Project 2008-06 - Cyber Security Order 706 - V5

Working Draft (April 10, 2012) of Consideration of Issues and Directives

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 233 (Related paragraph: 25) Para 233 "The Commission continues to believe and is further persuaded by the comments that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERCs Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences are divergent responsibilities and goals. NIST is providing standards and guidance for U.S. Federal Agencies in managing risks to their information and Systems in support of their unique missions. NERC, on the other hand, has the role of setting standards for managing risks to systems in support of a shared community mission to ensure the reliability of the BES. This difference is important because it enables the industry to develop better detail about the impacts that they need to avoid in order to achieve their mission. NIST does not enjoy this benefit, as they are providing standards to almost 200 different organizations, each with vastly different missions. The advantage that the NERC Standards enjoy enables a focus on a relatively small number of reliability services that need to be protected. This ultimately means that the NERC Standards can be more tailored and appropriate to the industry than a wholesale adoption of the NIST Risk Management Framework. Four key features of the NIST Risk Management Framework were incorporated into Version 5 of NERC CIP Standards: (1) ensuring that all BES Cyber Systems associated with the Bulk Power System, based on their function, receive some level of protection, (2) customizing protection to the mission of the cyber systems subject to protection, (3) a tiered approach to security controls which specifies the level of protection appropriate for systems based upon their importance to the reliable operation of the Bulk Power System, and (4) the concept of the BES Cyber System itself. Features 2 and 3 above are tightly coupled. In the NIST Risk Management Framework, there is a concept of tailoring and scoping which allows the organization to determine which controls are applicable to their specific environment. In the NERC compliance framework, all requirements are mandatory and enforceable, and, therefore, this concept does not translate directly. As such, the customization of protections by

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
for new CIP Reliability Standards, or as part of an assessment of NERCs performance of its responsibilities as the ERO." Para 25 "The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework. "		mission is based upon the environment that the BES Cyber System supports (control center, transmission facility, generation facility) and utilizes the tiered model and the requirement applicability to provide this customization to the individual environments that together support a combined mission of Bulk Power System reliability. The NIST Security Control Catalogue in 800-53, Revision 3 was also used as a reference in addressing many of the FERC directives in Order No. 706. Additionally, the SDT added members representing federal agencies and NIST, in particular, to the drafting team during development.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 249 Para 258 "Likewise, the ERO should consider Northern Californias suggestion that the ERO establish a formal feedback loop to assist the industry in developing policies and procedures." Para 249 "In contrast, FirstEnergy agrees that NERC should provide guidance to entities without a wide-area view, such as a generation owner or a partial generation owner, on how to approach a risk-based assessment. Likewise, Northern California suggests that NERC establish a process for informal, case-by-case consultations with responsible entities that need assistance in complying with CIP-002-1. In addition, as part of the re-examination of CIP-002-1, Northern California encourages the incorporation of a formalized feedback loop to assist the industry in developing policies and procedures."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. CIP-002-5, Attachment 1's bright line criteria were developed in consideration of a wide area view, and it obviates the need for a formal feedback loop or a need for a wide area view by smaller entities.
Para 258 and 252	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Having risk-based approaches to

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 "As to Entergys suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process." Para 252 "Entergy suggests, as an alternative approach to critical asset identification, that the ERO provide a Design-Basis Threat (DBT) a profile of the type, composition, and capabilities of an adversary that would assist the industry as a technical baseline against which to establish the proper designs, controls and processes. Entergy claims that a DBT approach would address many of the Commissions concerns regarding the risk-based methodology. For example, a DBT would focus the appropriate emphasis on the potential consequences from an outage of a critical asset. In addition, a DBT would address the Commissions concern that responsible entities will not have enough guidance in developing a risk-based methodology and not know how to identify a critical asset. Entergy contends that a DBT		applying cyber security requirements is a worthy objective and will continue to be explored, but the complexity and subjectivity it adds is beyond the scope of these revisions. CIP-002-5, Attachment 1's bright line criteria uses an impact-based approach as an alternative to DBT.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
approach would provide the industry with more certainty in implementing the CIP Reliability Standards."		
Para 272 (1 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, **the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.** In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."	FERC Order 706	This was completed by CIPC in the Version 3 CIP standards guidelines. The guidelines are entitled "Identifying Critical Assets" and "Identifying Critical Cyber Assets" and are available for download from www.nerc.com.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 272 (2 of 2) "Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. **Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data."**	FERC Order 706	Guidance developed for CIP-002-5 addresses situational awareness and inter-utility data exchange.
Para 285 (related paragraph: 278) Para 285 "The Commission directs the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5, and added as a scoping filter for requirements where: (i) the use of non-routable protocols is a mitigating factor for the vulnerabilities a requirement addresses, and (ii) implementation of routable protocols would be required to comply with the requirement (e.g. malware updates, security event monitoring, and alerting, etc.).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience]." Para 278 "ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable by testing and experience. In contrast, Energy Producers notes that CIP-002-1 as proposed by NERC provides that a critical cyber asset must have either routable protocols or a dial-up connection. Energy Producers states that this is a useful, objective criterion which will assist in the unambiguous identification of such assets and therefore should be retained."		

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 296 “With regard to METC-ITC’s comment, the ERO should consider in its Reliability Standards development process the suggestion that the CIP Reliability Standards require oversight by a corporate officer (or the equivalent, since some entities do not have corporate officers) rather than by a “senior manager.”	FERC Order 706	The requirement that the senior manager have “the overall authority and responsibility for leading and managing implementation of the requirements within this set of standards” ensures that the senior manager is of the sufficient position in the Responsible Entity to ensure that cyber security receives the prominence that is necessary. In addition, given the range of business models for Responsible Entities; from municipal, cooperative, federal agencies, investor-owned utilities, privately owned utilities, and everything in between, the SDT believes that requiring the senior manager to be a “corporate officer or equivalent” would be extremely difficult to interpret and enforce on a consistent basis. In Version 5, this is addressed in the definition of CIP Senior Manager. The SDT believes the filing for Version 2 also addressed this issue.
Para 321 " SPP and ReliabilityFirst suggest modifying CIP-002-1 to allow an entity to rely upon the assessment of another entity with interest in the matter. We believe that this is a worthwhile suggestion for the ERO to pursue and the ERO should consider this proposal in the Reliability Standards development process. We note that, even without such a provision, an entity such as a small generator operator is not foreclosed from consulting with a balancing authority or other appropriate entity with a wide-area view of the transmission system."	FERC Order 706	The SDT considered this suggestion, and it believes that the change to “bright line” criteria for identifying BES Cyber Systems, along with refining the scope of certain requirements through applicability columns based on impact and connectivity characteristics, addresses this concern.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 355 (also see paragraph 356) "The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1."		The SDT has chosen to provide guidance to Responsible Entities through the introduction of topical areas in the requirement language that must be addressed in cyber security policies in CIP-003-5, Requirement R1 and R2. Additionally, as directed, the SDT has provided guidance about these topical areas in the Guidelines and Technical Basis section of Reliability Standard CIP-003-5.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 376 ". . . the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards. In response to EEI, we believe that this clarification is needed because, for example, it is important that a responsible entity understand that exceptions that individually may be acceptable must not lead cumulatively to results that undermine compliance with the Requirements themselves."	FERC Order 706	The SDT removed the CIP-003-4 requirement to document exceptions to the Cyber Security Policy. • The SDT considers this a general management issue that is not within the scope of a compliance requirement. • The SDT found no reliability basis in this requirement. • Removal of this requirement provides clarity that the only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 386 "The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly. In general, the Commission agrees with commenters and believes that access to protected information should cease as soon as possible but not later than 24 hours from the time of termination for cause."	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities must revoke access to the electronic and physical locations where it stores BES Cyber System Information. This could include records, closets, substation control houses, records management systems, file shares, or other physical and logical areas under the Responsible Entity's control.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 397 and 398 "The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes. The Commission believes that these considerations are significant aspects of change control and configuration management that deserve express acknowledgement in the Reliability Standard. While we agree with Entergy that the NIST Security Risk Management Framework offers valuable guidance on how to deal with these matters, our concern here is that the potential problems alluded to be explicitly acknowledged. Our proposal does not speak to how these problems should be addressed. We do not believe that the changes will have burdensome consequences, but we also note that addressing any unnecessary burdens can be dealt with in the Reliability Standards development process."	FERC Order 706	Two new requirements were added to address this change CIP-010-1, Requirement R1 (Item 1.4), requires additional testing prior to a configuration change in a test environment. CIP-010-1, Requirement R2 (Item 2.1), requires monitoring of the configuration of the BES Cyber System. • The SDT proposes the introduction of a defined baseline configuration and an explicit requirement for monitoring for changes to the baseline configuration in High Impact Control Centers in order to capture malicious changes to a BES Cyber System. • Additionally, the SDT proposes that changes to High Impact Control Centers be tested in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) prior to their implementation in the production environment to aid in identifying any accidental consequences of the change.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 412 "The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world."	FERC Order 706	The SDT addresses this through the defense in depth framework that has been designed through the full suite of revised CIP Standards. The standards address defense in depth through personnel management, systems management, and information management. The Standards are written in the perspective that the Responsible Entity is required to protect its critical systems from internal and external threat. The requirements include both preventive and detective controls. The requirements mandate appropriate vetting of personnel to minimize the risk of internal threat. They then build upon this through secure system design for internal use and remote access. These controls are further enhanced by the requirement of robust monitoring and alerting activities.
Para 433 ". . . we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard."	FERC Order 706	The SDT addressed this by determining that identification of certain core training elements would be beneficial, and the identification of those core training elements that must be provided in the training program should be role based, as required in CIP-004-5, Requirement R2.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 434 "The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."	FERC Order 706	The SDT added this as a topic for role-specific training in CIP-004-5, Requirement R2 (Part 2.10). Core training programs are intended to encompass networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 435 "Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves."	FERC Order 706	The SDT has considered the issue and has determined that no modifications are necessary. In practice, this training is often conducted as computer-based training (CBT), and the training is aimed at an entity's own policies. As such, as long as the training material itself is adequate, which can be evaluated through the existing audit process, security trainers themselves do not need any particular or specialized training.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (1 of 2) (Review the referenced Comments) " APPA/LPPC seek **clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees.** SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees. The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by requiring the Responsible Entity to establish and document criteria for personnel risk assessments. The requirements in CIP-004-5 also provide additional detail about what type of records (whether criminal, work history, domicile, etc) a Responsible Entity must examine.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 446 (2 of 2) (Review the Referenced Comments) "APPA/LPPC seek clarification regarding discretion in reviewing results of personnel risk assessments and in coming to conclusions regarding the subject employees. **SDG&E seeks refinements on various issues, including an industry-wide protocol for periodic background and criminal checks, and the use of pre-employment background check procedures for current employees.** The ERO should consider these issues when developing modifications to CIP-004-1 pursuant to the Reliability Standards development process."	FERC Order 706	In CIP-004-5, Requirement R4, the SDT has specified that the seven-year criminal history records check must include current residence, regardless of duration; and cover at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more, resided, been employed, and/or attended school.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 460 "The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination)."	FERC Order 706	In CIP-004-5, Requirement R7, the SDT has addressed this directive by requiring revocation of access concurrent with the termination or disciplinary action (Part 7.1), or by the end of the calendar day in cases of transfers or reassignments (Part 7.2). In reviewing how to modify the requirement relating to transfers or reassignments, the SDT determined the date a person no longer needs access after a transfer was problematic because the need may change over time. As a result, the SDT adapted this requirement (Part 7.2) from NIST 800-53, Version 3, to review access authorizations on the date of the transfer. The SDT felt this was a more effective control in accomplishing the objective to prevent a person from accumulating unnecessary authorizations through transfers. CIP-004-5, Requirement R7 (Part 7.4) augments the requirements in Parts 7.1 and 7.2 that respond to the directive. In order to meet the immediate time frame, Entities will likely have initial revocation procedures to prevent remote and physical access to the BES Cyber System. Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (Part 7.4) provides the additional time to review and complete the revocation process. Although the initial actions already prevent further access, this step provides additional assurance in the access revocation process.
Para 464 "We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification."	FERC Order 706	The SDT notes that it addresses this issue in previous versions of the CIP standards. Version 2 added the requirement for a Personnel risk assessment prior to being granted access, and Version 3 required implementation of a visitor control program. The changes made to the requirements in Version 5 maintain and improve upon these requirements. CIP-004-5, Requirement R5 makes clear that individuals not properly authorized for unescorted physical access will not have such access. CIP-006-5 restricts access through implementation of a visitor management program.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 473 "The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entitys obligations regarding vendors with access to critical cyber assets."	FERC Order 706	CIP-002-5, Requirement R1 makes clear that asset owners are responsible for complying with the standards.
Para 476 "We direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commissions determinations above."	FERC Order 706	Guidance in CIP-002-5 states that the owning Responsible Entity is responsible for complying with the CIP Cyber Security Standards. Furthermore, the guidelines and technical basis for CIP-002-5 states that where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 496 (Related: Para 503) Para 496 "The Commission adopts the CIP NOPRs proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter" Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	FERC Order 706	The drafting team addresses this in CIP-005-5, Requirement R1 (Item 1.4). Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures, such that the cyber assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls; thus the drafting team has decided to add the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs. The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.
Para 502 "The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process."	FERC Order 706	The directive for two defensive measures when constructing an ESP indicates a defense-in-depth approach and not simple redundancy of firewalls. CIP-005-5 adds the security measure of malicious traffic inspection (IDS/IPS) a requirement for these ESPs as a second security measure for High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 504 (Related: Para 495) Para 504 "The ERO should consider in the Reliability Standards development process Northern Indiana's and Xcel's concerns regarding the phrase "single access point at the dial up device." Para 495 "Northern Indiana and Xcel ask the Commission to clarify or direct the ERO to clarify the phrase "single access point at the dial up device" in CIP-005-1, Requirement R1.2. Xcel asks whether this refers to the initiating device, the device at the point of termination, or both. Northern Indiana would not modify CIP-005-1, but urges that any modifications to Requirement R2 should allow continued reliance on legacy systems."	FERC Order 706	The SDT has deleted the troublesome language relating to "single access point at the dial up device," and the SDT has clarified that an Electronic Security Perimeter applies to routable connectivity.CIP-005-5 also separated the requirement for dial-up connectivity, specifying in CIP-005-5, R1.4, that a Responsible Entity must perform authentication when establishing dial-up connectivity with the BES Cyber System, where technically feasible, on its high and medium impact BES Cyber Systems with dial-up connectivity.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 511 "The Commission adopts the CIP NOPRs proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies."	FERC Order 706	CIP-005-5, Requirement R2 has additional security requirements for remote access from the work started in the Urgent Action Revisions to CIP-005-3. One of these requirements is two-factor authentication and specific examples of two-factor authentication are provided in the referenced guideline.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 525 "The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require logs to be reviewed more frequently than 90 days, but clarifies its direction in several respects. At this time, the Commission does not believe that it is necessary to require responsible entities to review logs daily…" Para 628. "Requirement R6 of CIP-007-1 does not address the frequency with which log should be reviewed. Requirement R6.4 requires logs to be retained for 90 calendar days. This allows a situation where logs would only be reviewed 90 days after they are created. The Commission continues to believe that, in general, logs should be reviewed at least weekly…"	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. CIP-007-5, Requirement R4, combines CIP-005-4, Requirement R5 and CIP-007-4, Requirement R6, and addresses FERC's directives from a system-wide perspective. The primary feedback received on this requirement from the informal comment period was the vagueness of terms "security event" and "monitor". The term "security event" or "events related to cyber security" is problematic because it does not apply consistently across all platforms and applications. To resolve this term, the requirement takes an approach to specify a minimum set of security event types to log and review, and allows the entity to define relevant security events in addition to the specified minimum. In addition, CIP-007-5, Requirement R4, sets up parameters for the logging and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings.
Para 526 (1 of 2) ". . . the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. (Also see response to paragraph 525).

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 526 (2 of 2) "The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs."	FERC Order 706	CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. (Also see response to paragraph 525).
Para 528 "The Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks. In addition, CIP-007-5, Requirement R4, sets up parameters for the monitor and review processes. It is rarely feasible or productive to look at every security log on the system. Paragraph 629 of the FERC Order 706 acknowledges this reality when directing a manual log review. As a result, this requirement allows the manual review to consist of a sampling or summarization of security events occurring since the last review. Additionally, consistent with FERC Order 706, the requirement makes clear that the objective of this control is to identify unanticipated Cyber Security Incidents and potential event logging failures, thereby improving automated detection settings. (Also see response to paragraph 525).
Para 541 ". . . we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments."	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 542 ". . . the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems."	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 544 (1 of 2) "the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification."	FERC Order 706	The SDT addresses this paragraph in CIP-010-1, Requirement R3. • The SDT has proposed that prior to adding a new cyber asset into a BES Cyber System, that the new Cyber Asset undergo an active vulnerability assessment. • An exception is made for specified CIP Exceptional Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (Part 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required security controls are not adversely affected.
Para 544 (2 of 2) ". . . we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment"	FERC Order 706	The SDT has added a requirement in CIP-010-5, R3.3, to perform an active vulnerability assessment of a new Cyber Asset in High Impact BES Cyber Systems.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 547 ". . . we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years"	FERC Order 706	In CIP-010-1, Requirement R3, the SDT has added requirements for an "active vulnerability assessment" to occur at least once every three years for High Impact Control Centers using a test system so as to prevent unforeseen impacts on the Bulk Electric System. Requirement R3 requires annual paper assessments in the intervening years.
Para 572 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R1 (Part 1.3) for High Impact BES Cyber Assets, by requiring Responsible Entities to "utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access."
Para 581 "The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years."	FERC Order 706	The SDT addressed this in CIP-006-5, Requirement R3 (Part 3.1) by changing the frequency to a 24-month testing cycle; after deliberation and consideration, the SDT determined that a requirement of more frequent testing (e.g., 12 months), was too often.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 5 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. **We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly.** The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."	FERC Order 706	The SDT has introduced the concept of a "baseline configuration" around which the change control process is based. The SDT further utilizes this "baseline configuration" to provide clarity as to what is considered a representative System as it relates to performing active vulnerability assessments in CIP-010-1.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 609, Sentence 6 "The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a representative system one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a representative system and to modify CIP-007-1 accordingly. **The Commission directs the ERO to consider providing further guidance on testing systems in a reference document."**	FERC Order 706	The SDT has provided additional guidance on testing systems in the Guidelines and Technical Basis section of CIP-010-1. Furthermore, and in addition to guidance, the requirements of CIP-010-1 R1.5 and CIP-010-1 R3.2 identify a “representative system” as a system that exists in a test environment (or production environment where tests can be performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. This baseline configuration concept is developed by entities in CIP-010-1 R1.1 and further contains details on what constitutes a “representative system”.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 610 ". . . we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above."	FERC Order 706	CIP-010-1, Requirements R1 (Part 1.5) requires Responsible Entities to account for any additional differences between the two systems, the SDT proposes using the words similar to those directly from FERC Order No. 706, paragraph 610: "Document the differences between the test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) and the production environment including a description of the measures used to account for any differences in operation between the test and production environments."
Para 611 "With respect to MidAmericans proposal that the differences between the testing and production environments only be reported when the production and test environments are established, the ERO should consider this matter in the Reliability Standards development process However, the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production."	FERC Order 706	The SDT has added a requirement for the Responsible Entity to, "document…the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments." The SDT has included this requirement for each test performed in the representative environment. The SDT appreciates the concern brought up by MidAmerican and believes that entities should be free to use the same documentation multiple times to provide compliance with this requirement so as to minimize the documentation overhead, but also believes that it is important for entities to give consideration to the configuration of their representative system each time a test is performed in order to ensure the validity of the test results.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Paras 622 (Related: See Paras 614 and 619) "Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere."	FERC Order 706	The "acceptance of risk" language was removed in Version 2, and it has not been used in Version 5. Malicious software prevention exceptions have been placed under the TFE process since Version 2.
Para 622 (Related: See Paras 614 and 619) "The Commission also directs the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above."	FERC Order 706	The drafting team addressed this in CIP-007-5, Requirement R3. The drafting team is taking the approach of making this requirement a competency-based requirement where the entity must document how the malware risk is handled for each BES Cyber System, but it does not prescribe a particular technical method nor does it prescribe that it must be used on every component. The BES Cyber System is the object of protection. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (Part 2.1) and guidance is further included for the cyber security policy in CIP-003-5, Requirement R2 to maintain up-to-date anti-malware software and patch levels before initiating interactive remote access.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 628 "The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1."	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples a minimum of every two weeks.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 633 "The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it."	FERC Order 706	The SDT addresses this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 635 "the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data."	FERC Order 706	The SDT addresses this directive in CIP-011-1, Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from the BES Cyber Asset. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal. Additional guidance was added to the standard as further clarification: Media sanitization is generally classified into four categories: Disposal, clearing, purging, and destroying. For the purposes of this requirement, disposal by itself, with the exception of certain special circumstances such as the use of strong encryption on a drive used in a SAN or other media, should never be considered acceptable. The use of clearing techniques may provide a suitable method of sanitization for media that is to be reused whereas purging techniques may be more appropriate for media which is ready for disposal. Entities are strongly encouraged to review NIST SP800-88 for guidance on how to develop acceptable media sanitization processes. This requirement allows for BES Cyber Systems to be removed from service and analyzed with their media intact as this should not constitute a release for reuse. However, following the analysis, if the media is to be reused outside of a BES Cyber System or disposed of, it should be properly cleared using a method to prevent the unauthorized retrieval of BES Cyber System Information from the media.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 643 (1 of 2) **"The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments**, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."	FERC Order 706	In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance in CIP-010-1 on active and paper vulnerability assessment. The SDT further referenced NIST SP800-115 to provide entities additional guidance on how to conduct a vulnerability assessment.
Para 643 (2 of 2) "The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, **and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan."**	FERC Order 706	In CIP-010-1, R3 (Part 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 660 (Related, See Para 661) "The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident."	FERC Order 706	In addition to defining the term Reportable Cyber Security Incident as one that compromises or disrupts the functional tasks of a Responsible Entity, CIP-008-5 also provides further guidance for determining a Reportable Cyber Security Incident in the "Guidelines and Technical Basis" section of the standard. The definition and guidance describe a reportable incident based on characteristics of impact to the BES, rather than enumerating threats and characteristics of malware. The draft Standard EOP-004-2 provides reporting criteria for Reportable Cyber Security Incidents.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 661 (Related, See Para 660) "the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced."	FERC Order 706	CIP-008-5 addresses the four parts of this directive as follows: 1. Added: Reportable Cyber Security Incidents include, as a minimum, any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. In turn, a Cyber Security Incident includes a malicious act or suspicious event that compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter. 2. Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3. 3. See 1 above 4. Guidance and measurements have been developed to be auditable and enforceable.
Para 673 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contained provisions for reporting Cyber Security Incidents. This is now addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 676 "The Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report."	FERC Order 706	Cyber Security - Incident Reporting and Response Planning: Retired CIP-008-4, R1.3 which contains provisions for reporting Cyber Security Incidents. This is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.
Para 686 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of which must include lessons learned.The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned."	FERC Order 706	In CIP-008-5, R3 (Parts 3.3 and 3.4) the SDT includes additional specification on the update of response plan and modifies the response plan requirements to incorporate lessons learned. Maintenance of documentation of paper drills, full operational drills, and responses to actual incidents is part of the documentation required to demonstrate compliance with the security controls in CIP-008-5 and is already subject to the evidence retention requirements associated with all NERC Reliability Standards.
Para 687 (also see Footnote in Order) "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1,	FERC Order 706	CIP 008-5 Part 2.1 is written to allow the testing requirement to be satisfied by responding to an actual Reportable Cyber Security Incident; or with a paper drill or table top exercise; or with a full operational exercise. The reporting of Cyber Security Incidents is addressed in the draft EOP-004-2, Requirement 1, Part 1.3.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
such testing need not require a responsible entity to remove any systems from service. The Commission understands that use of the term full operational exercise in this context can be confusing. We interpret the priority of the testing required by this provision to be that planned response actions are exercised in reference to a presumed or hypothetical incident contemplated by the cyber security response plan, and not necessarily that the presumed incident is performed on the live system. A responsible entity should assume a certain type of incident had occurred, and then ensure that its employees take what action would be required under the response plan, given the hypothetical incident. A responsible entity must ensure that it is properly identifying potential incidents as physical or cyber and contacting the appropriate government, law enforcement or industry authorities. CIP-008-1 should require a responsible entity to verify the list of entities that must be called pursuant to its cyber security incident response plan and that the contact numbers at those agencies are correct. The ERO should clarify this in the revised Reliability Standard and may use a term different than		The Guidelines and Technical Basis section of CIP-008-5 refer to operational exercises in the FEMA Homeland Security Exercise Evaluation Program as one of the following three types: drill, functional exercise, and full-scale exercise. It defines that “[a] full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operation centers, etc.) and "boots on the ground" response (e.g., firefighters decontaminating mock victims).” The SDT believes the term operational exercise has become well understood and appropriate for both incident response and recovery exercises.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
full operational exercise.”		
Para 694 “For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard”	FERC Order 706	The SDT added in CIP-009-5, R2, a requirement to implement the recovery plan.
Para 706 "The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard."	FERC Order 706	CIP-009-5, R1 (Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. The SDT captured the objective of this control, but did not explicitly use the term “forensics” due to the legal interpretations associated with the term.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 710 (Related: Para 706) "Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report."	FERC Order 706	CIP-009-5, R1 (Part 1.5) requires a process to preserve data for analysis or diagnosis of the cause of any problem that adversely impacts a BES Reliability Operating Service. .
Para 725 "The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years."	FERC Order 706	CIP-009-5, R2 (Part 2.3) requires an operational exercise at least once every three calendar years.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 739 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes."	FERC Order 706	In CIP-009-5, R1 (Part 1.4) the SDT added requirements related to restoration processes based on review of the DHS Controls, and requires verification initially after backup to ensure that the process completed successfully. In CIP-009-5, R2 (Part 2.2), requires a Responsible Entity to ensure that the information is useable and is compatible with current system configurations at High Impact BES Cyber Systems or Medium Impact BES Cyber Systems at Control Centers.
Para 748 "The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use."	FERC Order 706	In CIP-009-5, R1 (Part 1.4) the SDT added requirements related to restoration processes based on review of the DHS Catalog of Control Systems Security: Recommendations for Standards Developers (a derivation of NIST SP800-53 for Control Systems), and requires verification initially after backup to ensure that the process completed successfully.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
	NERC Alert regarding remote access VPN vulnerabilities	Addressed in CIP-005-5 ▪ Creates basic requirements to protect critical systems from untrusted networks. ▪ Identifies protective measures that provide secure access to critical systems. ▪ Helps ensure secure practices by employees, contractors, and service vendors to minimize exploitation of vulnerabilities. ▪ Addresses questions regarding ability to audit or enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. Additional information is provided in "Guidance for Secure Interactive Remote Access" published by NERC in July 2011. Additionally, remote access is specifically required to be included in an entity's cyber security policy. Guidance is included to assist the entity in determining what this topic in the cyber security policy should address.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 13 "The Commission recognizes and encourages NERC's intention to address physical ports to eliminate the current gap in protection as part of its ongoing CIP Reliability Standards project scheduled for completion by the end of 2010. Should this effort fail to address the issue, however, the Commission will take appropriate action, which could include directing NERC to produce a modified or new standard that includes security of physical ports."	Order Approving Interpretation of Reliability Standard CIP-007-2 in Docket No. RD10-3-000, March 18, 2010	CIP-007-5, R1 (Part 1.2) requires Responsible Entities (for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers) to "protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media."