Project 2008-06 Cyber Security Order 706

Consideration of Issues and Directives — DRAFT

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 25 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.	FERC Order 706	It is important to highlight differences between NERC's and NIST's approaches. At the root of these differences is the 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 two hundred 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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		features of the NIST Risk Management Framework were incorporated into version 5 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 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 706.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 258 and 252 "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 Commission's 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 approach would provide the industry with more certainty in implementing the CIP Reliability Standards."	FERC Order 706	CIP-002-5 classifies BES Cyber Systems through impact thresholds, and does not use risk-based assessments performed by individual entities. Risk-based approaches to 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.
Para 282 The Commission directs the ERO to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets.	FERC Order 706	The definition of BES Cyber Asset as used in CIP-002-5 requires Responsible Entities to consider misuse of the Cyber Assets in identifying BES Cyber Systems.
Para 285 The Commission directs the ERO to consider the comment from	FERC Order 706	The exclusion of Cyber Assets based on non-routable protocols has been removed from CIP-002-5 and added as a

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
ISA99 Team [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].		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.).
Para 321 "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.
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.”	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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		only exceptions to the requirements is through the defined Technical Feasibility Exception process, where specifically allowed.
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.	FERC Order 706	To address this directive, in CIP-004-5, Requirement R7, Responsible Entities are required to revoke access to 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.
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."	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 prior to their implementation in the

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		production environment to aid in identifying any accidental consequences of the change.
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
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 (item 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.
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). 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.
Para 446 "Para 446. 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	FERC Order 706	The SDT clarifies the discretion in reviewing personnel risk assessments in CIP-004-5, Requirement R4, by establishing criteria for personnel risk assessments.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
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."		
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 (item 7.1) or by the end of the calendar day in cases of transfers or reassignments (item 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 (item 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 (item 7.4) augments the requirements in items 7.1 and 7.2 that respond to the directive. In order to meet the immediate timeframe, 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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		access revocation on individual Cyber Assets and applications without affecting reliability. This requirement (item 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	CIP-004-5, Requirement R5 (item 5.1), requires a personnel risk assessment as a condition of being granted access, with exceptions only for specific CIP Exceptional Circumstances which are outlined in the proposed glossary definition of the aforementioned term.
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	FERC Order 706	Guidance in CIP-002-5 advises the owning Responsible Entities determine who is responsible for complying with the CIP Cyber Security Standards.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
determinations above.		
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"	FERC Order 706	The proposed requirement requires a Responsible Entity to deploy methods to inspect communications and detect potential malicious communications for all External Connectivity (Intrusion Detection). The drafting team addresses this in CIP-005-5, Requirement R1 (item 1.4). Per FERC Order 706, p 496-503, ESP's need two distinct security measures such that the cyber assets do not lose all perimeter protection if one measure fails or is mis-configured. 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.
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.
Para 503 "The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures."	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 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.
Paras 525, 526, 528, and 628 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 526. "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. 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." 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	FERC Order 706	In CIP-007-5, Requirement R4, the SDT proposes the performance of a review of log summaries or samples 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 similar to NIST 800-53 and requires the entity to define the security events relevant to the system. In addition, this requirement 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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
or filtered logs." 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…"		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.
Paras 541, 542, and 547 Para 541. we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments." Para 542. "the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems." 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 544 "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." "we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability	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 undergoes an active vulnerability assessment. • An exception is made for specified CIP Exceptional

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
assessment”		Circumstances. • Additionally, the new requirement in CIP-010, Requirement R1 (item 1.5) requires testing of all changes for High Impact BES Cyber Systems that deviate from the baseline configuration in a test environment to ensure that required security controls are not adversely affected.
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 (item 1.3) for High Impact BES Cyber Assets
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 (item 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.
Paras 609, 610, and 611 Para 609. “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.” Para 610. “we direct the ERO to revise the Reliability Standard to	FERC Order 706	CIP-010-1, Requirement R1 (item 1.4), provides clarity on when testing must occur and requires additional testing to ensure that accidental consequences of planned changes are appropriately managed. • The SDT proposes to require a “representative system” or test system for those High Impact Control Centers to use for the purposes of testing proposed

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above." Para 611. "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."		changes and performing active vulnerability assessments. • The SDT proposes using the defined baseline configuration of a BES Cyber System for the measuring stick as to whether a test system is truly representative of the production system. • To account for any additional differences between the two systems, the SDT proposes using the words directly from FERC Order 706 "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."
Paras 620 and 622 Para 620. "The Commission will not adopt Consumers' recommendation that every system in an electronic security perimeter does not need antivirus software. Critical cyber assets must be protected, regardless of the operating system being used. Consumers has not provided convincing evidence that any specific operating system is not directly vulnerable to virus attacks. Virus technology changes every day. Therefore we believe it is in the public interest to protect all cyber assets within an electronic security perimeter, regardless of the operating system being used…"	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.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Para 622. "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.		• The SDT rewrote the requirement as a competency based requirement that does not prescribe technology. • The SDT added Maintenance to cover malware on removable media. The drafting team also created a new requirement, CIP-007-5, Requirement R3 (item 3.4), to protect against personnel introducing malicious code when temporarily connecting to a BES Cyber Asset for Maintenance purposes. When remote access is used to connect to a BES Cyber Asset, an intermediate device is required in CIP-005-5, Requirement R2 (item 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.
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 every two weeks.
Paras 633 and 635	FERC Order 706	The SDT addresses these directives in CIP-011-1,

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." 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."		Requirement R2. The requirements clarify that the goal is to prevent the unauthorized retrieval of information from media. The SDT removed the word "erase" as, depending on the media itself, erasure may not be sufficient to meet this goal.
Para 643 "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 (item 3.4), the SDT added a requirement for an entity planned date of completion to the remediation action plan following a vulnerability assessment. In order to provide more direction on what "features, functionality, and vulnerabilities" should be addressed in a vulnerability assessment, the SDT included guidance 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 661 "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 a BES Reliability Operating Service. 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.

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		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
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 (items 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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		NERC Reliability Standards.
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, R1, 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 (item 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.
Para 710 and 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 (item 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 (item 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 (item 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 (item 2.2), the SDT requires an initial and once every calendar year test of the data 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 NERC Alert regarding remote access VPN vulnerabilities	In CIP-009-5, R1 (item 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. 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

Project 2008-06 Cyber Security Order 706		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforce the requirement through the design of clear measures. ▪ Significant guidance provided to address implementation options for organizations of differing sizes, capabilities, and complexity. 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.
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	The SDT addressed this issue in CIP-007-5, R1, by having a requirement to disable or restrict use of physical I/O ports. The SDT changed the 'needed for normal or emergency operations' to those ports that are documented with reasons why they are necessary. In the March 18, 2010 FERC issued an order to approve NERC's interpretation of Requirement R2 of CIP-007-2. In this order, FERC agreed the term "ports" in "ports and services" refers to logical communication (e.g. TCP/IP) ports, but they also encouraged the drafting team to address unused physical ports.