NIST Example Augmentation of Standard CIP–005

Cyber Security — Cyber Security Perimeter Protection

October 7, 2008

========== General comments ==========

Discussion (set off by "======" and colored blue) is not part of the NIST augmentation. It is provided to assist the drafting committee.

Order 706 ¶ 61 gives the ERO direction to provide additional guidance in the CIPs or in a separate reference document. For convenience, the guidance is placed in this manuscript. This guidance is part of NIST's augmentation.

==========

A. Introduction

1. Title: Cyber Security — ~~Electronic~~ Cyber Security Perimeter~~(s)~~ (CSP) Protection

2. Number: CIP-005-~~1~~2

3. Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009~~ using reasonable business judgment~~.

4. Applicability

4.1. [4.1] Within the text of Standard CIP-005, "Responsible Entity" shall mean all entities that could affect the reliability of the bulk electric grid by virtue of cyber connection to any control system component of the bulk electric system.. Responsible Entities include, but are not limited to:

==========

NIST recommends that all entities that could affect the reliability of the bulk electric grid should be included. Advances in digital electronics technology and computer hardware and software have obsoleted prior distinctions among computing, communications, and control systems. Today, all are collectively considered Information Technology (IT). Until recently, Industrial Control Systems (ICS) had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the Responsible Entity's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

The interconnection of infrastructures has obsoleted prior distinctions. Distribution Systems and Energy Management Systems should be included. Enumeration can be helpful as examples, providing the enumeration states "including, but not limited to."

==========

- Reliability Coordinator.
- Balancing Authority.
- Interchange Authority.
- Transmission Service Provider.

- Transmission Owner.
- Transmission Operator.
- Generator Owner.
- Generator Operator.
- Load Serving Entity.
- NERC.
- Regional Reliability Organizations.

4.2. [4.2] The following are exempt from Standard CIP-005:

4.2.1 [4.2.1] Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.

==========

NIST notes that on September 18, 2008 FERC issued the following Proposed Clarification: facilities within a nuclear generation plant in the United States that are not regulated by the U.S. Nuclear Regulatory Commission are subject to compliance with the eight mandatory "CIP" Reliability Standards approved in Commission Order No. 706.

==========

4.2.2 [4.2.2] Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters that are not under the direct control and management of the Responsible Entity..

4.2.3 [4.3.3] Responsible Entities that, in compliance with Standard CIP-002, identify that they have no Critical Cyber Assets.

5. Effective Date: ~~June 1, 2006~~TBD

~~5.~~6. Exceptions

==========

In Order No. 706 FERC directed the development of a framework to provide accountability when a Responsible Entity relies on technical infeasibility or certain other factors to take exception to specific Requirements. FERC specified that the structural elements of this framework include mitigation steps, a remediation plan, a timeline for eliminating use of the technical feasibility exception unless appropriate justification otherwise is provided, regular review of whether it continues to be necessary to invoke the exception, internal approval by the senior manager, wide-area approval through the ERO's audit process, and cooperation with the ERO to provide the Commission with high-level, wide-area analysis regarding the effects the technical feasibility exception on the reliability of the Bulk-Power System. See ¶ 152, 157-163, 178-187, 192-195, and 209-222.

==========

6.1. The Responsible Entity may take exception to any Requirement based on the Responsible Entity's determination that any of the following conditions apply:

- The Requirement interferes with ICS functions
- The Requirement poses a risk to the reliability of the bulk electric grid
- The ICS cannot support the use of the required mechanisms or implement the required function
- The Requirement will have a significant adverse impact on performance, safety, or reliability

6.2. The Responsible Entity shall document all exceptions in an Exception Plan provided to the ERO and Regional Reliability Organization containing:

6.2.1 A convincing argument why the exception is necessary

6.2.2 Compensating controls or mitigation steps to address the intent of the Requirement

6.2.3 A plan of action, milestones, and schedule for implementing the compensating controls or mitigation steps

6.3. The Exception Plan must be approved annually by a Responsibility Entity senior manager.

6.4. The Exception Plan must be approved annually by the Regional Reliability Organization, or the ERO if there is no applicable RRO.

6.5. The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

B. Requirements

The Responsible Entity shall comply with the following requirements of Standard CIP-005:

==========

Information may be stored, transmitted, and processed using multiple digital and analog media including electro-magnetic fields in space on media in frequencies commonly described as electrical and optical. For example, fiber optic, infrared, and radio wireless communications are all common, but are not "electronic." NIST believes that "Electronic" is too limited a term and has replaced it with "Cyber" as being more inclusive. "Logical" is another term that could be used.

==========

R0. Cyber Security Perimeter Policy and Procedures — The Responsible Entity shall: develop, disseminate, and periodically review and update: (i) a formal, documented, policy on the protection of all Cyber Security Perimeter(s), the cyber assets contained within, and identification and authentication. This policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among Responsible Entity's sub-entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of this policy and associated controls.

GUIDANCE: This requirement does not prescribe an organization structure for the Responsible Entity 's cyber security policy. The Cyber Security Perimeter Policy and Procedures may be included as part of the general information security policy for the Responsible Entity, or the ICS cyber security policy.

========== based on AC-1 & IA-1 ==========

~~R0.~~**R1.** [R1] ~~Electronic~~ Cyber Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within a~~n Electronic~~ Cyber Security Perimeter. The Responsible Entity shall identify and document the ~~Electronic~~ Cyber Security Perimeter(s) and all access points to the perimeter(s).

~~R0.1.~~**R1.1.** [R1.1] Access points to the ~~Electronic~~ Cyber Security Perimeter(s) shall include any externally connected communication ~~end~~ interface point (for example, dial-up modems) terminating at any device at ~~within~~ the ~~Electronic~~ Cyber Security Perimeter(s).

==========

The concept of logically locating the modem at the Perimeter eliminates the need to physically protect the circuit between the modem and the Perimeter, as required in CIP-006.

==========

~~R0.2.~~R1.2. [R1.2] For a dial-up accessible Critical Cyber ~~Asset that~~Asset that uses a non-routable protocol, the Responsible Entity shall define an ~~Electronic~~ Cyber Security Perimeter for that single access point at the dial-up device or shall include the Asset within a defined Cyber Security Perimeter.~~.~~

~~R0.3.~~R1.3. [R1.3] Communication links that are not under the direct control and management of any Responsible Entity connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, ~~end~~ interface points of these communication links ~~within~~ at the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

==========

The interface between assets controlled by the Responsible Entity and assets controlled by another party is not necessarily the end point for communication. The interface may simply be the demarcation between two domains of responsibility and may also provide changes in information representation or addressing (e.g., optical to electronic, network access translation (NAT)).

==========

~~R0.4.~~R1.4. [R1.4] Any non-critical Cyber Asset within a defined ~~Electronic~~ Cyber Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

~~R0.5.~~R1.5. [R1.5] Cyber Assets used in the access control and monitoring of the ~~Electronic~~ Cyber Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

~~R0.6.~~R1.6. [R1.6] The Responsible Entity shall maintain documentation of ~~Electronic~~ Cyber Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

GUIDANCE: Any connections to the Internet, or other external networks, communication systems, cyber assets, or information systems that are not under the control of the Responsible Entity, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber assets at any designated alternate processing sites are provided the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact cyber assets into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with the Responsible Entity's assessment of risk .

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are

commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the Responsible Entity implements appropriate compensating security controls.

========== guidance based on SC-7 ==========

R1.7. The Responsible Entity physically allocates publicly accessible cyber assets to separate subnetworks with separate, physical network interfaces.

GUIDANCE: Publicly accessible cyber assets include, for example, emergency cut-off activators. Generally, public access to ICS information is not permitted.

========== based on SC-7 control enhancement 1 Appx F & I==========

R1.8. The Responsible Entity shall prevent public access into the Responsible Entity's internal networks except as appropriately mediated.

========== based on SC-7 control enhancement 2 ==========

~~R0.7.~~**R1.9.** The Responsible Entity shall limit the number of access points to the Cyber Security Perimeter to allow for better monitoring of inbound and outbound network traffic.

========== based on SC-7 enhancement 3 ==========

~~R0.8.~~**R1.10.** The Responsible Entity shall implement a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

========== based on SC-7 enhancement 4 ==========

~~R1.~~**R2.** [R2] ~~Electronic~~ Cyber Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of ~~electronic~~ cyber access at all ~~electronic~~ cyber access points ~~to~~ at the ~~Electronic~~ Cyber Security Perimeter(s)~~.~~, and at key internal boundaries within the Cyber Security Perimeter(s).

~~R1.1.~~**R2.1.** [R2.5] The required documentation shall, at least, identify and describe:

~~R1.1.1.~~**R2.1.1.** [R2.5.1] The processes for access request and authorization.

~~R1.1.2.~~**R2.1.2.** [R2.5.2]The authentication methods.

~~R1.1.3.~~**R2.1.3.** [R2.5.3] The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

~~R1.1.4.~~**R2.1.4.** [R2.5.4] The controls used to secure dial-up accessible connections.

GUIDANCE: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Cyber security boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the Responsible Entity considers partitioning higher-impact information systems into separate physical domains (or

environments) and applies the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an Responsible Entity's assessment of risk.

The Responsible Entity carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions.

========== based on SC-7 ==========

~~R1.2.~~R2.2. [R2.1] These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.3. [R2.3] The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s). The Responsible Entity shall:

R2.3.1. Employ automated mechanisms to facilitate the monitoring and control of dial-up access.

R2.3.2. Determine if cryptography is required to protect the confidentiality and integrity of dial-up access sessions.

R2.3.3. Permit dial-up access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: The Responsible Entity restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Dial-up access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of dial-up access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication, dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity).

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful

consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications===

~~R1.3.~~R2.4. The Responsible Entity shall authorize and document all connections between cyber assets inside the Cyber Security Perimeter and cyber assets outside of the Cyber Security Perimeter.

GUIDANCE: The Responsible Entity carefully considers the risks that may be introduced when cyber assets are connected to other cyber assets with different security requirements and security controls, both within the Responsible Entity and external to the Responsible Entity. Risk considerations also include cyber assets sharing the same networks.

========== additions based on CA-3 ==========

~~R1.4.~~R2.5. [R2.4] Where ~~external interactive~~ access through ~~into~~ the ~~Electronic~~ Cyber Security Perimeter has been authorized and enabled, the Responsible Entity shall implement multifactor ~~strong~~ procedural or technical controls at the access points to ensure authenticity of the accessing ~~party~~parties, ~~where technically feasible~~and monitors/controls the access on an ongoing basis.

GUIDANCE: Multifactor authentication is a system wherein more than one different factors are used to authenticate, thereby delivering a higher level of authentication assurance. Using more than one factor is sometimes called strong authentication.

========== based on IA-2 control enhancement 1 ==========

R2.6. The Responsible Entity shall:

R2.6.1. Employ automated mechanisms to facilitate the monitoring and control of remote access methods.

R2.6.2. Determine if cryptography is required to protect the confidentiality and integrity of remote access sessions.

R2.6.3. Control all remote accesses through a limited number of managed access control points.

R2.6.4. Permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the Cyber Security Perimeter .

GUIDANCE: Remote access is any access to an Cyber Security Perimeter by a user (or a cyber asset) communicating through an external network not under the control of the Responsible Entity (e.g., the Internet, public switched telephone network). Examples of remote access methods include dial-up, broadband, and wireless. The Responsible Entity protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special

Publication 800-63 provides guidance on remote electronic authentication. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks.

Remote access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Cryptography is used for the protection of information and communications. At the core of all products offering cryptographic services is the cryptographic module. Weaknesses such as poor design or weak algorithms can render a product insecure and place highly sensitive information at risk. Adequate testing and validation of the cryptographic module and its underlying cryptographic algorithms against established standards is essential to provide security assurance.

The NIST Cryptographic Module Validation Program (CMVP) validates commercial cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards such as algorithms.

ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the Responsible Entity considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel).

==== based on AC-17, IA-7 Appx F&I and other NIST publications====

R2.7. The Responsible Entity shall:

R2.7.1. Develop a list of privileged functions

R2.7.2. Develop a list of authorized actions that can be taken with respect to privileged functions

~~**R1.4.1.**~~**R2.7.3.** Document the criteria and procedures for granting authorization to identified persons and entities.

The Responsible Entity shall manage cyber asset accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Privilege authorizations shall be granted in accordance with established policy and recorded. The Responsible Entity shall determine and implement the frequency for reviewing said accounts, at least annually.

GUIDANCE: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The Responsible Entity identifies authorized users of the cyber assets and specifies access rights/privileges. The Responsible Entity grants access to the cyber assets based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended usage. The Responsible Entity requires proper identification for

requests to establish accounts and approves all such requests. The Responsible Entity specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when cyber asset users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' cyber asset usage or need-to-know/need-to-share changes.

==========requirement and guidance based on AC-2 ==========

~~R1.5.~~R2.8. The cyber assets shall enforce assigned authorizations for controlling access in accordance with applicable policy.

GUIDANCE: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) within the cyber security perimeter. In addition to controlling access at the network layer of the ISO Reference Architecture, access enforcement mechanisms are employed at the application layer, when necessary, to provide increased information security. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events.

The Responsible Entity ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.6.~~R2.9. The cyber assets shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

GUIDANCE: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Within ICS, it is commonly the case that having access to specific devices (e.g., workstations, remote terminal units, field devices) is the equivalent to having privileged access; thereby restricting access to these devices is also restricting access to privileged functions and security-relevant information.

========== requirement & guidance based on AC-3 Appx F & I ==========

~~R1.7.~~R2.10. The Responsible Entity shall specify privileged functions that have impacts on facility, public, and environmental safety that require dual authorization.

GUIDANCE: The Responsible Entity does not employ dual-approval mechanisms when an immediate response is necessary to ensure public and environmental safety.

========== requirement & guidance based on AC-3 ICS-1 ==========

~~R1.8.~~R2.11. The cyber assets shall enforce assigned authorizations for controlling the flow of information within the Cyber Security Perimeter and between interconnected Cyber Security Perimeters in accordance with applicable policy.

GUIDANCE: Information flow control regulates where information is allowed to travel within a Cyber Security Perimeter and between Cyber Security Perimeters (as

opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the Responsible Entity, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by Responsible Entities to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within Cyber Security Perimeters and between interconnected Cyber Security Perimeters. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

========== requirement & guidance based on AC-4 ==========

~~R1.9.~~R2.12. The Responsible Entity shall identify roles and responsibilities where separation of duties is necessary. The cyber assets enforces separation of duties through assigned access authorizations.

GUIDANCE: The Responsible Entity establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the cyber assets that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct support functions are divided among different individuals/roles; (ii) different individuals perform cyber asset support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. In situations where the ICS cannot support the differentiation of roles or a single individual performs all roles within the ICS, the Responsible Entity shall employ appropriate compensating controls (e.g., providing increased personnel security and auditing measures).

========== requirement & guidance based on AC-5 Appx F&I ==========

R2.13. The Responsible Entity shall:

R2.13.1. Approve individual access privileges and enforce cyber access restrictions associated with changes to the critical cyber assets

~~R1.9.1.~~R2.13.2. Generate, retain, and review records reflecting all such changes.

GUIDANCE: Planned or unplanned changes to the hardware, software, and/or firmware components of the cyber assets can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications. In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

======== based on CM-5 from Appendixes F & I ==========

~~R1.10.~~R2.14. [R2.2] At all access points to the ~~Electronic~~ Cyber Security Perimeter(s) and at all Cyber Assets contained within the Perimeter, the Responsible Entity ~~shall enable~~shall enable only ports, functions, capabilities, and/or ~~services required~~services required for operations- ~~and for~~ including monitoring Cyber Assets within the ~~Electronic~~ Cyber Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports, functions, capabilities, and services.

GUIDANCE: Cyber Assets are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential Responsible Entity operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of a Cyber Asset, but doing so increases risk over limiting the services provided by any one component. The Responsible Entity limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by Cyber Assets, or individual components of Cyber Assets, should be carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

========== additions to requirement based on CM-7 ==========

R2.15. The Responsible Entity shall define and the cyber assets shall automatically enforce:

R2.15.1. A limit of consecutive invalid access attempts by a user during a specified time period, and restrictions on further accesses including

R2.15.2. A defined time period to lock the account, preventing access

~~R1.10.1.~~**R2.15.3.** A defined time period and algorithm to delays next login prompt.

GUIDANCE: Due to the potential for denial of service, automatic lockouts initiated by the cyber assets are usually temporary and automatically release after a predetermined time period established by the Responsible Entity.

In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting security personnel though alarms or other means when the number of Responsible Entity-defined consecutive invalid access attempts is exceeded).

========== additions to requirement based on AC-7 Appx F & I ==========

~~R1.11.~~R2.16. The Responsible Entity shall define an interval of user inactivity after which the cyber assets shall initiate a session lock. The session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

GUIDANCE: Users can directly initiate session lock mechanisms. The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after a time period defined by the Responsible Entity for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures)

========== additions based on AC-11 Appx F & I ==========

~~R1.12.~~R2.17. For remote access sessions, the Responsible Entity shall define an interval of user inactivity after which the cyber assets shall automatically terminate the session.

GUIDANCE: In situations where the ICS cannot support the automatic termination of remote sessions after a specified period of inactivity, or the ICS cannot automatically terminate remote sessions due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls (e.g., providing increased auditing measures for such sessions or limiting remote access privileges to key personnel).

========== based on AC-12 Appx F & I ==========

~~R1.13.~~R2.18. The Responsible Entity shall identify and document specific user actions that can be performed on the cyber assets without identification or authentication.

GUIDANCE: Emergency switches to stop operations are accessible to any individual with authorized physical access.

========== based on AC-14 ==========

~~R1.14.~~R2.19. [R2.6] Appropriate Use Banner — ~~Where technically feasible, electronic a~~Access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The banner shall inform potential users: (i) that the user is accessing a private system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The banner shall provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on. The Responsible Entity shall maintain a document identifying the content of the banner.

========== additions to requirement based on AC-8 ==========

~~R2.~~R3. [R3] Monitoring ~~Electronic~~ Cyber Access — The Responsible Entity shall define, periodically review, and update, a list of auditable events and uses that list to generate audit records. The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging audit records for these events ~~access at access points to the Electronic Security Perimeter(s)~~twenty-four hours a day, seven days a week.

========== additions to requirement based on AU-2 ==========

GUIDANCE: The purpose of monitoring and logging audit records is to identify important events which need to be audited as significant and relevant to the reliability of the bulk electric grid. The Responsible Entity specifies which events require auditing and how the audition is implemented. Auditing activity can affect system performance. Therefore, the Responsible Entity decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The Responsible Entity defines auditable events that are adequate to support after-the-fact investigations of security incidents. Most auditing occurs at the application level. In situations where the Responsible Entity cannot support the use of automated mechanisms to generate

audit records, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls

========== based on AU-2 Appendix F & I ==========

~~R2.1.~~R3.1. Cyber assets shall produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Cyber assets shall provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

GUIDANCE: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

========== based on AU-3 ==========

~~R2.2.~~R3.2. The Responsible Entity allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

========== based on AU-4 ==========

~~R2.3.~~R3.3. The Responsible Entity shall define actions to be taken in the event of an audit processing failure (e.g., overwrite oldest audit records, stop generating audit records). Cyber assets that perform auditing shall alert appropriate Responsible Entity officials and take these actions in the event of an audit processing failure.

GUIDANCE: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including response to audit failures, the Responsible Entity employs compensating controls (e.g., providing an auditing capability on a separate information system).

========== requirement based on AU-5 Appx F & I ==========

~~R2.4.~~R3.4. [R3.1] For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device~~, where technically feasible.~~.

~~R2.5.~~R3.5. [R3.2] ~~Where technically feasible, t~~The Responsible Entity's security monitoring process(es) shall regularly review/analyze audit records with respect to the enforcement and usage of cyber asset access controls for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel who take necessary actions. The Responsible Entity shall employ automated mechanisms to facilitate the review of user activities. If the Responsible Entity takes an exception to ~~Where~~ alerting ~~is not technically feasible~~as specified in section A.6, the Responsible Entity shall review or otherwise assess ~~access logs~~audit records for attempts at or actual unauthorized ~~accesses~~ activities at least every ninety calendar days.

GUIDANCE: The Responsible Entity reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with Responsible Entity procedures. The Responsible Entity investigates any unusual cyber asset-related activities and periodically reviews changes to access authorizations. The Responsible Entity reviews more frequently the activities of users with significant cyber asset roles and

responsibilities. In situations where the ICS cannot support the use of automated mechanisms for reviewing user activities, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

Responsible Entities increase the level of audit monitoring and analysis activity within the system whenever there is an indication of increased risk based on law enforcement information, intelligence information, or other credible sources of information.

========== based on AC-13 Appx F & I and AU-6 ==========

~~R2.6.~~R3.6. The Responsible Entity shall define a list of inappropriate or unusual activities with security implications that are to result in automated alerts that shall be sent to designated security personnel.

========== requirements based on AU-6 ==========

R3.7. The Responsible Entity shall provide an audit reduction and report generation capability. The audit reduction and report generation system shall provide the capability to automatically process audit records for events of interest based upon selectable, event criteria..

GUIDANCE: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records. In general, audit record processing is not performed on the Critical Cyber Asset, but on a separate cyber asset.

========== based on AU-7 Appx F & I ==========

~~R2.7.~~R3.8. The Responsible Entity shall employ time stamps in audit record generation. The Responsible Entity shall define the frequency for synchronizing internal clocks. The cyber assets shall synchronize internal system clocks at this frequency.

GUIDANCE: Time stamps (including date and time) of audit records are generated using internal system clocks.

========== requirement based on AU-8 ==========

~~R2.8.~~R3.9. The Responsible Entity shall protect audit information and audit tools from unauthorized access, modification, and deletion.

GUIDANCE: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity

========== based on AU-9 ==========

R4. -Cyber Security Perimeter Assessment — The Responsible Entity shall establish a program to assess the security of the Cyber Security Perimeter.

R4.1. The Responsible Entity shall develop detailed Cyber Security Perimeter testing standards, processes, and procedures (called "CSP Security Assessment Guide") to provide direction and guidance on security testing; the Guides must:

R4.1.1. Identify who is to be held accountable and responsible for ensuring that information security tests comply with Responsible Entity requirements.

R4.1.2. Identify the Responsible Entity requirements with which security tests must comply, i.e., test scenarios must map to and support security requirements, must specify the minimum set of security controls evaluated during tests, as well as the depth and breadth of tests.

R4.1.3. Specify the appropriate roles and responsibilities, i.e., there must be well-qualified personnel in both security testing and analysis, and care must be

taken to ensure separation of duties when testing; for example, testing and analysis must be performed by an independent person(s).

R4.1.4. Adhere to established methodology that identify and test for security controls for the types of testing being performed, viz., NIST guidelines describe these methods as interview, examine and test.

R4.1.5. Specify a testing environment and criteria to be added per NIST SP 800-53A and SP 800-115 and describe these methods, such as the use of dedicated test equipment that must be used for security testing.

R4.1.6. State the frequency of assessmentswhen and how often testing is to be performed.

R4.1.7. Provide the documentation requirements, such as test plans and test results; i.e., adequately securing the results and analysis information and artifacts from testing.

R4.1.8. Specify the criteria for the analysis of the tests and the dissemination of results and recommendations.

R4.1.9. Develop a plan of action, milestones, and schedule to correct deficiencies found during testing.

~~**R2.9.**~~**R4.2.** [R4] Cyber Vulnerability Assessment — The Responsible Entity shall employ a qualified independent agent or team to conduct assessment of (a) ~~perform a~~ cyber vulnerabilities ~~y assessment~~ of the ~~electronic~~ access points to the ~~Electronic~~ Cyber Security Perimeter(s)~~-~~ at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported.. The vulnerability assessment shall be conducted in accordance with the CSP Security Assessment Guide. The vulnerability assessment shall include, at a minimum, the following:

========== based on CA-4 and RA-5 ==========

~~**R2.9.1.**~~**R4.2.1.** [R4.1] A document identifying the vulnerability assessment process;

~~**R2.9.2.**~~**R4.2.2.** [R4.2] A review to verify that only ports and services required for operations at these access points are enabled;

~~**R2.9.3.**~~**R4.2.3.** [R4.3] The discovery of all access points to the ~~Electronic~~ Cyber Security Perimeter;

~~**R2.9.4.**~~**R4.2.4.** [R4.4] A review of controls for default accounts, passwords, and network management community strings; ~~and,~~

~~**R2.9.5.**~~**R4.2.5.** [R4.5] Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

========== based on CA-4 ==========

GUIDANCE: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The Responsible Entity trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with Responsible Entity policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the Responsible Entity to help eliminate similar vulnerabilities in other cyber assets. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code).

Vulnerability scanning tools are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the Responsible Entity cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct scanning)

========== guidance based on RA-5 Appx F & I ==========

~~R2.10.~~R4.3. Cyber Control Assessment - The Responsible Entity shall employ a qualified independent agent or team to conduct an assessment of the implementation of all the cyber security controls in the Cyber Security Perimeter at least annually, or when significant new vulnerabilities potentially affecting the cyber assets are identified and reported. The implementation assessment shall -determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. The implementation assessment shall be conducted in accordance with the CSP Security Assessment Guide.

~~R3.~~R5. [R5] Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.

R5.1. The Responsible Entity shall develop, document, and maintain a current inventory of the cyber assets in the Cyber Security Perimeter and relevant ownership information. The Responsible Entity shall update the inventory of cyber assets as an integral part of component installations.

GUIDANCE: The Responsible Entity determines the appropriate level of granularity for the cyber asset components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of cyber asset components includes any information determined to be necessary by the Responsible Entity to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the Cyber Security Perimeter.

========== based on CM-8 ==========

R5.2. The Responsible Entity shall develop, document, and maintain a current baseline configuration of all the cyber assets in the Cyber Security Perimeter.

GUIDANCE: This requirement establishes a baseline configuration for the cyber assets. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the cyber assets architecture. The baseline configuration also provides the Responsible Entity with a well-defined and documented specification to which the cyber assets are built and deviations, if required, are documented in support of mission needs/objectives.

========== based on CM-2 ==========

R5.3. [R5.1] The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect the current ~~configurations~~baseline configurations and processes and

shall review the documents and procedures referenced in Standard CIP-005 at least annually.

========== based on CM-2 ==========

R5.4. The Responsible Entity shall:

R5.4.1. Authorize, document, and control changes to the cyber assets in the Cyber Security Perimeter.

R5.4.2. Test, validate, and document changes (e.g., patches and updates) before implementing the changes on the operational CSP.

~~R3.1.1.~~**R5.4.3.** Employ automated mechanisms to: (i) document proposed changes to the cyber assets; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the cyber assets.

GUIDANCE: The Responsible Entity manages configuration changes to the information system using an Responsible Entity-approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The Responsible Entity includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The Responsible Entity audits activities associated with configuration changes to the information system.

The Responsible Entity ensures that testing does not interfere with ICS functions. The individual/group conducting the tests fully understands the Responsible Entity information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an ICS must be taken off-line for testing, the tests are scheduled to occur during planned ICS outages whenever possible. In situations where the Responsible Entity cannot, for operational reasons, conduct live testing of a production ICS, the Responsible Entity employs compensating controls (e.g., providing a replicated system to conduct testing).

In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the Responsible Entity employs nonautomated mechanisms or procedures as compensating controls.

========== based on CM-3 ==========

~~R3.2.~~**R5.5.** [R5.2] The Responsible Entity shall update the documentation to reflect the modification of the cyber assets in the Cyber Security Perimeter~~network or controls~~ within ninety calendar days of the change.

R5.6. The Responsible Entity shall:

R5.6.1. Establish mandatory configuration settings for cyber assets employed within the Cyber Security Perimeter

R5.6.2. Configure the security settings of cyber assets to the most restrictive mode consistent with operational requirements

R5.6.3. Document the configuration settings

R5.6.4. Enforce the configuration settings in all cyber assets

R5.6.5. Employ automated mechanisms to centrally manage, apply, and verify configuration settings. In situations where the cyber assets cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the Responsible Entity shall employ nonautomated mechanisms or procedures as compensating controls.

==========requirement based on CM-6 Appx F & I ==========

~~R3.3.~~R5.7. [R5.3] The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.

R6. Identification and Authentication — The Responsible Entity shall maintain identification and authentication to support access control.

~~R3.4.~~R6.1. The Responsible Entity shall require critical cyber assets to uniquely identify and authenticate users (or processes acting on behalf of users).

GUIDANCE: Authentication is the process of establishing confidence in user identities presented. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Human authentication factors are generally classified into three cases: (1) Something the user has (e.g., ID card, security token, software token, phone, or cell phone); (2) Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN)); and (3) Something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature or voice recognition, unique bio-electric signals, or another biometric identifier)[1]. The Office of Management and Budget (OMB) has issued guidance that defines levels of authentication[2]. NIST has published further guidance[3].

Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS must not be hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the Responsible Entity determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the Responsible Entity employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures). For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access.

Local and remote user access to ICS components is enabled only when necessary, approved, and authenticated. Remote access refers to access to a cyber asset by a user

[1] Derived from *Wikipedia* http://en.wikipedia.org/wiki/Two-factor_authentication, there being no authoritative definition available.

[2] *E-Authentication Guidance for Federal Agencies*, Office of Management and Budget memorandum M 04-04, December 2003.

[3] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.1, September 2004.

(or a cyber asset) communicating through an external network not controlled by the Responsible Entity.

========== based on CA-3 & IA-2 Appx F&I ==========

~~R3.5.~~R6.2. The Responsible Entity shall manage user identifiers by:

- Uniquely identifying each user
- Verifying the identity of each user
- Receiving authorization to issue a user identifier from an appropriate Responsible Entity official
- Issuing the user identifier to the intended party
- Define and implement a period of inactivity for disabling a user identifier
- Archiving user identifiers.

GUIDANCE: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

==========requirement based on IA-4 Appx F&I ==========

~~R3.6.~~R6.3. The cyber assets shall identify and authenticate specific devices before establishing a connection.

GUIDANCE: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the Responsible Entity employs compensating controls

========= requirements and guidance based on IA-3 Appx F&I ==========

R6.4. The Responsible Entity shall manage authenticators by:

R6.4.1. Defining initial authenticator content

R6.4.2. Establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators

R6.4.3. Changing default authenticators upon information system installation

~~R3.6.1.~~R6.4.4. Changing/refreshing authenticators periodically.

GUIDANCE: Authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the cyber assets: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the cyber assets: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account.

Many ICS devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great

security risk, and therefore must be changed. Authentication may be role-based, group-based, or device-based.

========== requirement and guidance based on IA-5 Appx F&I ==========

~~R3.7.~~R6.5. Cyber Assets shall obscure feedback of authentication information during an interactive human authentication process to protect the information from possible exploitation/use by unauthorized individuals.

GUIDANCE: The feedback from the cyber assets does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

========== based on IA-6 ==========

C. Measures

The following measures will be used to demonstrate compliance with the requirements of Standard CIP-005. Responsible entities may document controls either individually or by specified applicable grouping.

M1. Documents about the Electronic Security Perimeter as specified in Requirement R1.

M2. Documentation of the electronic access controls to the Electronic Security Perimeter(s), as specified in Requirement R2.

M3. Documentation of controls implemented to log and monitor access to the Electronic Security Perimeter(s) as specified in Requirement R3.

M4. Documentation of the Responsible Entity's ~~annual vulnerability~~Cyber Security Perimeter assessment as specified in Requirement R4.

M5. Access logs and documentation of review, changes, and log retention as specified in Requirement R5.

M6. Documentation of the indetification and authentication controls as specified in Requirement R6.

~~M5.~~M7. Documentation of the Exception Plans as specified in Section A.6 Exemptions.

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Monitoring Responsibility

1.1.1 Regional Reliability Organizations for Responsible Entities.

1.1.2 NERC for Regional Reliability Organization.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Annually.

1.3. Data Retention

1.3.1 The Responsible Entity shall keep logs for a minimum of ninety calendar days, unless longer retention is required pursuant to Standard CIP-008, Requirement R2.

1.3.2 The Responsible Entity shall keep other documents and records required by Standard CIP-005 from the previous full calendar year.

1.3.3 The compliance monitor shall keep audit records for three years.

1.4. Additional Compliance Information

1.4.1 Responsible Entities shall demonstrate compliance through self-certification or audit, as determined by the Compliance Monitor.

1.4.2 Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and approved by the designated senior manager or delegate(s). Duly authorized exceptions will not result in noncompliance. Refer to CIP-003 Requirement R3.

2. Levels of Noncompliance

2.1. Level 1:

2.1.1 All document(s) identified in CIP-005 exist, but have not been updated within ninety calendar days of any changes as required; or,

2.1.2 Access to less than 15% of electronic security perimeters is not controlled, monitored; and logged;

2.1.3 Document(s) exist confirming that only necessary network ports and services have been enabled, but no record documenting annual reviews exists; or,

2.1.4 At least one, but not all, of the Electronic Security Perimeter vulnerability assessment items has been performed in the last full calendar year.

2.1.5 The Exception Plan exists but has been approved, but not in the last full calendar year by a Responsibility Entity senior manager.

2.2. Level 2:

2.2.1 All document(s) identified in CIP-005 but have not been updated or reviewed in the previous full calendar year as required; or,

2.2.2 Access to between 15% and 25% of electronic security perimeters is not controlled, monitored; and logged; or,

2.2.3 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed in the previous full calendar year.

~~2.2.3~~2.2.4 The Exception Plan exists and has been approved in the last full calendar year by a Responsibility Entity senior manager, but has not been approved in the last full calendar year by the Regional Reliability Organization.

2.3. Level 3:

2.3.1 A document defining the Electronic Security Perimeter(s) exists, but there are one or more Critical Cyber Assets not within the defined Electronic Security Perimeter(s); or,

2.3.2 One or more identified non-critical Cyber Assets is within the Electronic Security Perimeter(s) but not documented; or,

2.3.3 Electronic access controls document(s) exist, but one or more access points have not been identified; or

2.3.4 Electronic access controls document(s) do not identify or describe access controls for one or more access points; or,

2.3.5 Electronic Access Monitoring:

2.3.5.1 Access to between 26% and 50% of Electronic Security Perimeters is not controlled, monitored; and logged; or,

2.3.5.2 Access logs exist, but have not been reviewed within the past ninety calendar days; or,

2.3.6 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than two full calendar years.

~~2.3.6~~2.3.7 The Exception Plan exists but has not has been approved in the last full calendar year by a Responsibility Entity senior manager, and has not been approved in the last full calendar year by the Regional Reliability Organization.

2.4. Level 4:

2.4.1 No documented Electronic Security Perimeter exists; or,

2.4.2 No records of access exist; or,

2.4.3 51% or more Electronic Security Perimeters are not controlled, monitored, and logged; or,

2.4.4 Documentation and records of vulnerability assessments of the Electronic Security Perimeter(s) exist, but a vulnerability assessment has not been performed for more than three full calendar years; or,

2.4.5 No documented vulnerability assessment of the Electronic Security Perimeter(s) process exists.

2.4.6 The Exception Plan does not exists.

E. Regional Differences

None identified.

~~**Version History**~~

~~Version~~	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~01/16/06~~	~~D.2.3.1 Change "Critical Assets," to "Critical Cyber Assets" as intended.~~	~~03/24/06~~