



RCIG

REGIONAL COMPLIANCE IMPLEMENTATION GROUP

RCIG Assessment

Monitoring and Implementation of

Reliability Standard CIP-004-01

Cyber Security – Personnel and Training

Prepared by: Regional Compliance Implementation Group (RCIG)
October 15, 2009
REMG Approved November 3, 2009

RCIG – A - 002



1. Introduction

This Assessment is intended to examine one of the most-violated Standards and provide information on compliance, including reasons for violations, and identifying suggested process enhancements to assist in improving compliance with CIP-004, in order to assist Registered Entities in their compliance efforts. The NERC Board of Trustees Compliance Committee (“BOTCC”) encouraged the RCIG to develop assessments based on the most-frequently violated Standards. This assessment will be revised in the future as regions gain more experience in monitoring it. It is offered for guidance purposes only.

The RCIG decided to examine Standard CIP-004-1 as the subject of this assessment. Although Reliability Standard CIP-004-1 does not become audit ably compliant for all entities and all requirements until the end of 2010, already it has been identified as one of the most frequently violated Reliability Standards. Furthermore, although this Reliability Standard carries a lower or medium Violation Risk Factor (VRF), it deals with significant security issues. Evidence suggests that an entity in violation of one of the Requirements may well be violating others; and early education and sharing lessons learned so far with entities will help them improve their performance.

This assessment will examine the implementation of this Standard, determine the reasons for violations, and identify suggested process enhancements to improve compliance with this Standard. Because many entities subject to this Standard are on a six year audit cycle, this assessment may provide an opportunity to improve compliance and may result in fewer violations uncovered through self-reports, self-certifications, or at the next audit.

The RCIG acknowledges and appreciates the work of NERC staff and the RCIG’s CIP Compliance Working Group in assisting in preparing this assessment.

2. CIP-004-1: Summary of Major Requirements and Violations

Standard CIP-004 requires that **personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness**. The major requirements, discussed more fully below, are:

- a. Awareness of Security Program
- b. Cyber Security Training
- c. Personnel Risk Assessment
- d. Personnel Access to Critical Cyber Assets

Recently, NERC analyzed 80 violations of CIP-004-1 and identified the specific requirement violated by the Registered Entities¹. NERC found that over 90% of the violations were identified through self-reports. Table 1, from the NERC draft report, shows how the 80 violations are classified according to requirement.

¹ “Summary Report for Violations of CIP Standard CIP-004- Cyber Security – Personnel and Training” (Prepared for the Board of Trustees Compliance Committee August 4, 2009, http://www.nerc.com/docs/bot/botcc/ITEM_3_Supplement_CIP-004_Analysis.pdf)

Table 1 CIP-004-1 by Requirement	Number of Violations
Requirement 1 – Awareness (All Sub levels) ²	0
Requirement 2 – Training (All Sub levels)	23
Requirement 3 – Risk Assessment (All Sub levels)	29
Requirement 4 – Access (All Sub levels)	28
Total	80

In its draft report, NERC succinctly stated:

There are many reasons identified for non-compliance by Registered Entities, from documentation to performance-related issues. NERC classified the 80 violations of CIP-004-1 by four (4) different types of violations given the information provided in the Violation Description and the Potential Impact fields of the regional workbook submissions to NERC. The classification buckets are:

Documentation - a lack of records to demonstrate compliance with the Standard;

Access - employees or contractors granted access to Critical Cyber Assets without proper clearance or escorted access;

Training - training was not offered or completed on time by employees or contractors; and

Risk Assessment - employees or contractors with access to Critical Cyber Assets did not complete nor had an incomplete background check.

The intent of this RCIG Assessment is to flesh out the various reasons for violations and to offer suggestions for entities to improve their cyber security program. The examples cited in this Assessment were taken from actual violation reports and represent the types of issues that have resulted in a finding of non-compliance. In some instances, the examples are summarizations of multiple, similar reports. In preparing the recommendations for improvement, the authors have attempted to go beyond simply restating the requirements and offer good business practices that can be implemented to help the Responsible Entity achieve and maintain compliance with the CIP-004 Standard. For example, the use of a suspense or “tickler” file is suggested to help the Responsible Entity prevent overlooking an upcoming requirement. While such a file is not required by the Standard, it is a good business practice offered for consideration.

3. Key Reasons for Non-Compliance and Suggested Process Enhancements

The following information is organized by requirement. For each, typical facts surrounding violations are noted and suggestions for improvement are offered, based on the experience to date of the regional CIP compliance staff.

² Not fully compliant for any entities before July 1, 2009. The other three requirements became fully compliant for Table 1 and 2 entities July 1, 2008.

R 1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- **Direct communications (e.g., emails, memos, computer based training, etc.);**
- **Indirect communications (e.g., posters, intranet, brochures, etc.);**
- **Management support and reinforcement (e.g., presentations, meetings, etc.).**

Although this requirement achieved the Compliance (“C”) date for Table 1 and Table 2 entities on July 1, 2009, there have been no self-reported violations to date. This may be as a result of the short period of time entities have had to be compliant. Audits of this requirement will not commence until July 2010.

R 2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary

Common violations fell into two categories:

➤ **Entity had no cyber security training program**

Example: Due to a late identification of one or more critical assets and associated Critical Cyber Assets, the entity did not have a documented cyber security training program by the time the entity was required to be fully compliant with the CIP Standard requirement.

Suggested Enhancement: Appropriate training is a cornerstone of any good cyber security program, is a good business practice, and should be established irrespective of identifying Critical Cyber Assets under the CIP Standards.

➤ **Entity’s training program documentation was not up to date**

Example: The entity’s training program was compliant with the CIP Standards requirements; however, the training policy and procedure were not up to date.

Suggested Enhancement: Developers of an entity’s cyber security training program and the entity’s management should understand and emphasize the importance of not only updating training programs, but also updating all documentation related to the program whenever changes are made to the program. An entity’s review and approval process for its training program should include a specific process to review and update any relevant documentation.

R.2.1 This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

➤ **Training not completed within 90 days of being granted access**

Example 1: The entity granted temporary access for a period less than 90 days. The entity believed that since access was revoked before the 90 day training window expired, there was no longer a need to conduct the required training.

Example 2: The entity's access management policy required verification of the required cyber security training before granting access even though Version 1 allows training up to 90 days following access. However, the implementation procedures failed to include the verification step. As a result, personnel were found to have been granted access without having undergone the required training.

Example 3: A transferred employee did not receive the required cyber security training within 90 days of being granted access.

Example 4: The entity did not have the proper documentation and training in place for replacement following the loss of a key employee.

Example 5: In preparation for compliance with the requirement, the entity bulk uploaded a large number of employees into the access management and tracking system. Due to an administrative oversight, a small number of those employees did not receive the required training.

Example 6: Employees granted authorized cyber or unescorted physical access either did not receive training within the 90-day timeframe, or received training beyond the 90 day timeframe.

Example 7: Entity failed to apply training to its existing employees upon implementation of the program once the requirement reached the compliant stage.

Suggested Enhancement: Version 2 of the CIP Standards will require verification of the required cyber security training *before* granting access. This differs from Version 1, which allows up to 90 days for training to be completed. Registered Entities should review and update current physical and cyber access management policies and procedures to include the version 2 requirements. An entity choosing to rely on the version 1 language until version 2 is in effect, should establish a process to ensure the training is completed by the end of the 90 day period. Granting temporary access of less than 90 days without training, or revoking access after 90 days if training is not completed, does not excuse the entity from the requirement of the Standard.

➤ **Contractor/vendor support personnel not trained**

Example: The entity determined that contractors with authorized unescorted physical access had not completed the required cyber security training.

Suggested Enhancement: Ensure the access management program requires all personnel who are granted either authorized electronic or unescorted physical access to receive the training specified by the requirement. The personnel must include all personnel with such access, such as janitorial staff and maintenance personnel with unescorted physical access and vendor support staff who provide remote support of the Critical Cyber Assets or other cyber assets within the Electronic Security Perimeter.

R 2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities

- R1.2.1.** The proper use of Critical Cyber Assets;
- R1.2.1.** Physical and electronic access controls to Critical Cyber Assets;
- R1.2.2.** The proper handling of Critical Cyber Asset information; and,
- R1.2.3.** Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

➤ **Cyber security training program does not meet the Standard**

Example: Entity had an established training program; however, it did not include training on entity-specific procedures.

Suggested Enhancement: Review the cyber security training program to ensure training is provided specific to the identified Critical Cyber Assets. The training should be tailored and appropriate for the roles and responsibilities of the trainees. To assist the Responsible Entity in ensuring the proper training is provided, a roles and responsibilities matrix may be helpful. Having definitive documentation of an individual's responsibilities and the type of access granted will guide the development and conduct of the required training and will also help the Responsible Entity demonstrate that the training was "appropriate to personnel roles and responsibilities" as required by the Standard.

Requirement 2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

➤ **Incomplete documentation**

Example 1: The entity did not have records confirming that all required employees have completed the annual cyber security training.

Example 2: Entity lacked accurate training records demonstrating all employees, contractor, and vendor support staff had completed the annual cyber security training.

Suggested Enhancement: If training is conducted in a formal classroom setting, ensure all trainees have signed the dated class attendance roster. If training is computer-based, investigate utilizing technology that will automatically track progress and report completion of the training, preferably with a reporting database that can be queried. If static training materials, such as a PowerPoint presentation with or without voiceover, are distributed electronically or in hardcopy form, include a certification page that the trainee signs, dates, and returns. In all cases, follow up with scheduled trainees to ensure the training is completed within the required

time frame and immediately revoke access at the end of the annual training window for any employee, contractor, or vendor support personnel who fail to complete the training.

R 3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include....

The most common violations found for this requirement were:

➤ **Access granted without personnel risk assessment**

Example 1: In reviewing the results of a bulk upload of personnel with authorized access to Critical Cyber Assets, several personnel were found to have not completed the required personnel risk assessment.

Example 2: Personnel were granted authorized access to Critical Cyber Assets as a result of a job change without completing the personnel risk assessment within 30 days of being granted access.

Example 3: Contractor personnel with authorized access to Critical Cyber Assets were overlooked and did not undergo a personnel risk assessment.

Example 4: The entity had not contracted with a service provider for conducting personnel risk assessments.

Example 5: Master access list did not accurately reflect authorized access. Discrepancy determined when comparing the master list against access control system records.

Example 6: Quarterly review identified personnel with authorized access that had not completed a personnel risk assessment.

Example 7: Documentation was missing or incomplete. Thus, the entity could not demonstrate that the required personnel risk assessments for employees with access to Critical Cyber Assets were conducted at the time of their hiring.

Suggested Enhancement: Review and update the physical and cyber access management policies and procedures to include verification of the required personnel risk assessment before granting access as will be required with version 2 of the CIP Standards. If the entity chooses to rely on the version 1 language until version 2 is in effect, establish a process to ensure the personnel risk assessment is completed by the end of the 30 day period. Granting temporary access of less than 30 days without completing a personnel risk assessment or revoking access after 30 days if the personnel risk assessment is not completed does not excuse the entity from the requirement of the standard.

➤ **Entity Policy/Procedure not updated**

Example 1: Company personnel risk assessment policy was not updated to conform to the CIP Standard requirements.

Example 2: Entity access management policy was not updated to require a personnel risk assessment within 30 days of granting authorized electronic or unescorted physical access to Critical Cyber Assets.

Example 3: Entity policy conforming to the CIP Standard requirement was in draft and had not been approved.

Example 4: Personnel risk assessments were not updated every seven years for employees or contractors, or more than seven years had elapsed since the last such check

Example 5: Entity's personnel were vetted and trained as required. However, the entity changed its vetting methodology and implemented that change without changing its written program. Changing the way the PRA is conducted without changing the documented program is a violation of the requirement.

Suggested Enhancement: Review the applicable personnel management policies and procedure to ensure a personnel risk assessment is required for any employee, contractor, or vendor support staff with authorized access to Critical Cyber Assets. Ensure the access management policy requires verification of completion of the personnel risk assessment.

➤ **Company policy not followed**

Example: An employee did not receive the required personnel risk assessment when hired, contrary to established company policy.

Suggested Enhancement: Ensure all hiring managers are properly trained, understand, and adhere to the company hiring policy.

R 3.1 The Responsible Entity shall ensure that each assessment conducted includes, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

➤ **Personnel Risk Assessment did not go back seven years**

Example: Entity's policy called for a personnel risk assessment going back five years and the entity was not able to update the personnel risk assessment with a seven year check before reaching the full compliance date.

Suggested Enhancement: Ensure the personnel risk assessment policy requires a seven-year criminal check and that sufficient time is allocated to complete the seven-year check for all personnel with authorized electronic and unescorted physical access to Critical Cyber Assets prior to reaching the full compliance date.

R 3.2 The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

➤ **Seven year update not completed**

Example 1: Entity discovered a number of personnel who had retained access without having updated their personnel risk assessment within the past seven years.

Example 2: Entity did not update the personnel risk assessment within seven years for a number of contractors.

Suggested Enhancement: Review records for existing employees, contractors, and vendor support staff to ensure the personnel risk assessment has been completed within the past seven years. Establish a suspense file to trigger a seven-year recheck in sufficient time to complete the assessment before the seven year expiration is reached. Federal agencies should consult with the Office of Personnel Management to determine if regulations permit a seven year criminal check and retain documentation of the determination.

R 3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

➤ **Missing/incomplete documentation**

Example 1: No record of a completed personnel risk assessment existed for a number of employees with authorized electronic access or unescorted physical access.

Example 2: Entity did not have 100% of the data, documents, documentation, logs, and records that would demonstrate to an auditor compliance with CIP-004 R3. For some individuals who were authorized to have cyber or unescorted physical access to Critical Cyber Assets in the past, there was no documentation evidencing the completion of Personnel Risk Assessments.

Example 3: Entity had a personnel screening policy for hiring and for determining who is granted access to secure areas. Documentation of the risk assessment was insufficient to meet this Standard.

Suggested Enhancement: Without disclosing any information protected under the Health Insurance Portability and Accountability Act (HIPAA), the Fair and Accurate Credit Transaction Act (FACTA), or any other federal, state, or provincial regulation, entities must be able to present documentation verifying that (1) the personnel risk assessment was performed for the staff in question and (2) all required elements of the personnel risk assessment have been included. Simply having a policy prescribing the personnel risk assessment is not sufficient.

All personnel, including contractors and vendor support staff, with authorized electronic or unescorted physical access to Critical Cyber Assets must have documentation on record. The contractor or vendor company can certify the personnel risk assessment was performed as long

as the certification is on company letterhead, is signed by an authorized official (senior manager or HR manager), asserts the checks performed for the named individual, when the assessment was completed, whether or not any adverse information was found, and includes some sort of evidence that the Personnel Risk Assessment was actually performed, such as an invoice or redacted report with the subject of the Personnel Risk Assessment identified.

The Responsible Entity should clearly document what it considers to be adverse information and make that information available to the contracted company's contact for completing and reporting the Personnel Risk Assessment results. If adverse information is found, it should be considered in the contracting decision. As this information is generally protected by federal, state, or provincial laws, the Responsible Entity may need to perform its own personnel risk assessment in order to obtain the details of the adverse information.

While it is appropriate to include the Personnel Risk Assessment requirement in the language of a contract, the Responsible Entity is ultimately responsible for ensuring the required checks are completed. Simply having language in a contract does not demonstrate compliance and similarly, not having language in a contract is not grounds for a finding of non-compliance. If the contracted company is unwilling or unable to provide the necessary documentation to enable the Responsible Entity to demonstrate compliance, the Responsible Entity will need to perform the vendor/contractor Personnel Risk Assessment itself.

R4 Access. The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

➤ **Missing or incomplete documentation**

Example 1: Entity had a list of authorized personnel; however the list was incomplete in that it did not cover all access rights to all Critical Cyber Assets.

Example: Entity did not update its list of personnel with authorized access when access rights were modified.

Example 2: Due to administrative errors, a number of contractor personnel were inadvertently placed on the list of personnel with unescorted physical access. The contractors in question did not, in fact, have access to the Critical Cyber Assets.

Example 3: Electronic and physical access was properly revoked for a retired employee; however the list of personnel with access was not updated within the seven days allowed for revoking access.

Example 4: The entity was unable to document the authorized electronic or unescorted physical access for all of the electronic and physical security perimeters prior to the full compliance date.

Example 5: The entity could produce a list of the personnel with authorized electronic and unescorted physical access; however the list did not include the specific access rights granted.

Suggested Enhancement: An entity has an option to rely upon the access control systems to produce the list of authorized access and the specific access rights, rather than manually maintaining a master list. If this option is implemented, entities need to be aware of the following risks:

- Each system must be queried to ensure all access is identified for revocation or review.
- The access control system must be able to produce a date-stamped transaction log to demonstrate changes and revocations are completed within the required timeframes.
- Evidence of access authorization is required and may need to continue to be supported by a separate process or system.

If a master list is also maintained, ensure the applicable policies and procedures document the requirement to update the master list and ensure all personnel responsible for managing access rights are properly trained and adhere to the procedures.

Verify that all Critical Cyber Assets are covered by the reports regardless of the source.

➤ **Inaccurate documentation of access**

Example: The entity's master list was not complete. As a result, certain personnel had access unbeknown to the entity.

Suggested Enhancement: Consider relying upon the access control systems to produce the list of authorized access and the specific access rights instead of manually maintaining a master list. If relying upon the access control system, be aware of the risks previously discussed, including the need to demonstrate the access was properly approved. Often a workflow tool, such as an automated help desk utility, is very helpful for demonstrating authorization. Manual (paper) authorization documentation may also be appropriate for the smaller entity with limited access to manage. If a master list is also maintained, regularly reconcile the master list and the authorization records against the access control systems to ensure the master list is accurate and all access granted is properly authorized.

➤ **Not all access modes were documented**

Example: The entity failed to consider all modes of physical access. As a result, personnel with emergency key access were not documented.

Suggested Enhancement: Evaluate all means for entering the Physical Security Perimeter, including ways to bypass the access control systems. Types of uncontrolled access include maintenance or janitorial staff with keys and personnel with access to a key in an emergency. Implement a key control program to ensure that:

- anyone with key access is identified;
- keys cannot be replicated except as authorized by the Responsible Entity; and
- keys are retrieved from the employee, contractor, or vendor support staff upon termination or other revocation of access.

Finally, change locks immediately if keys are lost, stolen, or cannot be accounted for.

➤ **Improper access management processes**

Example: Entity policy and procedure did not prohibit badge cloning. As a result, certain access was granted by inheritance from the clone source record without authorization.

Suggested Enhancement: Update access management policies and procedures to specifically prohibit physical or electronic access cloning. Ensure all personnel managing access are trained, understand, and comply with the anti-cloning policy.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

➤ **Quarterly access review not performed**

Example: The entity did not have a complete list of personnel with access and their access rights. As a result, the entity has not performed the required quarterly review.

Suggested Enhancement: Establish a regular schedule for performing the quarterly review. Ensure all documentation is maintained and available as required by CIP-004-1, Requirement R4.

R4.2 The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

➤ **Failure to remove access within the required timeframe**

Example 1: Automated processes to revoke access failed and access was not revoked within the required timeframe.

Example 1: Entity did not retrieve physical access cards in all cases when revoking physical access.

Example 3: Access control system administrator removed the wrong access and there were no checks and balances to detect the entry error.

Example 4: Due to an overload of transactions following a merger, a number of personnel did not have their access revoked within the required seven-day period.

Example 5: Entity failed to update the master access list when personnel terminated and access was revoked.

Suggested Enhancement: Include a verification step in the revocation process to ensure automated access management processes are working properly. Introduce a verification step for manual revocation processes to ensure the correct access is revoked. Ensure access revocation and modification notices are sent at the time of termination or transfer and that the requested revocation actions are promptly performed. If a master access list is being maintained, ensure the master list is updated at the time access is revoked or modified.

➤ **Missing or incomplete documentation**

Example: The entity did not have the evidence necessary to demonstrate access was revoked in the required timeframe.

Suggested Enhancement: Ensure automated systems are capable of producing historical transaction logs for the entire audit period or that the transaction logs are periodically archived. Ensure manual logs are dated and signed and retained for the entire audit period.

➤ **Policy/Procedure deficiency**

Example 1: Internal entity processes were not updated to revoke access within seven days upon transfer of personnel.

Example 2: Manual termination process did not trigger an access revocation request, thus access was not removed within the required time frame.

Suggested Enhancement: Ensure the personnel policies and procedures include the necessary steps to initiate access revocation within the required time frame. Certain access management staff should be notified in advance of a termination for cause whenever possible to allow time for preparation. Notices to revoke access should be issued at the same time the termination for cause takes place such that access is revoked before the terminated staff departs the facility following the termination action.

4. Conclusion

Unless approved protocols and procedures are in place, personnel with physical or electronic access to Critical Cyber Assets can pose a significant risk to the reliability and availability of the key cyber systems essential to the reliability of the bulk electric system. To mitigate that risk, it is imperative that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

Registered entities need to be particularly diligent when it comes to revocation of access. There have been numerous incidents, including known incidents within the electric utility industry, where failure to promptly terminate both physical and electronic access to an entity's Cyber Assets has resulted in a successful malicious attack by a disgruntled former employee or contractor. In one recent attack, a disgruntled contract system administrator was able to gain physical access after being terminated for cause, shutting down key business systems but luckily not shutting down critical grid reliability systems. The entity had properly terminated electronic access when the contractor was terminated, but failed to revoke physical access.

As the CMEP matures and Registered Entities, particularly those who have had little experience with formal compliance programs, become more familiar with the program it is expected that

compliance to the CIP-004 Reliability Standard will improve as long as the Registered Entities, NERC, and the Regional Entities are rigorous in their pursuit of an effective compliance program, culture and awareness to the sensitivity of Critical Cyber assets.

SUMMARY OF REQUIREMENTS AND SUGGESTIONS

This Summary is intended to capture the foregoing discussion by listing the essential elements of the requirements, and by offering some suggestions for consideration. It is not a complete list of all possible actions; undertaking such actions does not guarantee compliance. This is included for informational purposes only.

- 1) Awareness of Security
 - a) Document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
 - b) The awareness program needs to be conducted at least quarterly.
 - c) The awareness program can use such mechanisms as:
 - i) Direct communications (e.g., emails, memos, computer based training, etc.);
 - ii) Indirect communications (e.g., posters, intranet, brochures, etc.);
 - iii) Management support and reinforcement (e.g., presentations, meetings, etc.).

- 2) Cyber Security Training
 - a) Establish a cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets.
 - b) Ensure the training program is conducted annually
 - c) The program must be reviewed annually and updated as necessary.
 - d) The program must require documentation that training has been completed by all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. "All personnel" includes:
 - i) Employees
 - ii) Contractors
 - iii) Vendor support staff
 - e) Training records need to identify each person receiving training and the date training was completed.
 - f) Training must be conducted within 90 days of granting access, whether or not access is temporary and less than 90 days. Once version 2 of the Standards is approved and enforceable, training must be completed **before** access is granted.
 - g) Training must cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004.
 - h) Training must include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
 - i) The proper use of Critical Cyber Assets;
 - ii) Physical and electronic access controls to Critical Cyber Assets;
 - iii) The proper handling of Critical Cyber Asset information; and,
 - iv) Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.
 - i) Training can be computer based, self-paced, or classroom based.
 - j) Records can be paper based (class rosters, signed assertions of completion, completion certificates) or electronic (computer based training completion logs).

- 3) Personnel Risk Assessment
- a) Implement and document a personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access.
 - b) The personnel risk assessment must be conducted within 30 days of granting access, whether or not access is temporary and less than 30 days. Once version 2 of the Standards is approved and enforceable, the personnel risk assessment must be completed **before** access is granted.
 - c) The personnel risk assessment must include identity verification and a seven-year criminal history check. The personnel risk assessment may include additional requirements per the Responsible Entity's company policy, however there is no requirement that the additional requirements be completed before access is granted for CIP-004 compliance purposes.
 - d) The personnel risk assessment must be performed every seven years.
 - e) The personnel risk assessment must be performed sooner than seven years if there is cause to do so. The personnel risk assessment program should define what constitutes cause.
 - f) The Responsible Entity can rely upon the contractor/vendor company to perform the personnel risk assessment under the following conditions:
 - i) The Responsible Entity retains documentation of the contractor/vendor personnel risk assessment program.
 - ii) The program implemented by the contractor/vendor meets the minimum requirements of the Standard.
 - iii) The contractor/vendor provides documentation that each individual authorized for access to the Responsible Entity's Critical Cyber Assets has had a personnel risk assessment performed. This documentation must include the employee's identity, the date of the assessment and whether or not adverse information was found.
 - g) The Responsible Entity must maintain documentation that the personnel risk assessment has been completed by all personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets. All personnel includes, but is not limited to:
 - i) Employees
 - ii) Contractors
 - iii) Vendor support staff
 - h) The documentation needs to demonstrate that the personnel risk assessment was performed for the person in question. Documentation should not disclose personal information subject to regulatory protections. Examples of documentation include:
 - i) Invoice from a third-party service performing the personnel risk assessment.
 - ii) Redacted report of the personnel risk assessment results.
 - iii) Attestation from the vendor or contractor company that the personnel risk assessment was performed for each named contract or vendor support staff person, including the date the assessment was performed and whether or not adverse information was found.
 - i) If the Responsible Entity relies upon the contractor/vendor to conduct personnel risk assessments of their staff and adverse information is found, the Responsible Entity may have to repeat the personnel risk assessment itself in order to be able to make an informed decision on whether to grant access.

- 4) Personnel Access to Critical Cyber Assets
- a) The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
 - b) Access rights documentation needs to be specific. For example:
 - i) Specific electronic access rights for a specific Critical Cyber Asset.
 - ii) Specific physical access rights such as which doors can be entered and at what times.
 - iii) The employee, contractor, or vendor support staff possessing the access rights. Note that use of group membership to define access rights for an individual is permitted.
 - c) The access authorization records can be maintained by the Critical Cyber Asset or the physical access control system itself as long as add/update/delete transactions are logged and can be produced as required to evidence compliance.
 - d) The access list(s) must be updated within seven days of an authorized change, including revocation of access no longer needed.
 - e) The access list(s) must be reviewed quarterly (every three months) to ensure all granted access is authorized and still required.
 - f) Access must be revoked within 24 hours for any person terminated for cause.
 - g) For all other personnel, access must be revoked within seven days of termination or other reason access is no longer required.