Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC200900254	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-005-1 R2.6. FRCC determined that two of FRCC_URE1's firewall devices identified as access points to the electronic security perimeter had an acceptable use banner, but the banner did not conform to the language specified in the entity's procedure document.	CIP-005-1	R2; R2.6	Lower	Severe	This violation pose minimal risk and not a serious or substantial risk to the reliability of the bulk power system because the entity already had an acceptable use banner in place for electronic access control devices which was sufficient to inform, caution and deter an individual for any unauthorized access attempts even though that acceptable use banner did not exactly match the banner described in the entity's procedure.	When the Standard became mandatory and enforceable	When the banner was corrected	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 corrected the banner on the two firewall devices, developed, reviewed, and approved a checklist to use for new equipment	10/15/2009	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC200900317	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-005-1 R1. FRCC determined that FRCC_URE1 classified one device incorrectly when developing the list of Cyber Assets. The device was determined to be a communication link connecting discrete Electronic Security Perimeters (ESPs). The device connecting two ESPs formed a wide area network utilizing a point to point virtual private network. Since the device is used to ensure that all CCAs are within a secure ESP, it should have been classified as an "access point to the ESP" as required by CIP-005-1 R1.3.	CIP-005-1	R1	Medium	High	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because the device was located within a Physical Security Perimeter that was a secured and guarded facility which had no workstations present to connect to the corporate wide area network. In addition, the access point was in a dedicated encrypted point to point (VPN) tunnel with no remote access.	When the Standard became mandatory and enforceable	Mitigation Plan completion	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 verified and documented the ports and services in operation for the device, verified the required appropriate use banner was implemented for the device, verified the device was covered in a disaster recovery plan, and verified that the device disaster recovery plan includes requirements for backup and recovery.	12/17/2009	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000314	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-002-1 R3 and revised the Self-Report to include additional Critical Cyber Assets (CCAs). FRCC_URE1 staff performed a CIP-002-1 self-assessment at one of its facilities. FRCC_URE1 staff found that there were six CCA devices (two monitoring racks and four control racks) that were not identified in its CCA list as required by CIP-002-1 R3.	CIP-002-1	R3	High	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because the devices were not properly identified as CCAs for 26 days and the devices were within a locked 6-wall boundary protected by card access inside a fenced generating plant site with armed guards. Devices were not accessible remotely as the generating plant VLAN restricted any outside access.	When the Standard became mandatory and enforceable	Mitigation Plan completion	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 placed guards in identified rooms and logged access for the newly identified CCAs. FRCC_URE1 implemented balance of standards for the newly identified CCAs related to the Self-Report and performed a walk down of the plant's electronic security perimeter(s) with additional IT staff members. Corporate IT assisted and trained plant staff during the annual review of CCAs and Cyber Assets within the Electronic Security Perimeter. Finally, FRCC_URE1 implemented 6-walled protection and card readers.	5/21/2010	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000315	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-006-1 R2. FRCC_URE1 staff performed a CIP-006 self-assessment at one of its facilities and as a result reported that operational and procedural controls to manage physical access at all access points to the Physical Security Perimeters (PSPs) twenty-four hours a day, seven days a week had not been fully implemented at six PSPs. FRCC_URE1 has installed special locks on the PSPs to allow entry when card readers are inoperable. There were 5 keys available for the special locks (restricted keyway). The facility could not account for one key for the restricted keyways. All locks to the restricted keyways were changed as a result of the missing key. PSPs at the facility with a card reader door were also equipped with physical key locks (which were not restricted keyways) could be operated with a master key. The physical key locks on these doors were not disabled and special Locks (restricted keyways) were not installed.	CIP-006-1	R2	Medium	High	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because while the devices could have been compromised to trip the two units, the assets were located inside a secured facility with armed guards, and these devices could not be remotely accessed. Finally, the exposure was for 26 days for four PSPs and 45 days for two PSPs.	When the Standard became mandatory and enforceable	When guards were added to monitor, secure, and log access to the PSP	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 placed guards in identified rooms and manually logged access. FRCC_URE1 installed and programmed card readers for identified rooms for NERC CIP access. FRCC_URE1 replaced the special keys and key cores and installed a special key lock in at least one door in each protected area and disabled the key lock access to the other doors.	4/30/2010	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000382	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-007-1 R5.3. FRCC determined that FRCC_URE1 had Cyber Assets that could not enforce password requirements as required by CIP-007 R5.3, and were technically infeasible. FRCC_URE1 did not submit Technical Feasibility Exceptions (TFEs) in time and submitted a Self-Report on account of late submission of the TFE.	CIP-007-1	R5; R5.3	Lower	Lower	This violation posed minimal risk and not a serious or substantial risk to the reliability of the bulk power system because FRCC_URE1 has applied security controls that provide higher security for password complexity then required by CIP-007 R5.3.2.	When the Standard became mandatory and enforceable	When FRCC_URE1 submitted its TFEs	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 created and submitted TFEs for all assets that could not technically enforce CIP-007 R5.3 password complexity requirements. 16 TFEs were submitted to mitigate this item. FRCC_URE1 has applied security controls that provides higher security for password complexity then required by CIP-007 R5.3.2.	5/7/2010	3/23/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000386	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-005-1 R2.1 and 2.2. FRCC_URE1 did not apply the access control model of deny by default for its identified access points and failed to implement access control rules which permit a clearly identified unique host access to only ports and services required for normal operation. Their practice did not meet the requirement of R2.1 to provide explicit access permissions (deny by default) or R2.2 so that an access point only enables ports and services required for operations and monitoring.	CIP-005-1	R2; R2.1; R2.2	Medium	Moderate	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because the firewall rules did limit access to trusted networks and only allowed non-interactive ports and services as the interactive ports were blocked. In addition only three employees have access to the firewall ruleset and configuration files.	When the Standard became mandatory and enforceable	Mitigation Plan completion	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 modified its access control lists to build a least privilege model to bring firewalls within the requirements of the Standard. Some of the policy rules included a larger amount of hosts and were adjusted to be more specific. Rules were also reorganized to omit the "denies" within the ESP control areas. FRCC_URE1 also updated the ACLs to provide comments that better explain what firewall rules allow.	9/15/2010	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000387	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-007-1 R2. FRCC_URE1 documented but did not establish a process to ensure that only ports and services required for normal and emergency operations were enabled for the Physical Security Perimeter (PSP) access control devices at the generating sites (20 micro devices) and at the control center (4 micro devices).	CIP-007-1	R2	Medium	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because these devices use proprietary operating systems and remote access is not available from outside the FRCC_URE1 network. In addition, when accessing the micro devices from inside the network a user would need both the password and IP address which are not readily available.	When the Standard became mandatory and enforceable	Completed ports and services scan	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 created an add/remove Critical Asset/Critical Cyber Asset (CA/CCA) checklist around NERC CIP-007 R2 compliance. FRCC_URE1 reviewed and updated change and configuration management procedures to reference the CA/CCA checklist. FRCC_URE1 submitted Technical Feasibility Exceptions (TFEs) for devices where ports and services scans cannot be completed. FRCC_URE1 created add/remove checklists for CAs used in the access control and monitoring of the PSP and Electronic Security Perimeter to account for change and configuration management issues. Finally, FRCC_URE1 completed a ports and services scan.	1/31/2011	9/8/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000388	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-007-1 R5.2. FRCC determined that FRCC_URE1's factory default accounts for Cyber Assets used in the access control and monitoring of the Physical Security Perimeter (PSP) (micro devices) that authorize and/or log access to PSP(s) were not changed prior to putting the devices in service. The passwords were changed in 2010. FRCC_URE1 did not implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	CIP-007-1	R5; R5.2	Medium	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because these devices use proprietary operating systems and the account passwords are not commonly available and remote access is not available from outside the entity's network. In addition, when accessing the micro devices from inside the network a user would need both the password and IP address which are not readily available.	When the Standard became mandatory and enforceable	Date of the password change	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 completed changing factory default passwords for all the micro devices designated as Critical Cyber Assets (CCAs). FRCC_URE1 will ensure the personnel that administer these assets will be trained on the password administration requirement of the FRCC_URE1 cyber security policy. The Corporate Security procedure was revised to clarify responsibility for password maintenance on physical access control devices. FRCC_URE1 incorporated configuration management guidance in the Physical Access Control System Administration procedure to include a checklist for the addition, replacement and retirement of assets.	3/31/2011	7/13/11	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000389	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-007-1 R6.2 and 6.5. FRCC determined that FRCC_URE1 failed to properly configure logging devices to provide an alarm when a Cyber Security incident was detected and the entity failed to review the logging devices logs of system events as required by CIP-007-1 R6.2 and 6.5.	CIP-007-1	R6; R6.2; R6.5	Lower	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all the concerned devices were within the Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP), had card reader access controls and only a limited number of trusted users had access to these devices which required two-factor authentication and further, these devices did not have any control capability of the BPS.	When the Standard became mandatory and enforceable	When the devices were integrated with a central logging and monitoring solution and for the balance of devices, a Technical Feasibility Exception (TFE) was submitted)	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 submitted a Technical Feasibility Exceptions (TFE) with four mitigating factors of comparable security measures to managing shared accounts via a central password vault that requires two-factor authentication. FRCC_URE1 updated procedure to document how compliance with CIP-007 R6 will be met. FRCC_URE1 implemented technical (automated rules and alerts) and procedural changes. FRCC_URE1 integrated all Cyber Assets used in the access control and monitoring of the ESP with the enterprise logging and monitoring solution. FRCC_URE1 submitted closed-ended TFE devices and open-ended TFE devices. FRCC_URE1 applied needed configuration to close-ended devices and integrated closed-ended devices with central logging and monitoring solution.	7/31/2011	9/8/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000410	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-007-1 R5. FRCC determined that FRCC_URE1 failed to maintain list of users with access to shared accounts and shared user accounts that provide access to the Critical Cyber Assets (CCAs) (80 users) and other Cyber Assets (CAs) within the Electronic Security Perimeter (ESP), CAs used for access control and monitoring for the ESP (four users) and the Physical Security Perimeter (PSP) (three users) were not documented in the master account list.	CIP-007-1	R5	Lower	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because FRCC_URE1 failed to document the names of all individuals who had access to shared user accounts but these individuals had been appropriately granted access. In addition, two-factor authentication are required for access to the CCAs.	When the Standard became mandatory and enforceable	When FRCC_URE1 created the list of all shared and system accounts including users with authorization to use such accounts	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	For shared accounts used in the access and monitoring of the PSP, FRCC_URE1 created shared account master list 1 and updated procedure to reflect management of shared accounts. For Cyber Assets within the ESP, FRCC_URE1 created shared account master list 2 and updated worksite procedures to reflect management of shared accounts. For shared accounts used in the access and monitoring of the ESP, FRCC_URE1 created shared account master lists 3 and 4, created shared account master list 5, and updated procedure to reflect management of shared accounts.	12/23/2010	6/29/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100415	Settlement Agreement	FRCC_URE1 submitted a Self-Report to FRCC reporting a violation of CIP-004-1 R2.1. FRCC determined that one of FRCC_URE1's contractors was granted electronic access to Critical Cyber Assets (CCAs) without completing all the required training. As per CIP-004-1 R2.1, such training should be completed within 90 days from date of granting access. CIP-004-2 R2.1 requires that such training should be completed before granting any access to the CCA. The entity failed to comply with this requirement and upon realizing the error, it immediately revoked the access on June 30, 2010.	CIP-004-1	R2; R2.1	Medium	Lower	This violation posed moderate risk and not a serious or substantial risk to the reliability of the bulk power system because the contractor was from a trusted vendor, with a current personnel risk assessment (PRA), and trained on all but one of FRCC_URE1's training modules.	90 days from when the Standard became mandatory and enforceable	Date of access revocation	$55,000 (Settlement of FRCC200900254, FRCC200900317, FRCC201000314, FRCC201000315, FRCC201000382, FRCC201000386, FRCC201000387, FRCC201000388, FRCC201000389, FRCC201000410, and FRCC201100415)	Self-Report	FRCC_URE1 removed cyber access for the improperly trained contractor. The contractor completed the correct training. FRCC_URE1 consolidated the two training modules into one.	10/15/2010	7/1/2011	Neither Admits nor Denies	FRCC_URE1 has a documented internal compliance program which was reviewed and considered a neutral factor by FRCC.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201000197	Settlement Agreement	MRO_URE1 submitted a Self-Report to MRO stating that it had discovered a violation of CIP-007 R2 while it was preparing for its self-certification. The Self-Report was submitted prior to the start of the self certification submission period. MRO_URE1 had encountered various technical problems during functional testing and assessment of a third-party security provider port management solution. MRO_URE1 engaged the security provider to assist with installation and to demonstrate proof of concept of its port management solution. The security provider purported to offer a solution that allows only authorized software to execute, and to utilize the ports and other system resources. MRO_URE1 encountered various conflicts with anti-virus software, intermittent system lock-ups and screen errors while testing the port management solution. MRO_URE1 tried working with the security provider to resolve the technical problems, but the efforts were ultimately unsuccessful. Upon reviewing MRO_URE1's system configuration and Self-Report, MRO determined that MRO_URE1 failed to enable only those ports and services rec	CIP-007-1	R2	Medium	Severe	MRO determined that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS), but did pose a moderate risk to the BPS because ports were improperly enabled for most of MRO_URE1's Critical Cyber Assets (CCAs) within the Electronic Security Perimeter (ESP). Although MRO_URE1 had other protective measures employed within the ESP to detect and alert of any malicious activity such as other anti-virus software, firewall, intrusion detection system, and port restrictions configured between VLANs (virtual local area networks), improper port management increases the risk of exposure to malicious software and other forms of cyber attack.	The date on which MRO_URE1 was required to be compliant with CIP-007-1 R2.	The date on which MRO_URE1 disabled the ports and services that were enabled on the network switch.	$0	Self-Report	1. MRO_URE1 revised its Critical Infrastructure Protection policies and procedures to reflect the port management solutions. 2. MRO_URE1 disabled all ports on CCAs not necessary for normal and emergency operations. 3. The firewall has been configured for all CCAs where applicable. For CCAs that do not support the firewall, MRO_URE1 configured firewall services and VLANs on the firewall services modules residing in network switches within the ESP as mitigating controls to secure all ports not necessary for normal and emergency operations. 4. For all CCAs, the network is strategically segmented and firewall services modules are enabled to manage the network traffic that is authorized between VLANs. These measures provide a defense in depth approach, which exceeds the requirements of CIP-007-2 R2. 5. In addition, MRO_URE1 will purchase cyber security training modules related to Reliability Standards CIP-006, CIP-007 and CIP-009. These training modules will be installed on MRO_URE1's electronic system operations training center and made available to all personnel with access to CCAs. These trainin	12/27/2010	1/21/2011	Admits	MRO considered MRO_URE1's internal compliance program a mitigating factor in this enforcement action.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000437	Settlement Agreement	RFC_URE1 submitted a self report identifying a possible violation of CIP-004-2, R2.1. RFC_URE1 has an established and documented cyber security training program. In this program, RFC_URE1 states that users with authorized access to Critical Cyber Asset (CCA) shall receive CIP specific training prior to receiving access authorization. RFC_URE1 authorized unescorted physical access to an area of RFC_URE1's operations building that contains RFC_URE1's energy control system, a CCA, to an employee who had not fully completed RFC_URE1's CIP specific training. The individual required physical access to this area to perform job duties related to coordinating distribution system restoration activities. The individual's job responsibilities did not include direct contact with the energy control system, but did require the individual to work in proximity to the energy control system, thus necessitating authorized physical access pursuant to CIP-004-2. RFC_URE1's CIP training consists of two programs: (1) business Cyber Security training; and (2) basic Cyber Security and Information Protection trai	CIP-004-2	R2.1	Medium	Lower	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power (BPS). The RFC_URE1 employee to whom RFC_URE1 granted access to CCAs successfully passed a personnel risk assessment and attended partial CIP training prior to RFC_URE1's grant of unescorted physical access. Moreover, RFC_URE1 has confirmed that the employee in question did not take any action relating to the energy control system other than performing his distribution restoration functions in the proximity of the energy control system.	When RFC_URE1 had an employee that did not have CIP training to access CCAs	When RFC_URE1 revoked access to the employee	$17,000 (For RFC201000437 and RFC201000438)	Self-Report	On the same day the of discovery RFC_URE1 revoked the individual in question's unescorted physical access rights to CCAs. The employee completed training and access was restored on the same day of discovery.	9/28/2011	10/26/2011	Neither Admits nor Denies	Certain aspects of the Internal Compliance program were a partial mitigating factor.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000438	Settlement Agreement	RFC_URE1 submitted a self report identifying a possible violation of CIP-004-1, R4.1 and R4.2. On six occasions, RFC_URE1 did not update its Access Control List (ACL) of personnel with access to Critical Cyber Assets (CCAs) within seven days of a change in personnel in violation of CIP-004-1, R4.1. On three occasions, RFC_URE1 personnel failed to correctly account for data transferred during an upgrade of a physical access control system . On two occasions, RFC_URE1 personnel failed to process the underlying access removal in a timely fashion. The remaining occasion is attributable to a software issue in RFC_URE1's previous physical access control system, which has since been upgraded. Additionally, on six occasions unrelated to the six occasions of the violation of CIP-004-1, R4.1, RFC_URE1 failed to revoke access to CCAs within seven days after personnel no longer required access in violation of CIP-004-1, R4.2. On four occasions, RFC_URE1 personnel failed to ensure access revocation information was transferred to the newly upgraded physical access control system. On two occasions, RFC_URE1 personnel failed to follow established RFC_URE1 violated CIP-004-1, R4 by failing to update its lists of personnel t	CIP-004-1	R4	Medium	High	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The six individuals for whom RFC_URE1 did not update its ACL and the other six individuals for whom RFC_URE1 did not revoke access to CCAs in a timely manner all received CIP training. These individuals had also successfully completed personnel risk assessments prior to the occurrence of the violation.	When RFC_URE1 first failed to update its list of personnel to reflect a change in access rights to CCAs and revoke access to CCAs within required timeframe	When RFC_URE1 updated its list of personnel that have access rights to CCAs	$17,000 (For RFC201000437 and RFC201000438)	Self-Report	RFC_URE1's internal department that coordinates access revocation requests will review on a daily basis, all CIP operational request tickets. This process helps ensure access revocation requests are not left open beyond the 24 hour or seven day time periods required by CIP-004-1, R4. RFC_URE1 upgraded its physical access control system to improve performance of the system and establish a dedicated system for CIP regulated panels. RFC_URE1's compliance and legal personnel with the personnel involved and reiterated the CIP-004 Standard requirements and company procedures for complying with those requirements. Additionally, RFC_URE1 implemented and executed targeted awareness communications covering key elements of its CIP-004 compliance program and delivered/distributed to all CIP designated personnel and their leadership.	9/28/2011	10/26/2011	Neither Admits nor Denies	Certain aspects of the Internal Compliance program were a partial mitigating factor.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100821	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-006-3c R5, because RFC_URE1 experienced a system failure where alarms on two doors to a Physical Security Perimeter containing Critical Cyber Assets (CCAs) were not functioning properly. Specifically at 7:57 p.m., security received a system communication failure notification indicating that the alarms on two doors to a Physical Security Perimeter were not transmitting back to RFC_URE2's security. The security officers attempted to monitor the two doors with video cameras, but could not locate the applicable cameras. They then alerted the field investigator to report the issue. Throughout the night, the field investigator and other security individuals periodically monitored the two doors and brought in technicians to fix the issue. However, the technicians reported that they could not fix the issue that night. On the following morning, corporate security staff reviewed the incident report and immediately advised security to begin monitoring the two doors *via*	CIP-006-3c	R5	Medium	Severe	ReliabilityFirst determined that the violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the two doors are emergency exit only doors and cannot be opened from the outside. One of the two doors opens into the main working area at the building, which houses the system control room, and was monitored by the system control operator during the violation. In addition, all of RFC_URE2's system control operators receive cyber security training and understand the critical nature of the system control room. The other door was outside the proximity of the main working area of system control, and while the system control operator did not visually monitor it during the duration of the violation, this door was essentially sealed shut due to ongoing maintenance work. Opening the temporarily sealed door would have been very noisy, and the system control operator would most likely have heard any opening of the door.	The date on which RFC_URE2 failed to continuously monitor the access points.	The date on which monitoring resumed.	$35000 (Settlement of RFC201100821, RFC201100859, RFC201100860, RFC201100861, and RFC201100862)	Self-Report	RFC_URE2 fixed the issue with the door alarms. RFC_URE2 developed a quarterly review process of all applicable security job aids to ensure accurate information is maintained. RFC_URE2 also developed a new controls process that requires a comprehensive review, with sign off, of all changes to CCA security equipment. RFC_URE2 provided training to all security officers and corporate security field investigators on NERC requirements, CCA camera locations, types of CCA monitoring alarms and implications for those types of alarms. RFC_URE2 completed additional programming to provide direct links to any applicable cameras and playback in all CCA door alarms.	4/6/2011	6/7/2011	Neither admits nor denies/Stipulates to the Facts	ReliabilityFirst considered certain aspects of RFC_URE2's compliance program as mitigating factors.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100859	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-007-3 R5 because RFC_URE2 failed to reset a password for one account on a Critical Cyber Asset within an Electronic Security Perimeter (ESP). RFC_URE2 utilized a password reset tracking spreadsheet to track accounts in the ESP and uses that data as a basis for manually resetting passwords annually. While preparing for a routine password change task, RFC_URE2 discovered that a single account was missing from the 2010 password reset tracking spreadsheet, and it consequently failed to reset the password of that account in 2010. ReliabilityFirst determined that RFC_URE2 violated CIP-007-3 R5 by failing to change each password at least annually.	CIP-007-3	R5	Lower	Severe	ReliabilityFirst determined that the violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the missed account on the Cyber Asset resides on a server limited to archived data. In addition, RFC_URE2 changed the password annually in prior years.	The date by which RFC_URE2 should have at least annually reset the password.	The date the password was reset.	$35000 (Settlement of RFC201100821, RFC201100859, RFC201100860, RFC201100861, and RFC201100862)	Self-Report	RFC_URE2 updated the password tracking reset spreadsheet with the missing account information. RFC_URE2 reset the account password. RFC_URE2 will implement an automated process to manage the majority of the required password resets.	12/31/2011 (Approved Date)	TBD	Neither admits nor denies/Stipulates to the Facts	ReliabilityFirst considered certain aspects of RFC_URE2's compliance program as mitigating factors.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100860	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-006-3c R1.4 because RFC_URE2 failed to implement the physical security plan at its generating facility. RFC_URE2's generating facility has five different levels of Critical Cyber Asset (CCA) access, based on the needs of both employees and contractors to perform their work. RFC_URE2 discovered three instances at the generating facility where RFC_URE2's security staff granted a higher level of CCA access than the level authorized by RFC_URE2 site management. First, a RFC_URE2 security officer erroneously granted an individual employee (Employee 1) temporary, full access for approximately 16.5 hours, despite the fact that Employee 1 was authorized only for access levels 1, 2 and 3. Second, a RFC_URE2 security officer erroneously granted another individual employee (Employee 2) temporary, full access for approximately 15.5 hours, despite the fact that Employee 2 was only authorized for access levels 1, 2, 3 and 4. Third, a RFC_URE2 security officer again granted Employee 2 temporary, full access for approximately 1.5 hours because the se	CIP-006-3c	R1	Medium	Severe	ReliabilityFirst determined that the violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because both Employee 1 and Employee 2 received personnel risk assessments (PRA) and cyber security training. In addition, neither Employee 1 nor Employee 2 accessed any assets or areas beyond their respective authorized access levels.	The date of RFC_URE2's first instance of erroneously granting access rights to Employee 1.	The last date on which RFC_URE2 revoked erroneous access rights.	$35000 (Settlement of RFC201100821, RFC201100859, RFC201100860, RFC201100861, and RFC201100862)	Self-Report	RFC_URE2 revised the security procedures for its generating facility. RFC_URE2 had all security personnel at the generating facility review and sign off on the revised security procedures. RFC_URE2 created a new security procedure on the temporary CCA badge distribution process. RFC_URE2 had all appropriate security personnel review and signoff on the new procedure. RFC_URE2 administered discipline to the at-fault contracted security officer involved in the February 5, 2011 incident. RFC_URE2 reviewed all temporary CCA badge issuance and usage at the generating facility from January 1, 2010 through March 11, 2011 to ensure comprehensive identification of any additional violations.	3/14/2011	9/23/2011	Neither admits nor denies/Stipulates to the Facts	ReliabilityFirst considered certain aspects of RFC_URE2's compliance program as mitigating factors.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100861	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-006-2 R2.2 due to RFC_URE2's failure to protect its physical access control system by affording the protective measures specified in Standard CIP 007-3 R5. RFC_URE2 discovered that the database that stores data for its physical access control system software has a shared administrator account (Shared Account), for which RFC_URE2 never changed the password. Database administrators use the Shared Account to run the physical access control system and to generate related reports. In order to change the password, RFC_URE2 would have to take the physical access control system offline, which would disable physical access monitoring to Critical Cyber Assets. Therefore, RFC_URE2 did not reset the password on the Shared Account at least annually, as required by CIP-007-3 R5.3.3. In addition, RFC_URE2 identified four instances where personnel who had access to the Shared Account no longer required such access. RFC_URE2 failed to reset the password within 90 days from the date that personnel no longer required access to the Shared Account, in violation of its shared passwo	CIP-006-2	R2	Medium	Severe	ReliabilityFirst determined that the violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because none of the four individuals were terminated for cause. In addition, RFC_URE2 revoked the individuals' physical and cyber access rights, so they could not physically or electronically access the database after their employment ended. Furthermore, the system owner and IT security would be aware of human access to the Shared Account because the Shared Account is primarily accessed electronically automatically in order to run the physical access control system and generate reports, rather than by human users. Finally, RFC_URE1 tracks any attempted human use of the Shared Account with an alert sent to the system owner and to IT security. For example, over the past three months, there have been no occurrences of human use of the Shared Accounts.	The date by which RFC_URE2 should have at least annually reset the password.	The date the password was reset.	$35000 (Settlement of RFC201100821, RFC201100859, RFC201100860, RFC201100861, and RFC201100862)	Self-Report	RFC_URE2 reset the shared account password. RFC_URE2 developed an automated email notification that will inform the database administrators group and corporate security whenever there is a personnel change to the database administrators group. This would result in corporate security completing a review of the personnel change to determine if a password change is necessary. RFC_URE2 developed an automated email notification that will inform corporate security whenever there is a personnel change to the Shared Account and physical access control system test user group to corporate security. This would result in corporate security completing a review of the personnel change to determine if a password change is necessary. RFC_URE2 created an annual commitment through the company's commitments tracking database to ensure a shared account password reset is completed annually. RFC_URE2 created a physical access control system cross-functional committee that includes representatives from all stakeholder groups to be responsible for training and awareness. RFC_URE2 completed a full review of all password and confidenti	8/29/2011	10/4/2011	Neither admits nor denies/Stipulates to the Facts	ReliabilityFirst considered certain aspects of RFC_URE2's compliance program as mitigating factors.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100862	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-006-3c R6 due to its failure to record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. While conducting an annual review of its physical security plan, RFC_URE2 discovered that some of its manual log entries were incomplete. Specifically, 23 of more than 1,000 escorted visitor log entries made in a one-year period were incomplete and could not be completed with data from alternate sources. The incomplete visitor log entries, all from the generating facility, included eight log entries that were missing exit times, nine log entries that were missing the escort's name, and six log entries that were missing a combination of two of the following: escort's name, entry date, entry time or exit time.	CIP-006-3c	R6	Lower	Severe	ReliabilityFirst determined that the violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all Critical Cyber Asset access points are equipped with alarms for access denied attempts, door held situations, and door-forced situations. These alarms include a local audible alarm at each access point, in addition to notification back to security.	The date on which RFC_URE2 first failed to log a visitor entry.	The date after which there were no additional occurrences of improper logging.	$35000 (Settlement of RFC201100821, RFC201100859, RFC201100860, RFC201100861, and RFC201100862)	Self-Report	RFC_URE2 revised the Physical Security Perimeter log entry form to more clearly indicate how to properly complete the form, including format guidance and an example log entry. In addition, RFC_URE2 revised the physical security plan to include a process for regular retrieval and review of the log books. The revised physical security plan also includes a process for investigations of any log entry discrepancies.	7/1/2011	9/23/2011	Neither admits nor denies/Stipulates to the Facts	ReliabilityFirst considered certain aspects of RFC_URE2's compliance program as mitigating factors.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000696	Settlement Agreement	RFC_URE3 submitted a Self-Report to ReliabilityFirst reporting a violation of CIP-006-3c R1. RFC_URE3 reported that it did not use its visitor pass management control program appropriately, pursuant to CIP-006-3c R1.4. RFC_URE3 also determined that it did not document the entry and exit of two visitors, including the date and time, to and from RFC_URE3's Physical Security Perimeter (PSP), and did not continuously escort visitors within the PSP, pursuant to CIP-006-3c R1.6. A RFC_URE3 employee with authorized physical access to RFC_URE3's PSP used his badge to gain access to the PSP, and then allowed two maintenance employees to enter the PSP without logging the required information in the visitor's log book. In addition, the same RFC_URE3 employee failed to escort the maintenance employees inside the PSP for a period of 12 minutes while they performed the necessary repairs. When the two maintenance employees completed their repairs, they pressed the emergency release button in order to exit the PSP, which immediately notified RFC_URE3 security of the situation. RFC_URE3 security followed its docum ReliabilityFirst determined that RFC_URE3 failed to: a) Appropriately use vis	CIP-006-3c	R1	Medium	Severe	ReliabilityFirst determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). RFC_URE3 reviewed video evidence for the time period of the violation and confirmed that the violation was limited to only the two maintenance employees, both of whom worked for RFC_URE3. RFC_URE3 further verified that the two maintenance employees did not alter, and in fact did not have the ability to alter, any of the settings for the equipment in the PSP at issue. Additionally, both of the maintenance employees had authorized physical access to the plant site, and had to present their badges at multiple security points before gaining access to the plant site. Further, one of the maintenance employees has been an employee of RFC_URE3 for approximately 30 years, and voluntarily underwent CIP training prior to the violation. RFC_URE3 performed a background check for the other maintenance employee prior to the time period of the violation when he was hired in 2008, which revealed no issues.	The time period which the maintenance employees gained entry to the PSP without escort.	When RFC_URE3 secured the perimeter of the PSP.	$5,000	Self-Report	Upon discovery, RFC_URE3's CIP compliance department notified the supervisor of the RFC_URE3 employee involved in the incident, and disciplinary action was taken. RFC_URE3 also conducted re-education training for its generation CIP personnel. In this training, RFC_URE3 emphasized CIP and the RFC_URE3 CIP-006 physical security plan, which includes the appropriate visitor pass management control program.	10/28/2010	3/15/2011	Neither Admits nor Denies	ReliabilityFirst considered certain aspects of RFC_URE3's internal compliance program as mitigating factors.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002191	Settlement Agreement	In its self-report, WECC_URE1 stated that it did perform a Critical Asset Assessment as required by CIP-002-1 R2 prior to the date it was required to comply with the Standard, but the assessment was completed verbally and without written documentation. Almost a week later, WECC_URE1 submitted its Self-Certification stating it was in violation of CIP-002-1 R2. WECC_URE1 submitted a revised self-report stating that it incorrectly labeled certain assets as "Critical." WECC_URE1 submitted its Critical Asset Assessment document to WECC, which detailed WECC_URE1's Critical Assets.	CIP-002-1	R2	High	Severe	WECC determined that this violation posed a minimal risk to the reliability of the Bulk Power System (BPS). Non-identification of Critical Assets could result in the subsequent failure to protect Critical Assets essential to reliable operation of the BPS. Unidentified and unprotected Critical Assets may be vulnerable to threats and may put the operation of the BPS at risk. Though it wasn't document, WECC_URE1 performed a Critical Asset Assessment verbally which minimized risk and promoted reliable operation. Because WECC_URE1 had only three misidentified Critical Assets and WECC_URE1 has less than 100 miles of transmission lines, WECC determined that its impact on the BPS with respect to its CIP 002-1 R2 violation would be minimal.	When WECC_URE1 was required to comply with the Standard	Mitigation Plan Completion Date	$27,000 (For WECC201002191, WECC201002192, WECC201002351, WECC201002371 mad WECC201002368)	Self-Report	To mitigate these self reported issues, WECC_URE1 initiated the following milestones for completion to ensure that a reassessment of Critical Assets be performed, fully documented and approved to meet compliance requirements. -Completed the review of requirements and definitions for determining Critical Assets. -Completed the Reassessment of WECC_URE1 assets for determination of whether they are Critical Assets. -Completed the full documentation, approval, and reporting to WECC of a reassessment of critical assets for WECC_URE1. In addition, WECC_URE1 required staff to document its verbally completed Critical Cyber Asset Assessment that was completed prior to June 30, 2009, and have it reviewed, and approved by senior management for inclusion in the Mitigation completion documentation.	5/21/2010	10/22/2010	Agrees and Stipulates to the Facts	WECC reviewed WECC_URE1's Internal Compliance Program (ICP) and considered it a mitigating factor.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002192	Settlement Agreement	WECC_URE1 self-reported noncompliance with CIP-002-1 R4 for not having its Critical Asset Assessment list approved by a senior manager or a delegate thereof.	CIP-002-1	R4	Lower	High	WECC determined that this violation posed a minimal risk to the reliability of the BPS. The failure of an entity to have its list of Critical Assets reviewed and approved by a senior manager could also result in the failure of an entity to identify and protect its Critical Assets. Though it was not documented, WECC_URE1 performed a Critical Asset Assessment verbally which minimized risk and promoted reliable operation. WECC_URE1 had only three misidentified Critical Assets and WECC_URE1 has less than 100 miles of transmission lines, WECC determined that the impact on the BPS as a result of its CIP-002-1 R4 violation would be minimal.	When WECC_URE1 was required to comply with the Standard	Mitigation Plan Completion Date	$27,000 (For WECC201002191, WECC201002192, WECC201002351, WECC201002371 mad WECC201002368)	Self-Report	To mitigate these self reported issues, WECC_URE1 initiated the following milestones for completion to ensure that a reassessment of Critical Assets be performed, fully documented and approved to meet compliance requirements. -Completed the review of requirements and definitions for determining Critical Assets. -Completed the reassessment of WECC_URE1 assets for determination of whether they are Critical Assets. -Completed the full documentation, approval, and reporting to WECC of a reassessment of critical assets for WECC_URE1 In addition, WECC_URE1 required staff to document its verbally completed Critical Cyber Asset Assessment that was completed prior to the date it was required to comply with the Standard, and have it reviewed, and approved by senior management for inclusion in the Mitigation completion documentation.	5/21/2010	10/22/2010	Agrees and Stipulates to the Facts	WECC reviewed WECC_URE1's ICP and considered it a mitigating factor.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002351	Settlement Agreement	WECC_URE1 self-reported that it was in violation of CIP-003-1 R1.2 for failing to make its security policy readily available to all personnel who have access to or are responsible for Critical Cyber Assets. The next day, WECC_URE1 submitted its Self-Certification stating it was in violation of CIP-003-1 R1.2. A WECC Subject Matter Expert (SME) held a conference call to discuss WECC_URE1's self reported CIP-003-1 R1.2 violation. On the conference call, the WECC SME concluded that WECC_URE1 was not in violation of CIP-003-1 R1.2 because WECC_URE1 had made its Cyber Security Policy readily available to all personnel who have access to or are responsible for Critical Cyber Assets. However, on the conference call, the WECC SME also determined that WECC_URE1 was in violation of CIP-003-1 R1.1 and CIP-003-2 R1.1 because its Cyber Security Plan did not address all the requirements in Standards CIP-002-2 through CIP-009-2. Specifically, WECC_URE1 is in violation of CIP-003-2, R1.1 because its Cyber Security Plan did not address: • CIP-002-2, R1, R2, R3, R4; • CIP-003-2, R1, R2, R6; • CIP-004-2, R3, R4; • CIP-005-2, R1, R2, R3, R4, R5; • CIP-006-2, R1, R2, R3, R5, R6, R7, R8B; • CIP-007-2, R1, R2; • CIP-008B-2, R1, R2; and • CIP-009-2, R1, R2, R3, R5.	CIP-003-2	R1	Lower	Severe	WECC determined that this violation posed a minimal risk to the reliability of the BPS. WECC_URE1's cyber security policy did not reflect all the requirements in Standards CIP-002 through CIP-009. It is not clear that WECC_URE1's management is committed to the security of WECC_URE1's Critical Cyber Assets at the level required by the CIP Standards. Despite the failure to develop a comprehensive policy, WECC_URE1 did perform an assessment of its Critical Assets. Also, WECC_URE1 has less than 100 miles of transmission lines.	When WECC_URE1 was required to comply with the Standard	Mitigation Plan Completion Date	$27,000 (For WECC201002191, WECC201002192, WECC201002351, WECC201002371 mad WECC201002368)	Self-Report	WECC_URE1 submitted to WECC evidence including a revised WECC_URE1 Cyber Security Policy. This policy was reviewed and verified by WECC as part of WECC_URE1's Mitigation Plan.	6/30/2010	4/29/2011	Agrees and Stipulates to the Facts	WECC reviewed WECC_URE1's ICP and considered it a mitigating factor.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002371	Settlement Agreement	WECC_URE1 self-reported a potential violation of CIP-003-1 R2 because it could not provide documentation that it had assigned a senior manager responsible for implementing and assuring that WECC_URE1 was adhering to Standards CIP-002 through CIP-009. Although WECC_URE1 maintains it did designate a senior manager, WECC_URE1 was unable to provide documentation that it had designated, with all the information required by the Standard, a senior manager responsible for overall implementation of the Standards CIP-002 through CIP-009.	CIP-003-1	R2	Medium	Severe	WECC determined that this violation posed a moderate risk to the reliability of the BPS. Failure to assign a senior manager for leading and managing the entity's implementation of CIP Standards increases the risk that, due to a lack of executive supervision, the implementation of protective measures required by the CIP standards for Critical Cyber Assets. WECC_URE1 did designate a senior manager, but the designation wasn't documented. In addition, WECC_URE1 only has less than 100 miles of transmission lines making its impact on the BPS minimal. For this reason, WECC determined WECC_URE1's violation posed minimal risk to the reliability of the BPS.	When WECC_URE1 was required to comply with the Standard	Mitigation Plan Completion Date	$27,000 (For WECC201002191, WECC201002192, WECC201002351, WECC201002371 mad WECC201002368)	Self-Report	WECC_URE1 provided a document entitled that verified the manager of information technology, was designated as senior manager responsible for implementation, as well as ensuring that WECC_URE1 adheres to Standards CIP-002 through CIP-009	7/22/2009	2/8/2011	Neither Admits nor Denies	WECC reviewed WECC_URE1's ICP and considered it a mitigating factor.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002368	Settlement Agreement	WECC_URE1 self-reported a potential violation of CIP-004-1 R2.1 stating that it may be unable to provide satisfactory training records that would demonstrate training took place within the required timeframe for all applicable personnel. WECC_URE1 also self-reported a potential violation of CIP-004-1 R2.3 stating that it may be unable to provide training records for certain individuals. WECC_URE1 submitted to WECC a sufficient cyber security training program. According to WECC_URE1, its submitted cyber security training program was implemented earlier that year. A WECC Subject Matter Expert (SME) reviewed WECC_URE1's potential violations and determined that WECC_URE1 was not in violation of CIP-004-1 R2.1 or R2.3 because WECC_URE1 did provide sufficient documentation, but was in violation of CIP-004-1 R2.2 because its cyber security training program prior to the effective date did not address all of the requirements of the Standard. Based on this self-report and supporting evidence, the WECC determined that WECC_URE1 was in violation of CIP-003-2 R2.	CIP-004-1	R2	Medium	Severe	WECC determined that this violation posed a minimal risk to the reliability of the BPS. WECC_URE1 failed to have an adequate cyber security training program. Without an adequate cyber security training program, it is less likely that WECC_URE1's employees will be properly trained on cyber security exposing the BPS to an increased risk of cyber attacks. Although WECC_URE1's training program was incomplete, there was a program in place which immunized risk to the BPS and promoted reliable and safe operation. In addition, WECC_URE1 only has less than 100 miles of transmission lines. For this reason, WECC determined this violation posed minimal risk to the reliability of the BPS.	When WECC_URE1 was required to comply with the Standard	Mitigation Plan Completion Date	$27,000 (For WECC201002191, WECC201002192, WECC201002351, WECC201002371 mad WECC201002368)	Self-Report	WECC_URE1's CIP Manager submitted to WECC evidence including the newly implemented Training curriculum to personnel labeled. This program was reviewed and verified by WECC as part of WECC_URE1's Mitigation Plan.	6/15/2010	3/11/2011	Agrees and Stipulates to the Facts	WECC reviewed WECC_URE1's ICP and considered it a mitigating factor.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC200902018	Settlement Agreement	WECC_URE2 self-reported a violation of CIP-005-1 R1.5 for its failure to afford the protective measures as specified in CIP-007-1 R5.1.2 and CIP-005-1 R3 to all of its Critical Cyber Assets. During an internal investigation WECC_URE2 discovered that 10 of its Critical Cyber Asset logs were not being gathered and stored by its central log collector system and were not, in accordance with the procedures WECC_URE2 developed pursuant to CIP-007-1 R5.1.2: (1) being processed in accordance with the policies and procedures for logging user account access; and (2) being monitored for access.	CIP-005-1	R1; R1.5	Medium	High	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because logging was being generated at the device level and was available for a manual review if required.	When WECC_URE2 was required to comply with the Standard	Mitigation Plan Completion Date	$37,000 (for WECC200902018, WECC201001972, WECC201001973, and WECC201002024)	Self-Report	1. WECC_URE2 gathered and monitored logs for its 10 access control Cyber Assets. 2. WECC_URE2 improved its change control and configuration management procedure for impact evaluation of its status event monitoring systems. 3. WECC_URE2 conducted training on the revised procedure. 4. WECC_URE2 developed a verification procedure to ensure that its status event monitoring systems are collecting appropriate messages when assets are being added and provided training. 5. WECC_URE2 developed a quarterly process for manual audits to ensure that all appropriate assets are being logged.	12/1/2009	6/29/2010	Admits	WECC considered that the violation constituted WECC_URE2's first occurrence of violation of the subject NERC Reliability Standard. In addition, WECC considered as a mitigating factor that WECC_URE2 had an internal compliance program (ICP) at the time of the violation.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201001972	Settlement Agreement	WECC_URE2 self-reported a violation of EOP-005-1 R1 for its failure to provide annual training on the implementation of its system restoration plan to four power dispatchers. According to the Settlement Agreement, WECC_URE2 discovered that, in 2008, four power dispatchers had not received the required annual training on the WECC_URE2 system restoration plan. Specifically, one employee was trained after 477 days instead of within 365 days; another was trained after 408 days; the third was trained after 445 days; and the fourth employee was trained after 446 days.	EOP-005-1	R1	Medium	Lower	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because (1) all four employees that are the subject of the violation had previously received the annual training; (2) copies of the plan were readily available to all WECC_URE2 operators; and (3) the annual training requirement for 2008 was exceeded by 112, 43, 80 and 81 days for the four employees.	When WECC_URE2 first missed the annual trainig	When WECC_URE2 trained the last dispatcher	$37,000 (for WECC200902018, WECC201001972, WECC201001973, and WECC201002024)	Self-Report	WECC_URE2 updated its system restoration plan to clarify that the annual training interval shall not exceed 13 months.	5/24/2010	6/16/2010	Admits	WECC considered that the violation constituted WECC_URE2's first occurrence of violation of the subject NERC Reliability Standard. In addition, WECC considered as a mitigating factor that WECC_URE2 had an internal compliance program (ICP) at the time of the violation.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201001973	Settlement Agreement	WECC_URE2 self-reported a violation of EOP-008-0 R1 for its failure to provide annual training on the implementation of its system restoration contingency plan in the event its control center becomes inoperable to eight power dispatchers. According to the Settlement Agreement, WECC_URE2 reported that eight power dispatchers, six in 2008 and two in 2009, did not receive the required annual training. In 2008, one employee was trained after 477 days instead of within 365 days; another employee was trained after 439 days; the third employee was trained after 420 days; the fourth employee was trained after 463 days; the fifth employee was trained after 420 days and the sixth employee was trained after 671 days. With regard to 2009, one employee received training after 419 days and the second employee was trained after 421 days.	EOP-008-0	R1	High	Lower	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because all eight employees that are the subject of the violation had received the training previously, and copies of the system restoration contingency plan were readily available to all WECC_URE2 operators.	When WECC_URE2 first missed the annual trainig	When WECC_URE2 trained the last dispatcher	$37,000 (for WECC200902018, WECC201001972, WECC201001973, and WECC201002024)	Self-Report	WECC_URE2 updated its system restoration contingency plan to clarify that the annual training interval shall not exceed 13 months.	5/25/2010	6/18/2010	Admits	WECC considered that the violation constituted WECC_URE2's first occurrence of violation of the subject NERC Reliability Standard. In addition, WECC considered as a mitigating factor that WECC_URE2 had an internal compliance program (ICP) at the time of the violation.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002024	Settlement Agreement	WECC_URE2 self-reported a violation of TOP-006-1 R6 for its failure to have a sufficient range for some of its metering to accurately monitor all operating conditions for both normal and emergency situations. WECC_URE2 conducted an internal review and discovered that the Energy Management System (EMS) Supervisory Control And Data Acquisition (SCADA) scaling limits were set below an alarm setting at 55 of its 736 monitoring points. As a result of these incorrect range settings, WECC_URE2 was using inaccurate data to monitor operating conditions, and could not perform timely monitoring of operating conditions for normal or emergency situations. Twenty-six of WECC_URE2's 120 substations were affected by the subject violation.	TOP-006-1	R6	High	Severe	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: (1) at all times, WECC_URE2 operators had real-time visibility of actual and predicted line flows; (2) WECC_URE2's state estimator performs data checking and line flow verification and alerts WECC_URE2's operators of any data mismatches; (3) WECC_URE2 conducts hourly reviews with its intertie neighbors during which any meter anomaly would trigger further review; and (4) WECC_URE2 performs contingency analysis studies that highlight any approaching reliability concerns, and WECC_URE2's Balancing Authority monitors and studies WECC_URE2's transmission system.	When WECC_URE2 was required to comply with the Standard	Mitigation completion date	$37,000 (for WECC200902018, WECC201001972, WECC201001973, and WECC201002024)	Self-Report	1. WECC_URE2 lowered the alarms of the impacted lines to within the scalable limits of the identified 55 devices. 2. WECC_URE2 documented processes relative to transmission lines and associated MW, MVA and kV measurements and critical data transfer to the EMS system, including new transmission projects and existing transmission system improvements. The process documentation is intended to make sure the metering package which includes the meters, SCADA and EMS elements are reviewed for suitable range and if necessary adjusted prior to finalizing critical data alarm settings associated with issuing new transmission ratings and rerating of existing facilities. This includes any procedural documents that need to be created or modified for how work is actually accomplished. 3. WECC_URE2 established a records management process for capturing the meter package range, accuracy rating and test data. 4. WECC_URE2 evaluated key elements of its critical BPS metering packages to validate that no other insufficiencies would prevent the trigger and receipt of critical data alarms. This may inc	2/15/2011	7/8/2011	Admits	WECC considered that the violation constituted WECC_URE2's first occurrence of violation of the subject NERC Reliability Standard. In addition, WECC considered as a mitigating factor that WECC_URE2 had an internal compliance program (ICP) at the time of the violation.

Attachment A-2
October 31, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Factors Affecting the Penalty and Other Considerations
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201102640	Notice of Confirmed Violation	WECC_URE3 failed to identify personnel with access to a shared account. WECC_URE3's shared account is on 25 routers and switches which are accessible via a serial or network connection within the Physical Security Perimeter (PSP). These devices are located at WECC_URE3's Control, Backup Control Center, and Generation facilities. WECC_URE3 also failed to have a policy for managing the use of shared accounts. Consequently, WECC_URE3 could not provide an audit trail of the account's use demonstrating that the account was secure in the event of personnel changes.	CIP-007-1	R5	Lower	Severe	WECC considered this violation to have a minimal impact on the reliability of the bulk power system (BPS). In this instance, WECC_URE3 failed to implement a policy to manage shared accounts, maintain an audit trail of account use and identify personnel with access to a shared account on 25 routers and switches. These routers and switches are CCAs that are located at the three Electronic Security Perimeters (ESPs) and are used for network access and management. As a compensating measure, WECC_URE3 stated that these devices were in identified ESPs and PSPs and had protections required by CIP-005 and CIP-006. In addition, WECC_URE3 stated that intrusion detection and prevention systems are in place at these ESPs. Alerts from these systems are reviewed 24x7 at the security operations center.	When WECC_URE3 was required to be compliant with the Standard	Mitigation completion date	$8,200	Self-Certification	In its mitigation plan, WECC_URE3 identifies four milestones: (1) Network Administrator to change console-port password on all network Critical Cyber Assets and all Network Cyber Assets inside the Electronic Security Perimeter, (2) At the time of Password change, identify and document any and all personnel given the password for the console-port password, (3) Develop and document a policy for managing the use of shared accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes, and (4) Communicate the policy above to the appropriate WECC_URE3 personnel and management. The policy will require that any personnel with access to the console-port are identified and documented. In addition, passwords for this account will be changed annually.	9/10/2011	10/6/2011	Does Not Contest	WECC considered WECC_URE3's Internal Compliance Program (ICP) as a mitigating factor.