# Cyber Security Standard 1300
# Frequently Asked Questions (FAQ's)

## Section 1301 — Security Management Controls

1. **Question:** *Does this Cyber Security Policy need to be a separate policy or can it be part of the corporation'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 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 grid maps, network connectivity diagrams, operating procedures, 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 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 provides a set of responsible controls over any inability to fully address the requirements of this standard. Furthermore, by reviewing these 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.

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:** By 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 as

well as determining what types of information should be restricted in the areas that he is responsible for. 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:

   - It provides 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.
   - It provides a method to help organize the process of assessing controls.
   - It recommends methods to measure the effectiveness of controls.
   - It helps 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 their 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 on the needs of the process owner. All personnel are responsible for examining business processes and pointing 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 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 assigns 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.

## Section 1302 — Critical Cyber Assets

1. **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 or greater than the generation limit in the 1300 standard.

2. **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 is not used in existing NERC policies.)*

   *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.

3. **Question:** *Does redundancy of a critical bulk electric system asset or a critical cyber asset change the criticality of these assets?*

   **Answer:** In the cyber security standard, 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 expose the cyber asset to more exposure. For the purpose of security, each critical asset or redundant critical asset(s) must be protected under the cyber security standard as a critical cyber asset.

4. **Question:** *Why have the following objectives from the definition of critical bulk electric system in the 1300 SAR been left out of the specific criteria used to identify critical bulk electric system assets in the proposed cyber security standard: "…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:** The cyber security standard criteria for identifying critical bulk electric system assets is focused on only reliability criteria in keeping with the NERC mission. 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 done by the asset owner in collaboration with federal, provincial, state governments, and local authorities as appropriate. Ultimately, the asset owners using a risk-based assessment must define the additional necessary criteria for identifying critical bulk electric assets.

5. **Question:** *What is NERC Policy 1.B, Section 2.4?*

   **Answer:** NERC Policy 1.B, Section 2.4 states: "REPORTABLE DISTURBANCES are contingencies that are greater than or equal to 80% of the MOST SEVERE SINGLE CONTINGENCY loss. Regions may optionally reduce the 80% threshold, provided that normal operating characteristics are not being considered or misrepresented as contingencies." The MOST SEVERE SINGLE CONTINGENCY is the largest single generator under the responsible entity's control.

6. **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 which do not use a routable protocol must meet the electronic security perimeters requirements for the remote access to that device but they do not require the physical security perimeter requirements or local electronic security

perimeter for actual critical cyber asset. This direction provides for secure remote access while meeting the intent of the current cyber standard providing a minimum level of security.

7. **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 their associated critical cyber asset since compliance to all sections of the cyber security standard would only affect 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.

## Section 1303 — Personnel

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 five 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 screening requirements for this section? None are specified under section 2.4, Background Screening?*

   **Answer:** As indicated in section 2.4.3, 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, a social security number verification and 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:** As indicated in section 2.3, Awareness, the awareness training is left to the discretion of the responsible entities and can take the form of memos, emails, 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:** Those are 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 who are unscreened per the standard should be escorted or otherwise supervised when being provided access to critical cyber security assets.

5. **Question:** *What does "for cause" mean in section 2.4.5, under Background Screening?*

   **Answer:** That is 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 in section 2.4.4, under Background Screening?*

   **Answer:** This could be the 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.

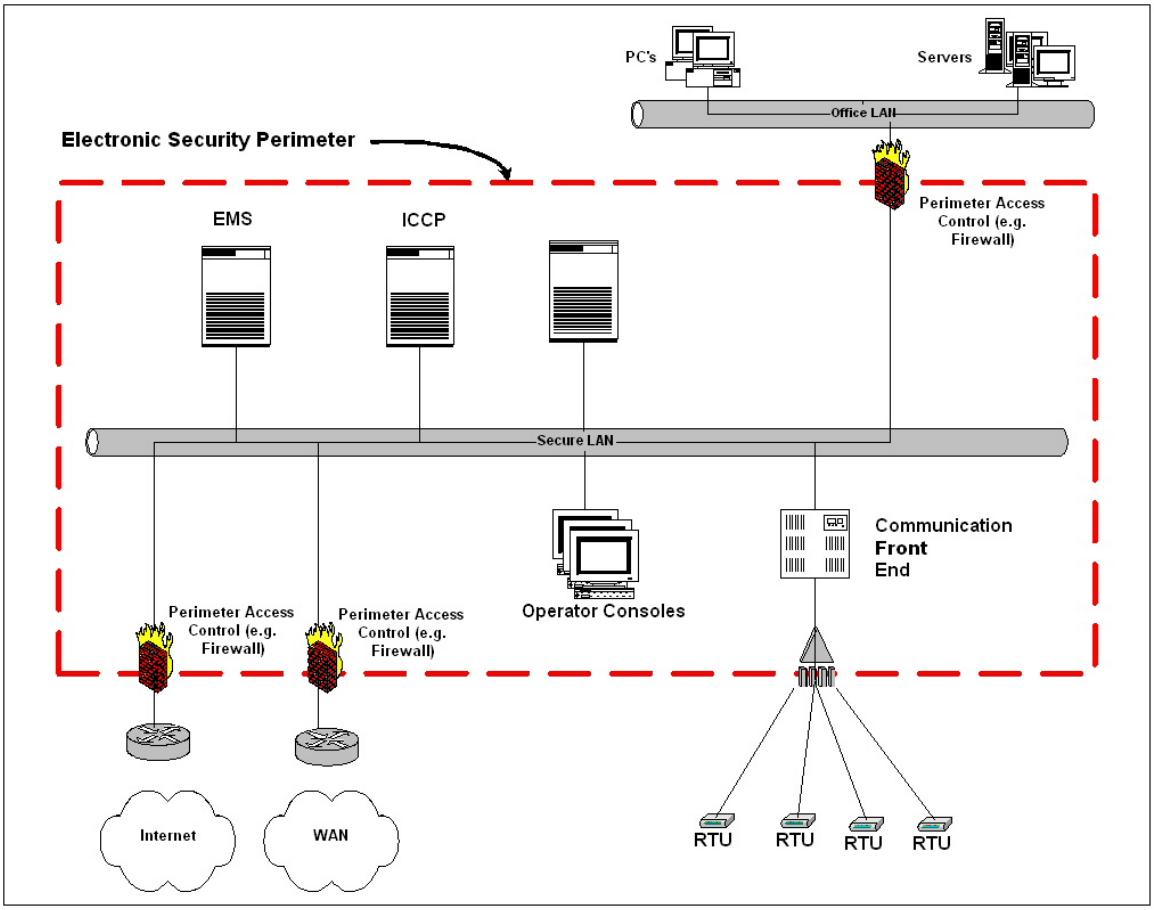
8. **Question:** *What if our existing labor agreement does not address or allow background screening of bargaining unit employees? How can we meet the standard?*

   **Answer:** Section 1303 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.

# Section 1304 — 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.

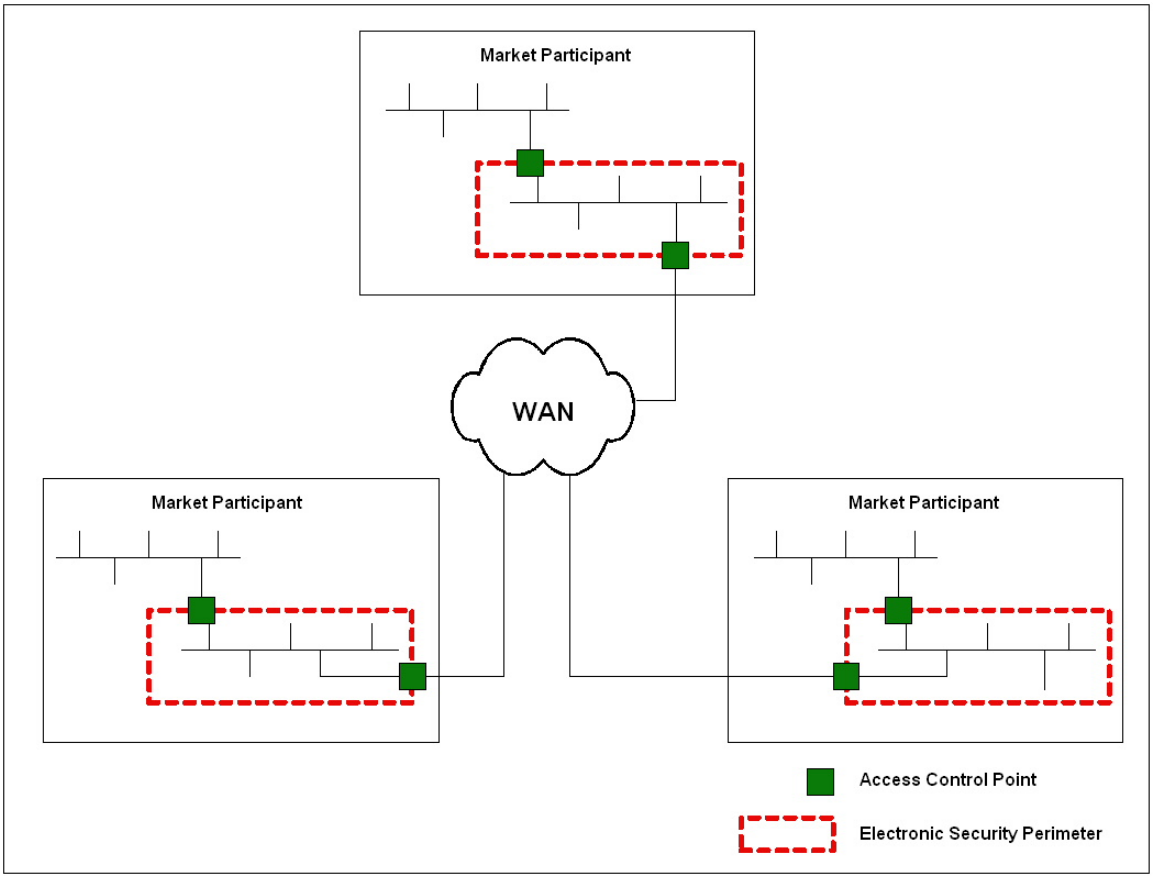



The RTUs may need an electronic security perimeter if they use a routable protocol and meet the definition of a critical cyber asset. Also, a single computer may need an electronic security perimeter if it meets the definition of a critical cyber asset.

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 section 1301 — Security Management Controls and 1306 — 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 and an electronic security perimeter is not required at the RTU if the RTU is not using a routable protocol. The RTUs that use a non-routable protocol have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO (select before operate) command to control devices at the RTU end.

   If a dial-up 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 (i.e., 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 that 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 that 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 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 that 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) 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 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:** *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 that deal with this issue.

   The following site provides a listing of NIST publications on computer security http://csrc.nist.gov/publications

## Section 1305 — 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 is 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 1300, 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 1300 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.

## Section 1306 — 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:** *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

3. **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.

4. **Question:** *If said test yields a failure of a "critical cyber asset" is that a reportable incident?*

   **Answer:** No

5. **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 vendor-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 a 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/vendor.

6. **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.

7. **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.

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

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

9. **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.

10. **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.

## Section 1307 — Incident 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 (ESISAC) 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.

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 ESISAC 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 planned for inclusion in article 1307.1.3 of the proposed 1300 series Cyber Security Standards. 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 ESISAC protected from disclosure?*

   ***Answer:*** NERC manages the ESISAC. 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.

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

   **Answer:** To name just two, the ESISAC 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.

## Section 1308 — 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.