended for new hardware and/or software, as well as new releases and patches of existing software.

   Significant changes do not include: re-partitioning or defragmentation of disc, clearing defunct process queues, simple presentation screen changes, data entry, or component for component replacements, etc.

   Significant changes include major product *releases*, characterized as "x to y", e.g., Oracle 7 to Oracle 8. New v*ersions* are significant software changes that constitute a major change to a release level, characteristically identified as "x.1 to x.2" or greater increments; these are sometimes referred to as "point releases." Version *revisions* are typically denoted as "x.1.1 to x.1.2.", but these typically *do not* constitute a significant change. This is not always the case however, so "read me" notes should be consulted for specific naming conventions, content, and impact applicability. In general, it is better to err on the side of conservatism when change impact is not well quantified.

   Significant change to database concerns database software itself, not data content. Changes to stored procedures *may* constitute a significant change insofar as they affect access controls.

Application software changes are considered significant whether internally developed or provided by a third party.

9. **Question:** *What is an appropriate process for managing administrator and generic accounts?*

   Answer: Documentation of administrator accounts should identify all personnel having access permission to use such accounts, and administrator policies should provide clear guidance concerning acceptable use. Logging mechanisms must be enabled 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 group account usage auditing: Where a generic or group-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 shall be changed, to the point of at least every 90 days for system administrator accounts.

   Refer to DOE or NIST SP–800 Series Standards for guidance on hardening passwords.

10. **Question:** *What is required for auditing of user activity?*

    Answer: The Responsible Entity must determine its own logging strategy that fits the requirement. This strategy must be sufficient to support the investigation of an event and that the integrity of these electronic records is maintained.

11. **Question:** *What is meant by "personal registration"?*

    Answer: "Personal registration" refers to a named individual identified as being responsible for ensuring appropriate use of the account.

12. **Question:** *Are patches required to be installed?*

    Answer: No, a process must be in place to manage the implementation of the patches. The process should include investigation, testing, implementation, back-out plans, and appropriate decisions made throughout the process. It is acceptable to make a conscious decision to not implement a patch, as long as a good reason is documented and compensating measures have been effected to mitigate the vulnerability the patch is intended to address.

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

    Answer: The application should provide you with adequate documentation as stated in question one above.

14. Question: *Does the standard require installation of non-security patches?*

Answer: No, installation of non-security patches is an operational and maintenance decision. However, in the case of layered software, a security patch may require the system to be running a base version, which may result in needing to upgrade other layered products. Follow the software vender's instruction and guidance.

15. Question: *What if anti-virus software is not available for the operating system being utilized?*

Answer: Appropriate steps should be taken and documented to mitigate a virus attack. These steps could include:

- Limiting network connectivity of that system to absolutely essential services.
- Disabling email services from that system.
- Disabling Internet browsing from that system.
- Installing a security appliance between the system and the network that provides a security perimeter. This appliance should have access controls like a firewall, virus scanning and blocking capabilities, and potentially intrusion detection capabilities.

16. Question: *What is mal-ware?*

Answer: Mal-ware is the name being used for malicious software such as viruses, worms, time-bombs, and Trojan horses. This software is distributed through email attachments, un-secured remote procedure calls, Internet downloads, and opening of infected files. Mal-ware 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.

17. Question: *Is a full shutdown of the production system required to test the backup and recovery process?*

Answer: No, the intent is to validate cyber recovery procedures as much as possible, and to ensure necessary personnel are proficient in those procedures. The use of tabletop exercises and structured walkthroughs may be appropriate in some cases. Utilizing recovery procedures for re-establishing the system following scheduled maintenance, following hardware failures, etc. can satisfy validation and training needs. Backup media should be tested at regular intervals for continuing viability in the event they may be needed for recovery, at least once per year.

18. Question: *How intrusive are the investigations?*

Answer: Investigations would be based on the ensuing complaint. They would be sufficient enough to determine the cause and remediation plans.

19. Question: *What would predicate an investigation?*

Answer: A complaint sufficient enough to note a major vulnerability that could affect the Bulk Electric System.

Standard CIP–008–1 — Cyber Security — Incident Reporting and Response Planning

1. **Question:** *Are there any plans to update the Indications, Analysis, & Warning Program Standard Operating Procedure (IAW SOP) on the Electricity Sector Information Sharing and Analysis Center (ES ISAC) website? It's dated 2/25/02.*

   Answer: The Critical Infrastructure Protection Committee plans to initiate a project to review and update the IAW SOP starting in September of 2004.
   http://www.esisac.com/IAW.htm

2. **Question:** *The IAW SOP states that it is a voluntary program, intended to provide information on known malicious or unknown cause events. Is reporting incidents to the ES ISAC optional?*

   Answer: There is a requirement in the 1200 series NERC Cyber Security Standard that makes reporting Cyber Security Incidents mandatory. This requirement is also included in draft standard CIP–008–1 Cyber Security — Incident Reporting and Response Planning, requirement R4. The IAW SOP defines what incidents must be reported, provides criteria, and describes how to report them.

3. **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 an organization that warrants an industry-wide warning, sensitive information provided by the reporting entity will be anonymized before being disseminated.

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

4. **Question:** *What is a reportable incident?*

   Answer: Physical and cyber event criterion and thresholds are defined in the IAW SOP. While the IAW SOP defines both physical and cyber events, the standard CIP-008-1 only

covers cyber incidents and those physical incidents that are directly related to Critical Cyber Assets. The reporting of other physical incidents should be covered under a separate standard.

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

   Answer: To name just two, the ES ISAC Indications, Analysis, & Warning Program Standard Operating Procedure:
   http://www.esisac.com/IAW.htm

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

6. **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. The Responsible Entity must establish procedures with the intermediary to ensure that the ES ISAC receives the report.

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

1. **Question:** *Are we going to have to have a documented recovery plan for every substation?*

   Answer: No. The short-term recovery plan for a specific substation may be managed on a daily basis by advanced power system applications such as state estimation, contingency & remedial action, outage scheduling, or others. One recovery plan should suffice for several similar facilities like 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 entity should perform a risk assessment of their 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 shall 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, the efficacy

of communications, and appropriateness of personnel. Document lessons learned and integrate 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 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 assets?*

Answer: No. Not every critical 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 and this will require a redundant or backup facility. Because of these differences, the Recovery Plans associated with Control Centers will differ a great deal with 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.