Federal Energy Regulatory Commission
Washington, D.C. 20426
January 13, 2021

FOIA No. FY19-30 (NP13-23)
Forty Eighth Determination Letter
(Release)

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This is a response to your correspondence received in January 2019, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated October 4, 2021, the submitter and an Unidentified Registered Entity (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. NP13-23, along with the names of one (1) relevant URE inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within NP13-23.

With respect to the remaining identities of UREs contained in RC13-23, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including

[1] 5 U.S.C. § 552 (2018).

[2] This docket involves multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the URE for whom FERC initially determined that disclosure of its identity may be appropriate.

whether there is a Technical Feasibility Exception involved that does not allow the Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of UREs associated with NP13-23 will not be disclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney T. Anthony Quinn by email at Tony.Quinn2@usdoj.gov, by phone at (202) 252-7558, or

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2022.01.13 15:37:27 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

Peter Sorenson, Esq.
Counsel for Mr. Mabee
petesorenson@gmail.com

James M. McGrane
Senior Counsel
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, D.C. 20005
James.McGrane@nerc.net

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
Reliability*First* Corporation (Reliability*First*)	PPL - Lower Mount Bethel Energy, LLC (LMBE)	NCR00882	RFC2011001116	Settlement Agreement	On September 9, 2011, LMBE, as a Generator Operator, submitted a Self-Report to Reliability*First* identifying a violation of VAR-002-1.1a R2 for failing to maintain generator voltage as directed by its Transmission Operator (TOP) in the voltage schedule. On September 20, 2011, LMBE submitted a revised Self-Report. LMBE follows a voltage schedule provided by PJM Interconnection, LLC (PJM), its TOP, that varies based upon the operation of the LMBE generating units and the operations of the adjacent generating station, PPL Martins Creek, L.L.C. (PPL MC). On April 20, 2010 and April 16, 2011, LMBE operated its generating units above the voltage schedule, which during those times was 233 kV, ± 4 kV. On April 20, 2010, LMBE operated between 237 kV and 241 kV for approximately ten hours (seven hours between 12:00 a.m. and 7:00 a.m., and three hours between 9:00 p.m. and 11:59 p.m.). On April 16, 2011, LMBE operated between 237 kV and 239 kV for approximately four hours. In addition, LMBE conducted an extent of condition review and discovered a total of 38 voltage excursions between March 26, 2010 and August 28, 2011. LMBE did not receive a revised voltage schedule from its TOP.	VAR-002-1.1a	R2	Medium	Lower	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 risk posed to the BPS was mitigated by the following factors. On average, LMBE's voltage excursions did not exceed 1.0% of the voltage schedule, with the greatest excursion being 2.3% of the voltage schedule. In addition, during these excursions, LMBE was operating its automatic voltage regulator (AVR) in automatic voltage control mode. PPL requested and received a letter from PJM confirming that the PPL Entities (LMBE, PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL MC, and PPL Montour, L.L.C (PPL Montour)) "have not caused any reliability concerns on the PJM Bulk Electric System with respect to their operating within the PJM voltage criteria outlined in PJM Manual 14D." This confirmation covered the period from June 18, 2007 to November 15, 2011.
Reliability*First* Corporation (Reliability*First*)	PPL - Lower Mount Bethel Energy, LLC (LMBE)	NCR00882	RFC2011001194	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that LMBE, as a Generator Owner, failed to clearly specify a maintenance and testing interval and basis, and a summary of maintenance and testing procedure for associated communications systems in its Protection System maintenance and testing program, as required by PRC-005-1 R1.1 and R1.2. Reliability*First* also determined that LMBE failed to cross-reference the basis documents for maintenance and testing intervals for relays and direct current (DC) control circuitry in its Protection System maintenance and testing program. Reliability*First* also determined that LMBE failed to include valid maintenance and testing intervals and their basis for voltage for current sensing devices in its Protection System maintenance and testing program. During the Compliance Audit, Reliability*First* discovered violations of PRC-005-1 R1 by the PPL Entities (LMBE, PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour, L.L.C. (PPL Montour)). Reliability*First* discovered that PPL BI, Holtwood, PPL MC, and PPL Montour's Protection System maintenance and testing program did not include valid maintenance and testing intervals for voltage and current sensing devices and their basis in their maintenance and testing program. Instead, the program stated that periodic maintenance for voltage and current sensing devices was not performed, but that PPL BI, PPL Holtwood, PPL MC, and PPL Montour would conduct visual inspections when accessible. PPL BI, PPL Holtwood, PPL MC, and PPL Montour presented evidence of maintenance and testing performed on voltage and current sensing devices during the time period of the violation. Nevertheless, PPL BI, PPL Holtwood, PPL MC, and PPL Montour failed to include maintenance and testing intervals and their basis, and a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.1 During the Compliance Audit, Reliability*First* found that LMBE utilized the same maintenance and testing program as its affiliates, PPL BI, PPL Holtwood, PPL MC, and PPL Montour. Subsequently, Reliability*First* determined that LMBE performed maintenance and testing under a different program that included maintenance and testing intervals and their basis and summaries of maintenance and testing procedures for voltage and current sensing devices. Reliability*First* determined there was an insufficient basis to proceed with the aspect of the violation related to LMBE. In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, the PPL Entities, including LMBE, did not correlate their basis documentation with the maintenance and testing intervals for relays and DC control circuitry. During the Compliance Audit, Reliability*First* found that the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for batteries as well. The PPL Entities previously completed a mitigation plan related to the maintenance and testing of batteries, wherein Reliability*First* reviewed their battery maintenance and testing procedure. As a result, Reliability*First* determined there was an insufficient basis to proceed with the aspect of the violation related to batteries. Specifically, the PPL Entities used a study performed by a PPL-affiliated entity, PPL Susquehanna, L.L.C., the 2001 Susquehanna Protective Relaying Study, as the basis for their maintenance and testing intervals for relays and direct current control circuitry. However, the PPL Entities failed to cross-reference the 2001 Susquehanna study in their Protection System maintenance and testing program document as the basis for their intervals. In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, PPL BI and LMBE included a general term, "control equipment," to describe the maintenance and testing interval of associated communications systems. However, the program did not define "control equipment" to specifically include associated communications systems. As a result, PPL BI and LMBE failed to clearly specify a maintenance and testing interval and basis and a summary of maintenance and testing procedures for associated communications systems in their Protection System maintenance and testing program, as required by PRC-005-1 R1.1 and R1.2.	PRC-005-1	R1	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The PPL Entities performed all maintenance and testing within defined intervals. In addition, the PPL Entities performed maintenance and testing on voltage and current sensing devices despite the lack of a periodic maintenance and testing interval. Also, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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
Reliability*First* Corporation (Reliability*First*)	PPL - Lower Mount Bethel Energy, LLC (LMBE)	NCR00882	RFC2011001195	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that LMBE, as a Generator Owner, failed to provide sufficient evidence that it performed Protection System maintenance and testing on certain Protection System devices as required by PRC-005-1 R2.1. Reliability*First* discovered violations of PRC-005-1 R2 during a Compliance Audit of the PPL Entities (LMBE, PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour, L.L.C. (PPL Montour)) because the PPL Entities failed to provide sufficient evidence that they performed maintenance and testing on their direct current (DC) control circuitry, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that the PPL Entities failed to include the last date they performed maintenance and testing on their DC control circuitry. Subsequently, Reliability*First* discovered that the PPL Entities did provide such dates, so Reliability*First* determined there was an insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in the PPL Entities' evidence of maintenance and testing is reflected in this violation of PRC-005-1 R2.1. The number of DC control circuits at issue and the total number of Protection System devices for each entity are as follows: Entity (PPL Holtwood; LMBE; PPL MC; and PPL Montour); DC circuits 1 (0.2%); 4 (2.3%); 3 (0.6%); and 4 (1.3%); Total Protection System devices 528; 172; 473; and 297. During the Compliance Audit, Reliability*First* discovered a violation for PPL BI regarding maintenance and testing of DC control circuitry. However, PPL BI submitted adequate evidence to Reliability*First* that it performed maintenance and testing on DC control circuitry. As a result, Reliability*First* did not find a violation for PPL BI for DC control circuitry. Second, PPL BI and LMBE failed to provide evidence that they performed maintenance and testing on their associated communications systems, which constitute 4 of 528 total (0.76%) Protection System devices for PPL BI and 1 of 172 total (0.58%) Protection System devices for LMBE, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that PPL BI and LMBE failed to include the last date they performed maintenance and testing on their associated communications systems. Subsequently, Reliability*First* discovered that PPL BI and LMBE did provide such dates, so Reliability*First* determined there was an insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in PPL BI and LMBE's evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1.	PRC-005-1	R2; R2.1	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. For their Protection System devices, PPL Holtwood, LMBE, PPL MC, and PPL Montour enter a date into an integrated database to indicate that they performed maintenance and testing. The test they perform on DC control circuitry is a "pass" or "fail" test. PPL Holtwood, LMBE, PPL MC, and PPL Montour would not have entered dates into the database if the device had "failed" the test. By virtue of entering a date into the database, it is implied that PPL Holtwood, LMBE, PPL MC, and PPL Montour performed testing on its DC control circuitry. Although that does not rise to the level of evidence of performing maintenance and testing, it reduces the likelihood that PPL Holtwood, LMBE, PPL MC, and PPL Montour did not perform maintenance and testing on these devices. In addition, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.
Reliability*First* Corporation (Reliability*First*)	PPL Montour, L.L.C. (PPL Montour)	NCR00888	RFC2011001196	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL Montour, as a Generator Owner, failed to include valid maintenance and testing intervals and their basis for voltage and current sensing devices in their Protection System maintenance and testing program as required by PRC-005-1 R1.1 and R1.2. Reliability*First* also determined that PPL Montour failed to cross-reference the basis documents for maintenance and testing intervals for relays and direct current (DC) control circuitry in its Protection System maintenance and testing program. During the Compliance Audit, Reliability*First* discovered violations of PRC-005-1 R1 by the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour). Reliability*First* discovered that PPL BI, PPL Holtwood, PPL MC, and PPL Montour's Protection System maintenance and testing program did not include valid maintenance and testing intervals for voltage and current sensing devices and their basis in their maintenance and testing program. Instead, the program stated that periodic maintenance for voltage and current sensing devices was not performed, but that PPL BI, PPL Holtwood, PPL MC, and PPL Montour would conduct visual inspections when accessible. Nevertheless, PPL BI, PPL Holtwood, PPL MC, and PPL Montour failed to include maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.1 In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for relays and DC control circuitry. During the Compliance Audit, Reliability*First* found that the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for batteries as well. The PPL Entities previously completed a Mitigation Plan related to the maintenance and testing of batteries, wherein Reliability*First* reviewed its battery maintenance and testing procedure. As a result, Reliability*First* determined there was an insufficient basis to proceed with the aspect of the violation related to batteries). Specifically, the PPL Entities used a study, the 2001 Susquehanna Protective Relaying Study, performed by a PPL affiliated entity, PPL Susquehanna, L.L.C., as the basis for their maintenance and testing intervals for relays and DC control circuitry. However, the PPL Entities failed to cross-reference the 2001 Susquehanna study in their Protection System maintenance and testing program document as the basis for their intervals.	PRC-005-1	R1	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The PPL Entities performed all maintenance and testing within defined intervals. In addition, the PPL Entities performed maintenance and testing on voltage and current sensing devices despite the lack of a periodic maintenance and testing interval. In addition, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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
Reliability*First* Corporation (Reliability*First*)	PPL Montour, L.L.C. (PPL Montour)	NCR00888	RFC2011001197	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL Montour, as a Generator Owner, failed to provide sufficient evidence that it performed Protection System maintenance and testing on certain Protection System devices as required by PRC-005-1 R2.1. Reliability*First* discovered violations of PRC-005-1 R2 during a Compliance Audit of the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour). PPL Holtwood, LMBE, PPL MC, and PPL Montour failed to provide sufficient evidence that they performed maintenance and testing on their direct current (DC) control circuitry, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that the PPL Entities failed to include the last date they performed maintenance and testing on their DC control circuitry. Subsequently, Reliability*First* discovered that the PPL Entities did provide such dates, so Reliability*First* determined there was an insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in the PPL Entities' evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1. The number of DC control circuits at issue and the total number of Protection System devices for each entity are as follows: Entity (PPL Holtwood; LMBE; PPL MC; and PPL Montour); DC circuits 1 (0.2%); 4 (2.3%); 3 (0.6%); and 4 (1.3%); Total Protection System devices 528; 172; 473; and 297. During the Compliance Audit, Reliability*First* discovered a violation for PPL BI regarding maintenance and testing of DC control circuitry. However, PPL BI submitted adequate evidence to Reliability*First* that it performed maintenance and testing on DC control circuitry.	PRC-005-1	R2	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. For their Protection System devices, PPL Holtwood, LMBE, PPL MC, and PPL Montour enter a date into an integrated database to indicate that they performed maintenance and testing. The test they perform on DC control circuitry is a "pass" or "fail" test. PPL Holtwood, LMBE, PPL MC, and PPL Montour would not have entered dates into the database if the device had "failed" the test. By virtue of entering a date into the database, it is implied that PPL Holtwood, LMBE, PPL MC, and PPL Montour performed testing on its DC control circuitry. Although that does not rise to the level of evidence of performing maintenance and testing, it reduces the likelihood that PPL Holtwood, LMBE, PPL MC, and PPL Montour did not perform maintenance and testing on these devices. In addition, the PPL Entities had alarms that alert the control room when a Protection System operates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.
Reliability*First* Corporation (Reliability*First*)	PPL Holtwood, L.L.C. (PPL Holtwood)	NCR00886	RFC2011001199	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL Holtwood, as a Generator Owner, failed to include valid maintenance and testing intervals and their basis for voltage and current sensing devices in their Protection System maintenance and testing program as required by PRC-005-1 R1.1 and R1.2. Reliability*First* also determined that PPL Holtwood failed to cross-reference the basis documents for maintenance and testing intervals for relays and direct current (DC) control circuitry in its Protection System maintenance and testing program. During the Compliance Audit, Reliability*First* discovered violations of PRC-005-1 R1 by the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour, L.L.C. (PPL Montour)). Reliability*First* discovered that PPL BI, PPL Holtwood, PPL MC, and PPL Montour's Protection System maintenance and testing program did not include valid maintenance and testing intervals for voltage and current sensing devices and their basis in their maintenance and testing program. Instead, the program stated that periodic maintenance for voltage and current sensing devices was not performed, but that PPL BI, PPL Holtwood, PPL MC, and PPL Montour would conduct visual inspections when accessible. PPL BI, PPL Holtwood, PPL MC, and PPL Montour presented evidence of maintenance and testing performed on voltage and current sensing devices during the time period of the violation. Nevertheless, PPL BI, PPL Holtwood, PPL MC, and PPL Montour failed to include maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.1 In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for relays and DC control circuitry. During the Compliance Audit, Reliability*First* found that the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for batteries as well. The PPL Entities previously completed a mitigation plan related to the maintenance and testing of batteries, wherein Reliability*First* reviewed its battery maintenance and testing procedure. As a result, Reliability*First* determined there was an insufficient basis to proceed with the aspect of the violation related to batteries. Specifically, the PPL Entities used a study, the 2001 Susquehanna Protective Relaying Study, performed by a PPL affiliated entity, PPL Susquehanna, L.L.C., as the basis for their maintenance and testing intervals for relays and DC control circuitry. However, the PPL Entities failed to cross-reference the 2001 Susquehanna study in their Protection System maintenance and testing program document as the basis for their intervals.	PRC-005-1	R1	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The PPL Entities performed all maintenance and testing within defined intervals. In addition, the PPL Entities performed maintenance and testing on voltage and current sensing devices despite the lack of a periodic maintenance and testing interval. In addition, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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
Reliability*First* Corporation (Reliability*First*)	PPL Holtwood, L.L.C. (PPL Holtwood)	NCR00886	RFC2011001200	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL Holtwood, as a Generator Owner, failed to provide sufficient evidence that it performed Protection System maintenance and testing on certain Protection System devices as required by PRC-005-1 R2.1. Reliability*First* discovered violations of PRC-005-1 R2 during a Compliance Audit of the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island (PPL BI), PPL Holtwood, PPL Martins Creek (PPL MC), and PPL Montour, L.L.C. (PPL Montour)). PPL Holtwood, LMBE, PPL MC, and PPL Montour failed to provide sufficient evidence that they performed maintenance and testing on their direct current (DC) control circuitry, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that the PPL Entities failed to include the last date they performed maintenance and testing on their DC control circuitry. Subsequently, Reliability*First* discovered that the PPL Entities did provide such dates, so Reliability*First* determined there was an insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in the PPL Entities' evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1. The number of DC control circuits at issue and the total number of Protection System devices for each entity are as follows: Entity (PPL Holtwood; LMBE; PPL MC; and PPL Montour); DC circuits 1 (0.2%); 4 (2.3%); 3 (0.6%); and 4 (1.3%); Total Protection System devices 528; 172; 473; and 297. During the Compliance Audit, Reliability*First* discovered a violation for PPL BI regarding maintenance and testing of DC control circuitry. However, PPL BI submitted adequate evidence to Reliability*First* that it performed maintenance and testing on DC control circuitry.	PRC-005-1	R2	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. For their Protection System devices, PPL Holtwood, LMBE, PPL MC, and PPL Montour enter a date into an integrated database to indicate that they performed maintenance and testing. The test they perform on DC control circuitry is a "pass" or "fail" test. PPL Holtwood, LMBE, PPL MC, and PPL Montour would not have entered dates into the integrated database if the device had "failed" the test. By virtue of entering a date into an integrated database, it is implied that PPL Holtwood, LMBE, PPL MC, and PPL Montour performed testing on its DC control circuitry. Although that does not rise to the level of evidence of performing maintenance and testing, it reduces the likelihood that PPL Holtwood, LMBE, PPL MC, and PPL Montour did not perform maintenance and testing on these devices. In addition, the PPL Entities had alarms that alert the control room when a Protection System operates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.
Reliability*First* Corporation (Reliability*First*)	PPL Brunner Island, L.L.C. (PPL BI)	NCR00883	RFC2011001201	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL BI, as a Generator Owner, failed to clearly specify a maintenance and testing interval and basis and a summary of maintenance and testing procedures for associated communications systems in its Protection System maintenance and testing program, as required by PRC-005-1 R1.1 and R1.2. Reliability*First* also determined that PPL BI failed to cross-reference the basis documents for maintenance and testing intervals for relays and direct current (DC) control circuitry in its Protection System maintenance and testing program. Reliability*First* also determined that PPL BI failed to include valid maintenance and testing intervals and their basis for voltage and current sensing devices in its Protection System maintenance and testing program. During the Compliance Audit, Reliability*First* discovered violations of PRC-005-1 R1 by the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL BI, PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour, L.L.C. (PPL Montour)). Reliability*First* discovered that PPL BI, PPL Holtwood, PPL MC, and PPL Montour's Protection System maintenance and testing program did not include valid maintenance and testing intervals for voltage and current sensing devices and their basis in their maintenance and testing program. Instead, the program stated that periodic maintenance for voltage and current sensing devices was not performed, but that PPL BI, PPL Holtwood, PPL MC, and PPL Montour would conduct visual inspections when accessible. PPL BI, PPL Holtwood, PPL MC, and PPL Montour presented evidence of maintenance and testing performed on voltage and current sensing devices during the time period of the violation. Nevertheless, PPL BI, PPL Holtwood, PPL MC, and PPL Montour failed to include maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.1. In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for relays and DC control circuitry. During the Compliance Audit, Reliability*First* found that the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for batteries as well. The PPL Entities previously completed a mitigation plan related to the maintenance and testing of batteries, wherein Reliability*First* reviewed its battery maintenance and testing procedure. As a result, Reliability*First* determined there was insufficient basis to proceed with the aspect of the violation related to batteries. Specifically, the PPL Entities used a study, the 2001 Susquehanna Protective Relaying Study, performed by a PPL affiliated entity, PPL Susquehanna, L.L.C., as the basis for their maintenance and testing intervals for relays and DC control circuitry. However, the PPL Entities failed to cross-reference the 2001 Susquehanna study in their Protection System maintenance and testing program document as the basis for their intervals. In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, PPL BI and LMBE included a general term, "control equipment" to describe the maintenance and testing interval of associated communications systems. However, the program did not define "control equipment" to specifically include associated communications systems. As a result, PPL BI and LMBE failed to clearly specify a maintenance and testing interval and basis and a summary of maintenance and testing procedures for associated communications systems in their Protection System maintenance and testing program, as required by PRC-005-1 R1.1 and R1.2.	PRC-005-1	R1	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The PPL Entities performed all maintenance and testing within defined intervals. In addition, the PPL Entities performed maintenance and testing on voltage and current sensing devices despite the lack of a periodic maintenance and testing interval. In addition, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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
Reliability*First* Corporation (Reliability*First*)	PPL Brunner Island, L.L.C. (PPL BI)	NCR00883	RFC2011001202	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL BI, as a Generator Owner, failed to provide sufficient evidence that it performed Protection System maintenance and testing on certain Protection System devices as required by PRC-005-1 R2.1. Reliability*First* discovered violations of PRC-005-1 R2 during a Compliance Audit of the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL BI, PPL Holtwood, L.L.C. (PPL Holtwood), PPL Martins Creek, L.L.C. (PPL MC), and PPL Montour, L.L.C. (PPL Montour)). PPL Holtwood, LMBE, PPL MC, and PPL Montour failed to provide sufficient evidence that they performed maintenance and testing on their direct current (DC) control circuitry, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that the PPL Entities failed to include the last date they performed maintenance and testing on their DC control circuitry. Subsequently, Reliability*First* discovered that the PPL Entities did provide such dates, so Reliability*First* determined there was insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in the PPL Entities' evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1. The number of DC control circuits at issue and the total number of Protection System devices for each entity are as follows: Entity (PPL Holtwood; LMBE; PPL MC; and PPL Montour); DC circuits 1 (0.2%); 4 (2.3%); 3 (0.6%); and 4 (1.3%); Total Protection System devices 528; 172; 473; and 297. During the Compliance Audit, Reliability*First* discovered a violation for PPL BI regarding maintenance and testing of DC control circuitry. However, PPL BI submitted adequate evidence to Reliability*First* that it performed maintenance and testing on DC control circuitry. As a result, Reliability*First* did not determine a violation for PPL BI for DC control circuitry. Second, PPL BI and LMBE failed to provide evidence that they performed maintenance and testing on their associated communications systems, which constitute 4 of 528 total (0.76%) Protection System devices for PPL BI and 1 of 172 total (0.58%) Protection System devices for LMBE, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that PPL BI and LMBE failed to include the last date they performed maintenance and testing on their associated communications systems. Subsequently, Reliability*First* discovered that PPL BI and LMBE did provide such dates, so Reliability*First* determined there was an insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in PPL BI and LMBE's evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1.	PRC-005-1	R2; R2.1	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. For their Protection System devices, PPL Holtwood, LMBE, PPL MC, and PPL Montour enter a date into an integrated database to indicate that they performed maintenance and testing. The test they perform on DC control circuitry is a "pass" or "fail" test. PPL Holtwood, LMBE, PPL MC, and PPL Montour would not have entered dates into the integrated database if the device had "failed" the test. By virtue of entering a date into an integrated database, it is implied that PPL Holtwood, LMBE, PPL MC, and PPL Montour performed testing on its DC control circuitry. Although that does not rise to the level of evidence of performing maintenance and testing, it reduces the likelihood that PPL Holtwood, LMBE, PPL MC, and PPL Montour did not perform maintenance and testing on these devices. In addition, the PPL Entities had alarms that alert the control room when a Protection System operates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.
Reliability*First* Corporation (Reliability*First*)	PPL Brunner Island, L.L.C. (PPL BI)	NCR00883	RFC2011001203	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL BI, as a Generator Owner, failed to maintain generator voltage as directed by the Transmission Operator (TOP) in the voltage schedule as required by VAR-002-1.1a R2. Until March 25, 2011 when PPL BI's TOP, PJM Interconnection LLC (PJM), revised its voltage schedule, PPL BI was required to operate its generating units following a variable voltage schedule. This variable schedule included three voltage levels for weekdays and two levels for weekends and holidays, with a voltage tolerance bandwidth of ±4.0 kV. However, PPL BI operated its generating units outside of that variable voltage schedule 22 times between January 1, 2010 and March 25, 2011 when the TOP revised the voltage schedule. When PPL BI compared the operating data for January 1, 2010 through March 25, 2011 to the revised voltage schedule, all data was within the bandwidth of the new voltage schedule.	VAR-002-1.1a	R2	Medium	Lower	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. On average, PPL BI's voltage excursions did not exceed 1.0% of the voltage schedule. In addition, PPL BI operated with its automatic voltage regulator (AVR) in automatic mode during this period. PPL requested and received a letter from PJM confirming that the PPL Generation entities "have not caused any reliability concerns on the PJM Bulk Electric System with respect to their operating within the PJM voltage criteria outlined in PJM Manual 14D." This confirmation covered the period from June 18, 2007 to November 15, 2011.
Reliability*First* Corporation (Reliability*First*)	PPL Martins Creek, L.L.C. (PPL MC)	NCR00887	RFC2011001204	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL MC, as a Generator Owner, failed to include valid maintenance and testing intervals and their basis for voltage and current sensing devices in their Protection System maintenance and testing program as required by PRC-005-1 R1.1 and R1.2. Reliability*First* also determined that LMBE failed to cross-reference the basis documents for maintenance and testing intervals for relays and direct current (DC) control circuitry in its Protection System maintenance and testing program. During the Compliance Audit, Reliability*First* discovered violations of PRC-005-1 R1 by the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL MC, and PPL Montour, L.L.C. (PPL Montour)). Reliability*First* discovered that PPL BI, PPL Holtwood, PPL MC, and PPL Montour's Protection System maintenance and testing program did not include valid maintenance and testing intervals for voltage and current sensing devices and their basis in their maintenance and testing program. Instead, the program stated that periodic maintenance for voltage and current sensing devices was not performed, but that PPL BI, PPL Holtwood, PPL MC, and PPL Montour would conduct visual inspections when accessible. PPL BI, PPL Holtwood, PPL MC, and PPL Montour presented evidence of maintenance and testing performed on voltage and current sensing devices during the time period of the violation. Nevertheless, PPL BI, PPL Holtwood, PPL MC, and PPL Montour failed to include maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.1 In addition, in their Protection System maintenance and testing program in effect until August 1, 2010, the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for relays and DC control circuitry. During the Compliance Audit, Reliability*First* found that the PPL Entities did not correlate their basis documentation with the maintenance and testing intervals for batteries as well. The PPL Entities previously completed a Mitigation Plan related to the maintenance and testing of batteries, wherein Reliability*First* reviewed its battery maintenance and testing procedure. As a result, Reliability*First* determined there was insufficient basis to proceed with the aspect of the violation related to batteries. Specifically, the PPL Entities used a study performed by a PPL affiliated entity, PPL Susquehanna, L.L.C., the 2001 Susquehanna Protective Relaying Study, as the basis for their maintenance and testing intervals for relays and DC control circuitry. However, the PPL Entities failed to cross-reference the 2001 Susquehanna study in their Protection System maintenance and testing program document as the basis for their intervals.	PRC-005-1	R1	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The PPL Entities performed all maintenance and testing within defined intervals. In addition, the PPL Entities performed maintenance and testing on voltage and current sensing devices despite the lack of a periodic maintenance and testing interval. In addition, the PPL Entities have alarms that alert the control room when a Protection System misoperates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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
Reliability*First* Corporation (Reliability*First*)	PPL Martins Creek, L.L.C. (PPL MC)	NCR00887	RFC2011001205	Settlement Agreement	During a Compliance Audit, conducted from September 12, 2011 through September 30, 2011, Reliability*First* determined that PPL MC, as a Generator Owner, failed to provide sufficient evidence that it performed Protection System maintenance and testing on certain Protection System devices as required by PRC-005-1 R2.1. Reliability*First* discovered violations of PRC-005-1 R2 during a Compliance Audit of the PPL Entities (PPL - Lower Mount Bethel Energy, LLC (LMBE), PPL Brunner Island, L.L.C. (PPL BI), PPL Holtwood, L.L.C. (PPL Holtwood), PPL MC, and PPL Montour, L.L.C. (PPL Montour)). PPL Holtwood, LMBE, PPL MC, and PPL Montour failed to provide sufficient evidence that they performed maintenance and testing on their direct current (DC) control circuitry, as required by PRC-005-1 R2.1. During the Compliance Audit, Reliability*First* found that the PPL Entities failed to include the last date they performed maintenance and testing on their DC control circuitry. Subsequently, Reliability*First* discovered that the PPL Entities did provide such dates, so Reliability*First* determined there was insufficient basis to proceed with this aspect of the violation. It was unclear, however, what occurred on those dates, and as a result, the lack of clarity in the PPL Entities' evidence of maintenance and testing is reflected in the violation of PRC-005-1 R2.1. The number of DC control circuits at issue and the total number of Protection System Devices for each entity are as follows: Entity (PPL Holtwood; LMBE; PPL MC; and PPL Montour); DC circuits 1 (0.2%); 4 (2.3%); 3 (0.6%); and 4 (1.3%); Total Protection System devices 528; 172; 473; and 297. During the Compliance Audit, Reliability*First* discovered a violation for PPL BI regarding maintenance and testing of DC control circuitry. However, PPL BI submitted adequate evidence to Reliability*First* that it performed maintenance and testing on DC control circuitry.	PRC-005-1	R2	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. For their Protection System devices, PPL Holtwood, LMBE, PPL MC, and PPL Montour enter a date into an integrated database to indicate that they performed maintenance and testing. The test they perform on DC control circuitry is a "pass" or "fail" test. PPL Holtwood, LMBE, PPL MC, and PPL Montour would not have entered dates into the integrated database if the device had "failed" the test. By virtue of entering a date into an integrated database, it is implied that PPL Holtwood, LMBE, PPL MC, and PPL Montour performed testing on its DC control circuitry. Although that does not rise to the level of evidence of performing maintenance and testing, it reduces the likelihood that PPL Holtwood, LMBE, PPL MC, and PPL Montour did not perform maintenance and testing on these devices. In addition, the PPL Entities had alarms that alert the control room when a Protection System operates. Furthermore, the PPL Entities have backup and redundant protection in place for all Protection System devices except the PPL MC units, which do not have 100% redundancy.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
3/26/2010 (when LMBE first exceeded its voltage schedule)	8/28/2011 (when LMBE resumed operating within its voltage schedule)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Self-Report	To mitigate this violation, LMBE: 1) Set up local plant alarms to provide notification when voltage schedule limits are approached or exceeded; 2) Advised LMBE combined cycle technicians (CCTs) of the VAR-002 issue, ensured that the CCTs understood the procedure to notify the generation power dispatch if the voltage schedule cannot be met or the plant is at a VAR limit; 3) Performed testing to verify or adjust VAR limits, and submitted new limits to PJM; 4) Set the distributed control system to automatically change the AVR's voltage set points based on changes in the voltage schedule due to the number of PPL MC units being in service; 5) Conducted an internal review of sample operating data to identify the extent of voltage excursions that were not within Facility Rating constraints; and 6) Revised voltage schedules and/or bandwidths as appropriate, based on internal reviews of VAR limits and voltage schedules and coordination with its Transmission Owner and TOP.	6/30/2012	10/22/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the fact that it discovered this violation through Self-Report, and applied mitigating credit. ReliabilityFirst did not apply mitigating credit for the violation, RFC2011001116, self-reported three days prior to the start of the Compliance Audit. ReliabilityFirst considered the fact that it discovered 11 of the violations during the Compliance Audit, rather than through a Self-Report and did not apply mitigating credit. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering a violation of VAR-002-1 R3 for PPL Montana, LLC was filed with FERC under NP10-59-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of VAR-002-1.1b.
6/18/2007 (when the Standard became mandatory and enforceable)	3/30/2012 (when the PPL Entities revised their Protection System maintenance and testing program)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities: 1) Restructured their Protection System maintenance and testing program by developing a new organization that is responsible for Protection System maintenance and testing; 2) Drafted new procedures for DC control circuitry, and voltage and current sensing devices. The maintenance and testing interval is 12 years, and the basis for the interval is included in the program; and 3) Prepared a PRC-005 summary table as part of their overall PRC-005 maintenance and training program. The summary table identified the intervals and cross-referenced the basis for the intervals with the PRC-005 categories of equipment, including associated communications systems. This summary table format listed all the required information that was included in various program documents in a single-page format.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst . ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
6/18/2007 (when the Standard became mandatory and enforceable)	9/14/2012 (Mitigation Plan completion date)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities revised testing procedures and associated test forms for DC control circuitry and communications devices. These new forms document the completion of testing.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.
6/18/2007 (when the Standard became mandatory and enforceable)	3/30/2012 (when the PPL Entities revised their Protection System maintenance and testing program)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, PPL Montour: 1) Restructured its Protection System maintenance and testing program by developing a new organization that is responsible for Protection System maintenance and testing; 2) The new organization drafted new procedures for DC control circuitry and voltage and current sensing devices. The maintenance and testing interval is 12 years, and the basis for the interval is included in the program; and 3) The PPL Entities prepared a PRC-005 summary table as part of their overall PRC-005 maintenance and training program. The summary table identified the intervals and cross-referenced the basis for the intervals with the PRC-005 categories of equipment, including communications systems. This summary table format listed all the required information that was included in various program documents in a single page format.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
6/18/2007 (when the Standard became mandatory and enforceable)	9/14/2012 (Mitigation Plan completion)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities included revised testing procedures and associated test forms for DC control circuitry and communications devices. These new forms document the completion of testing.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.
6/18/2007 (when the Standard became mandatory and enforceable)	3/30/2012 (when the PPL Entities revised their Protection System maintenance and testing program)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, PPL Holtwood: 1) Restructured its Protection System maintenance and testing program by developing a new organization that is responsible for Protection System maintenance and testing; 2) The new organization drafted new procedures for DC control circuitry and voltage and current sensing devices. The maintenance and testing interval is 12 years, and the basis for the interval is included in the program; and 3) The PPL Entities prepared a PRC-005 summary table as part of their overall PRC-005 maintenance and training program. The summary table identified the intervals and cross-referenced the basis for the intervals with the PRC-005 categories of equipment, including communications systems. This summary table format listed all the required information that was included in various program documents in a single page format.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
6/18/2007 (when the Standard became mandatory and enforceable)	9/14/2012 (Mitigation Plan completion)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities included revised testing procedures and associated test forms for DC control circuitry and communications devices. These new forms document the completion of testing.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst . ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.
6/18/2007 (when the Standard became mandatory and enforceable)	3/30/2012 (when the PPL Entities revised their Protection System maintenance and testing program)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, PPL BI: 1) Restructured its Protection System maintenance and testing program by developing a new organization that is responsible for Protection System maintenance and testing; 2) The new organization drafted new procedures for DC control circuitry and voltage and current sensing devices. The maintenance and testing interval is 12 years, and the basis for the interval is included in the program; and 3) The PPL Entities prepared a PRC-005 summary table as part of their overall PRC-005 maintenance and training program. The summary table identified the intervals and cross-referenced the basis for the intervals with the PRC-005 categories of equipment, including communications systems. This summary table format listed all the required information that was included in various program documents in a single page format.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst . ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
6/18/2007 (when the Standard became mandatory and enforceable)	10/31/2012 (proposed Mitigation Plan completion date)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities included revised testing procedures and associated test forms for DC control circuitry and communications devices. These new forms document the completion of testing.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.
1/1/2010 (when PPL BI first exceeded its voltage schedule)	10/3/2010 (when PPL BI last exceeded its voltage schedule)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, PPL BI reviewed the voltage operating data and, as necessary, requested revised voltage schedules from the Transmission Operator. PPL BI determined that no changes to its voltage schedule were required.	6/30/2012	10/22/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst did not apply mitigating credit for the violation, RFC2011001116, because self-reported three days prior to the start of the Compliance Audit. ReliabilityFirst considered the fact that it discovered 11 of the violations during the Compliance Audit, rather than through a Self-Report and did not apply mitigating credit. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering a violation of VAR-002-1 R3 for PPL Montana, LLC was approved filed with FERC under NP10-59-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of VAR-002-1.1b.
6/18/2007 (when the Standard became mandatory and enforceable)	3/30/2012 (when the PPL entities revised their Protection System maintenance and testing program)	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, PPL MC: 1) Restructured its Protection System maintenance and testing program by developing a new organization that is responsible for Protection System maintenance and testing; 2) The new organization drafted new procedures for DC control circuitry and voltage and current sensing devices. The maintenance and testing interval is 12 years, and the basis for the interval is included in the program; and 3) The PPL Entities prepared a PRC-005 summary table as part of their overall PRC-005 maintenance and training program. The summary table identified the intervals and cross-referenced the basis for the intervals with the PRC-005 categories of equipment, including communications systems. This summary table format listed all the required information that was included in various program documents in a single-page format.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the fact that it discovered one of the violations through Self-Report, and applied mitigating credit. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted Mitigation Plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC , a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-1
January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

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	"Admits," "Agrees/Stipulates," "Neither Admits nor	Factors Affecting the Penalty and Other Considerations
6/18/2007 (when the Standard became mandatory and enforceable)	9/14/2012 (Mitigation Plan completion	$0 (for RFC2011001116, RFC2011001194, RFC2011001195, RFC2011001196, RFC2011001197, RFC2011001199, RFC2011001200, RFC2011001201, RFC2011001202, RFC2011001203, RFC2011001204, and RFC2011001205)	Compliance Audit	To mitigate this violation, the PPL Entities included revised testing procedures and associated test forms for DC control circuitry and communications devices. These new forms document the completion of testing.	9/14/2012	11/6/2012	Admits	ReliabilityFirst considered certain aspects of the PPL Corporation's (PPL) internal compliance program (ICP) as a mitigating factor in the penalty determination. PPL's ICP governs the compliance activities of PPL's subsidiaries in the ReliabilityFirst region. PPL's chief compliance officer has independent access to the CEO as well as the Board of Directors, and senior management both supports and participates in compliance activities. PPL operates and manages its NERC compliance program separately from the departments primarily responsible for performance to the Standards. PPL has in place a responsible behavior program that consists of systematic reminders along with coaching and counseling, which is intended to correct unacceptable behaviors. Importantly, PPL cultivates a culture of compliance by motivating its employees to identify possible compliance issues. PPL implements a process to encourage employees to identify possible compliance issues, which in turn enables PPL to both promptly mitigate these compliance issues and self-report possible violations of the Reliability Standards to ReliabilityFirst. ReliabilityFirst considered the positive degree and quality of the PPL Entities' cooperation and remedial action during the enforcement processes and applied mitigating credit. The PPL Entities were cooperative throughout their interaction with ReliabilityFirst in connection with these violations. When assessing the penalty for the instant violations, ReliabilityFirst considered whether the facts of these violations evidenced any: (a) repeated or continuing conduct similar to that underlying a prior violation of the same or a closely related Reliability Standard Requirement; (b) conduct addressed in any previously submitted mitigation plan for a prior violation of the same or a closely-related Reliability Standard Requirement; or (c) multiple violations of the same Standard and Requirement. A Settlement Agreement covering violations of PRC-005-1 R2 for PPL BI, LMBE, PPL Holtwood, PPL MC, and PPL Montour was filed with FERC under NP11-74-000 on December 22, 2010. On January 21, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering a violation of PRC-005-1 R2.1 for PPL Electric Utilities was filed with FERC under NP10-71-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In addition, a Settlement Agreement covering violations of PRC-005-1 R2.1 for PPL Montana, LLC, a PPL affiliated entity, was filed with FERC under NP10-57-000 on March 1, 2010. On March 31, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. As a result, ReliabilityFirst considered the PPL Entities' violation history as an aggravating factor in the penalty determination for the violations of PRC-005-1.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007586	Settlement Agreement	FRCC_URE1 self-reported a violation of CIP-007-1 R4.1. Specifically, FRCC_URE1 failed to install and/or use anti-virus software and other malware prevention tools on workstations classified as Critical Cyber Assets (CCAs) even though it was technically feasible to do so. Instead of installing anti-virus software on each CCA, FRCC_URE1 maintained alternate, comparable security measures which included a network-based intrusion detection system (IDS) designed to protect all of the CCAs within FRCC_URE1's Electronic Security Perimeters (ESPs). FRCC_URE1 depended on its perimeter devices such as its IDS and hardened vendor-specified configuration to mitigate the risk of malware and maintained a locked down environment where all updates were evaluated for malware detection. However, FRCC_URE1's anti-virus and malware prevention measures were not sufficient for compliance with CIP-007-1 R4.1.	CIP-007-1	R4; R4.1
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007803	Settlement Agreement	During a NERC CIP Compliance Spot Check, FRCC determined that FRCC_URE1 was in violation of CIP-005-1 R2. Specifically, FRCC_URE1 failed to demonstrate that it applied access mechanisms at access points to the Electronic Security Perimeter (ESP) that use an access control model that denies access by default, such that explicit access permissions are specified. On the access points at issue, FRCC_URE1 did not specify explicit permissions for different trusted subnets, in violation of R2.1. FRCC_URE1 also failed to enable only ports and services required for normal and emergency operations, in violation of R2.2.	CIP-005-1	R2; R2.1; R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 devices were protected within the ESP, and FRCC_URE1 maintained a locked down environment where all updates were validated to ensure that they did not contain any malware, during the pendency of the violation. FRCC_URE1 maintains a hardened system environment where only energy management system (EMS) vendor-approved applications and configurations are installed. Any new application is installed after two levels of testing conducted by FRCC_URE1 and FRCC_URE1's EMS vendor. FRCC_URE1 also maintained an IDS which, for the duration of the violation, scanned and protected all network segments and monitored and logged all activities for these access points.
Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS). All of the subnets for which FRCC_URE1 failed to specify permissions were trusted subnets that were either owned and operated by FRCC_URE1's corporate groups or owned and operated by a secure vendor. FRCC_URE1 did not provide access to subnets from any unknown sources or other traffic and indicated that other traffic was denied at all of FRCC_URE1's access points. Access to the subnet owned and secured by FRCC_URE1's energy management system (EMS) vendor was controlled and secured by the entity at all times. FRCC_URE1 also maintained a complete intrusion detection system (IDS) which scanned and protected all network segments and monitored and logged all activities for each of the relevant access points.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to FRCC_URE1	when FRCC_URE1 updated its risk-based assessment methodology (RBAM)	$8,000 (for FRCC2011007586 and FRCC2011007803)	Self-Report	To mitigate this violation, FRCC_URE1 updated its RBAM to apply risk-based criteria based on CIP Version 4 Standards approved by FERC. FRCC_URE1 revised its systems management procedures document to state that all Cyber Assets within the ESP must have anti-virus and malware prevention tools installed, unless technically infeasible. This revision includes the requirement that, where technically infeasible, a Technically Feasibility Exception (TFE) will be submitted and compensating measures must be applied to mitigate risk exposure. Further, FRCC_URE1 updated and corrected its access control list of associated CCAs. The subject assets are no longer classified as CCAs. FRCC_URE1's staff was trained on the revised procedures to provide a clearer understanding of the requirements and further minimize the probability of future violations.	5/7/2012	10/23/2012	Neither Admits nor Denies
when the Standard became mandatory and enforceable to FRCC_URE1	when FRCC_URE1 updated its risk-based assessment methodology (RBAM)	$8,000 (for FRCC2011007586 and FRCC2011007803)	Spot Check	To mitigate this violation, FRCC_URE1 updated its RBAM to apply risk-based criteria based on CIP Version 4 Standards approved by FERC. Further, FRCC_URE1 updated and corrected its access control list of associated Critical Cyber Assets (CCAs) and access points. The assets within the subject ESPs are no longer classified as CCAs.	11/21/2011	10/23/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
FRCC_URE1 had an internal compliance program (ICP), in place at the time of the violation, which FRCC considered to be a mitigating factor in the penalty determination. Because FRCC_URE1 self-reported this violation shortly before a scheduled Spot Check, FRCC did not award credit for self-reporting the violation.
FRCC_URE1 had an internal compliance program (ICP), in place at the time of the violation, which FRCC considered to be a mitigating factor in the penalty determination. FRCC considered FRCC_URE1's compliance history a neutral factor in the penalty determination. FRCC_URE1 also corrected deficiencies in its firewall rules, which FRCC considered to be a mitigating factor in the penalty determination.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001001; RFC2011001070	Settlement Agreement	RFC_URE1 self-reported non-compliance with CIP-003-3 R6. RFC_URE1 reported that it did not implement its documented change control process when it replaced its anti-virus software with another anti-virus software on April 19, 2011, in violation of this Standard. (Violation ID:RFC2011001001) RFC_URE1 self-reported one additional instance of noncompliance with CIP-003-3 R6. (Violation ID: RFC2011001070) RFC_URE1 reported that on October 21, 2010, RFC_URE1 installed a firewall into its Electronic Security Perimeter (ESP) without implementing the change management procedures required by CIP-003-3 R6. ReliabilityFirst determined that RFC_URE1 violated CIP-003-3 R6 on two occasions, for a failure to implement its configuration management activities to document the changes it made to its firewall and to its anti-virus software.	CIP-003-3	R6
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001138	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. As a result of the Compliance Audit, ReliabilityFirst discovered that RFC_URE1 was in violation of CIP-004-3 R2.1. ReliabilityFirst discovered that RFC_URE1 granted two employees unescorted physical access and cyber access to Critical Cyber Assets (CCAs) prior to those employees completing required cyber security training. The two employees at issue included a systems administrator, who worked at the corporate helpdesk, and an executive level employee. ReliabilityFirst determined that RFC_URE1 granted two employees access to CCAs prior to providing those two employees with cyber security training, in violation of CIP-004-3 R2.1.	CIP-004-2; CIP-004-3	R2.1

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower	Severe	These violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, RFC_URE1 has a documented change management procedure in which RFC_URE1 addresses adding, modifying, replacing or removing Critical Cyber Asset (CCA) hardware or software as well as communication, resources, tools, configuration control processes, emergency change process, and roles and responsibilities. Second, the two violations at issue were isolated incidents that do not indicate a systemic compliance issue at RFC_URE1.
Medium	Severe	ReliabilityFirst and RFC_URE1 agreed and stipulated 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). NERC, based on evaluation of the facts and circumstances of this violation and similar violations from other regions, determined that this violation posed a minimal risk to the reliability of the BPS. The risk was mitigated by the following factors. First, both employees at issue underwent personnel risk assessments (PRAs) prior to RFC_URE1 authorizing access to CCAs. The PRAs did not identify any criminal history or issues that would have precluded RFC_URE1 from granting these employees access to CCAs. RFC_URE1 never provided the two employees at issue with the key cards necessary for either of the employees to independently access RFC_URE1's Physical Security Perimeter (PSP). Additionally, neither employee at issue ever entered the PSP without an appropriate escort, nor did either employee use their cyber access to gain access to CCAs during the duration of the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE1 installed the firewall into the ESP	when RFC_URE1 implemented its change management process and configuration management activities to document the changes it made to its firewall and anti-virus system	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Self-Report	In accordance with its Mitigation Plan, RFC_URE1 took the following actions: 1) Implemented a communications program to ensure all appropriate departments at RFC_URE1 are aware of any changes to its CCAs; and 2) Trained all relevant staff on its change management procedure for adding, modifying, replacing or removing CCA hardware or software.	7/7/2011	4/20/2012	Neither Admits nor Denies
when RFC_URE1 granted the employees access to CCAs	when both employees completed the required training	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 took the following actions: 1) Conducted the required cyber security training for the two employees at issue; 2) Revised its cyber security training procedure to minimize the possibility of RFC_URE1 granting an individual physical or cyber access to CCAs prior to completing the required cyber security training; 3) Notified all staff engaged in managing access to the CCAs the changes made to the documentation relevant to CIP-004 R2 and R3; and 4) Committed to perform periodic self-assessments of its access list to help ensure that only those individuals who have completed cyber security training have been granted access to CCAs.	5/1/2012	7/19/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001139	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. During the Compliance Audit, ReliabilityFirst determined that RFC_URE1 granted an employee unescorted physical access to Critical Cyber Assets (CCAs) prior to completing a personnel risk assessment (PRA) for that employee, in violation of CIP-004-3 R3. The employee at issue is RFC_URE1's manager of Federal Energy Regulatory Commission compliance.	CIP-004-2; CIP-004-3	R3
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001140	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. During the Compliance Audit, ReliabilityFirst determined that RFC_URE1 did not include the discovery of all access points to the Electronic Security Perimeter (ESP) or controls for default accounts, passwords, and network management community strings in its cyber vulnerability assessment, in violation of CIP-005-3 R4.3 and R4.4. ReliabilityFirst determined RFC_URE1 cyber vulnerability assessment, which RFC_URE1 did not include evidence demonstrating that RFC_URE1 performed an assessment to determine all access points to the ESP. Additionally, ReliabilityFirst determined RFC_URE1 could not provide evidence that it conducted a review of controls for default accounts, passwords, and network management community strings during its cyber vulnerability assessment. Community strings are passwords for network elements and are used to retrieve data from network elements.	CIP-005-2; CIP-005-3	R4.3; R4.4

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by several factors. First, the employee at issue completed the required CIP training prior to RFC_URE1 granting unauthorized unescorted physical access to CCAs. Additionally, when RFC_URE1 completed the PRA for the employee at issue, RFC_URE1 did not discover any criminal history or identity issues that would have precluded RFC_URE1 from granting the employee access to CCAs. Further, RFC_URE1 never provided the employee at issue with a key card necessary for the employee to independently access RFC_URE1's Physical Security Perimeter (PSP). Finally, the employee at issue never physically accessed the PSP without an escort during the duration of the violation.
Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although RFC_URE1 did not include a review of all access points to the ESP or controls for default accounts, passwords, and network management community strings, during this violation, RFC_URE1 protected all access points into the ESP with an intrusion prevention system that included logging, alerting, and constant monitoring of all access points.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE1 granted the employee unescorted physical access to CCAs	when RFC_URE1 completed the required PRA for the employee	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 took the following actions: 1) Conducted the PRA for the employee; 2) Revised its cyber security training procedure to minimize the possibility of granting an individual physical or cyber access to CCAs prior to the completion of a PRA; and 3) Notified all staff engaged in managing access to the CCAs the changes made to the documentation relevant to CIP-004 R2 and R3; and 4) Committed to perform periodic self-assessments of its access list to ensure only those individuals who have completed cyber security training and PRAs have access to CCAs.	6/15/2012	7/19/2012	Neither Admits nor Denies
when RFC_URE1 did not include a review of all access points to the ESP or controls for default accounts, passwords, and network management community strings	when RFC_URE1 completed a cyber vulnerability assessment that included the requirements of the Standard at issue	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 performed a cyber vulnerability assessment that included a review of all access points to the ESP, as well as controls for default accounts, passwords, and network management community strings. RFC_URE1 also updated all documentation relevant to the standard to assure that it is aligned with the requirement and establishes the expectations to maintain a state of compliance. After the documentation was updated, RFC_URE1 notified the changes to all staff that are engaged in managing access to the CCAs.	6/12/2012	8/21/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001144	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. During the Compliance Audit, ReliabilityFirst determined that RFC_URE1 violated CIP-007-3 R5 when it did not manage accounts in a manner that minimizes risk of unauthorized system access pursuant to CIP-007-3 R5 and several of this Standard's subrequirements. First, ReliabilityFirst determined RFC_URE1 was unable to demonstrate it granted access to individual and shared system accounts as well as authorized access permissions consistent with the concept of "need to know" with respect to work functions performed, in violation of CIP-007-3 R5.1. Second, ReliabilityFirst determined RFC_URE1 could not demonstrate it conducted an annual review of all its user accounts and access privileges, in violation of CIP-007-3 R5.1.3. Several individuals had access privileges for which RFC_URE1 had no record of granting access privileges. As a result, RFC_URE1 had not included these individuals in its annual review of all user accounts and access privileges as required by this Standard. Third, ReliabilityFirst determined RFC_URE1 could not demonstrate compliance with CIP-007-3 R5.2 and its subparts. Because RFC_URE1 had several individuals with access privileges for which RFC_URE1 had no record of granting such privileges, RFC_URE1 could not demonstrate it implemented its policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts pursuant to CIP-007-3 R5.2. Fourth, ReliabilityFirst determined RFC_URE1 did not have procedural controls in place to require the use of passwords that consist of alpha, numeric, and "special" characters, in violation of CIP-007-3 R5.3.2.	CIP-007-2a; CIP-007-3	R5.1; R5.1.3; R5.2; R5.3.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower/ Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, although unable to demonstrate evidence of compliance with CIP-007-3 R5.1, RFC_URE1 limited individual and shared system accounts and authorized access permissions to only those employees with "need to know" status. Further, while RFC_URE1 did not have procedural controls to enforce the password requirements of CIP-007-3 R5.3.2, RFC_URE1 required and used passwords that consisted of alpha, numeric, and "special" characters during the duration of the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE1 was required to comply with CIP-007-3 R5	Mitigation Plan completion	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 plans to complete the following actions: 1) Establish a complete list of individuals with access privileges; 2) Determine which Cyber Assets have the capability of complying with the password requirements of CIP-007-3 R5.3; 3) In the event any Cyber Assets cannot comply with the password requirements, RFC_URE1 will submit a Technical Feasibility Exception (TFE) request for the Cyber Asset at issue; 4) Review and modify, if necessary, existing documentation to include a procedure that utilizes the baseline documentation to assure continued compliance with this requirement; 5) Update all documentation relevant to CIP-007 R5 to assure that it is aligned with the requirement and establishes the expectations to maintain a state of compliance; and 6) Communicate updates to all relevant staff.	10/8/2012	1/21/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001146	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. During the Compliance Audit, ReliabilityFirst determined that while RFC_URE1 performed a cyber vulnerability assessment, RFC_URE1 could not demonstrate that it enabled only ports and services required for the operation of the Cyber Assets in its Electronic Security Perimeter (ESP). Specifically, RFC_URE1 included a list of all active ports and services in its cyber vulnerability assessment, but did not provide evidence to verify that RFC_URE1 enabled only ports and services required for the operation of the Cyber Assets within the ESP, in violation of CIP-007-3 R8.2. Also during the Compliance Audit, ReliabilityFirst determined RFC_URE1 did not demonstrate it performed a review of all default accounts as part of the cyber vulnerability assessment. Further, RFC_URE1 did not include evidence that it reviewed controls for default accounts, passwords, and network management community strings in its cyber vulnerability assessment, in violation of CIP-007-3 R8.3.	CIP-007-2a; CIP-007-3	R8.2; R8.3
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity1 (RFC_URE1)	NCRXXXXX	RFC2011001147	Settlement Agreement	ReliabilityFirst conducted a Compliance Audit of RFC_URE1. During the Compliance Audit, ReliabilityFirst determined that RFC_URE1 did not include procedures to characterize and classify events as reportable Cyber Security Incidents in its Cyber Response Plan, in violation of CIP-008-3, R1.1. Also, while RFC_URE1 did include roles and responsibilities of its Cyber Security Incident response team in its Cyber Response Plan, RFC_URE1 did not include other response actions, in violation of CIP-008-3 R1.2. Specifically, ReliabilityFirst determined RFC_URE1 did not demonstrate how the communication plan it presented during the Compliance Audit was triggered, executed, or related to its Cyber Response Plan.	CIP-008-2; CIP-008-3	R1.1; R1.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, during the duration of the instant violation, and where technically feasible, RFC_URE1 enabled monitoring, logging and alerting, as well as anti-virus protections on all Critical Cyber Assets (CCAs) within the ESP. Second, RFC_URE1 protected all access points into the ESP with an intrusion prevention system. This system included logging, alerting, and constant monitoring of all access points during the duration of the instant violation.
Lower	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, RFC_URE1 has a documented Cyber Response Plan that includes examples of potential incidents and categorization of the severity of such incidents. Second, prior to the discovery of the instant violation, RFC_URE1 performed a tabletop test of its response process, which resulted in the successful characterization of an event and the notification of proper individuals.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE1 was required to comply with CIP-007-3 R8	when RFC_URE1 determined which ports and services are necessary for the operation of Cyber Assets; enabled only those ports and services; performed a review of its default accounts	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 performed a cyber vulnerability assessment that included a review to verify that it enabled only ports and services required for operation of the Cyber Assets within the ESP, as well as a review of controls for default accounts. RFC_URE1 also updated all documentation relevant to the standard to assure that it is aligned with the requirement and establishes the expectations to maintain a state of compliance. After the documentation was updated, RFC_URE1 notified the changes to all staff that are engaged in managing access to the CCAs.	6/12/2012	8/21/2012	Neither Admits nor Denies
when RFC_URE1 was required to comply with this Standard	when RFC_URE1 revised its Cyber Response Plan	$40,000 (for RFC2011001001, RFC2011001070, RFC2011001138, RFC2011001139, RFC2011001140, RFC2011001144, RFC2011001146, and RFC2011001147)	Compliance Audit	In accordance with its Mitigation Plan, RFC_URE1 updated its Cyber Response Plan to include the following: 1) procedures to characterize and classify events as reportable Cyber Security Incidents; and 2) a communication response plan.	6/29/2012	10/12/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as a mitigating factor when determining the penalty amount.
ReliabilityFirst considered certain aspects of RFC_URE1's internal compliance program (ICP) as mitigating when determining the penalty amount.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001125	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst identifying a violation of CIP-007 R6. When RFC_URE2 installed its new log monitoring system, a subset of the devices were not properly configured to send logs to the monitoring system or capture the logs from all devices. RFC_URE2 uses a security monitoring tool for network device to store and monitor the access logs for all electronic access control and monitoring access points and network switches. RFC_URE2 also uses the system to provide alerts for security events RFC_URE2 analyzes to determine if there is a Cyber Security Incident. RFC_URE2 failed to configure two Cyber Assets within an Electronic Security Perimeter (ESP), and one Cyber Asset within another ESP (a backup for the Newark facility) to send their logs to a security monitoring tool for network device. As a result, RFC_URE2 failed to ensure that these Cyber Assets issued automated or manual alerts for detected Cyber Security Incidents (R6.2), and failed to maintain (R6.3), retain (R6.4), and review (R6.5) these logs. RFC_URE2 also failed to configure 17 switches within 16 of its ESPs to send logging information to a security monitoring tool for network device. These switches were sending their information to a server which maintained the logs and retained them for ninety calendar days. As a result, RFC_URE2 failed to ensure that these Cyber Assets issued automated or manual alerts for detected Cyber Security Incidents (R6.2) and failed to review logs of system events related to cybersecurity and to maintain records documenting review of logs (R6.5).	CIP-007-2a	R6; R6.2; R6.3; R6.4; R6.5

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower	Severe	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 risk was mitigated by the following factors. The corporate monitoring system logged and monitored the traffic to and from the ESPs containing Cyber Assets at two ESPs. Since this was the case, while the corporate log server did not monitor or alarm for attempts to log into the Cyber Assets directly, the corporate monitoring system monitored and alarmed for any attempts to access the ESPs and the devices within them. The corporate log server retained the logs for more than ninety days. Regarding the 17 network switches, the server to which the logs were being sent retained the logs for ninety calendar days, although the server did not provide alerting. In addition, RFC_URE2 restricts electronic access to the network switches for the purpose of managing or configuring the switch. Any unauthorized logical access attempt would require an attacker to first pass through the access point to the ESP or have direct physical access to the device. RFC_URE2's configuration management system monitors any configuration changes. This system was functional during the violation, and no unauthorized changes to the configurations occurred. The foregoing decreases the likelihood of successful unauthorized access. Fourteen of the 17 network switches operate as Open System Interconnection Layer 2 switches, which only function to provide pass-through communications, reducing the likelihood that compromising these switches would affect the system beyond the local area network. Furthermore, the protections provided to the Critical Cyber Assets within the ESPs were not compromised during the violation. The access point protections were operational and did not permit unauthorized traffic into the ESP.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE2 installed new devices	when RFC_URE2 configured all missed devices to send security and event logs to the log monitoring system	$0	Self-Report	To mitigate this violation, RFC_URE2 : 1) Reviewed all devices that either formed the ESPs or were contained with the ESPs; 2) Configured the individual devices to create logs and send them to the log monitoring system; 3) Ensured the viability of the communications between the reporting devices and the log monitoring system; 4) Configured the log monitoring system to receive the logs; 5) Configured the configuration management system to report all deviations in the device configurations that would disrupt the delivery of logs to the log management system; and 6) Configured all devices to create periodic test log entries to ensure that the log management system is capturing logs from all devices.	10/28/2011	12/26/2012	Admits

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of the RFC_URE2's internal compliance program (ICP) as mitigating factors. ReliabilityFirst considered that the violation concerns RFC_URE2's logging procedures. ReliabilityFirst also considered that it discovered the violation through a Self-Report and applied mitigating credit. Effective oversight of the reliability of the BPS depends on robust and timely self-reporting by registered entities. RFC_URE2 promptly identified and reported the violation due to the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. As a result, ReliabilityFirst seeks to encourage this type of self-reporting, characterized by spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action, and imposed a zero dollar penalty for the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012001321	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst identifying a violation of CIP-006-3c R2. RFC_URE2 utilizes net controllers to control access to the information technology (IT) data center and electric system operations center racks located in the IT data center. Net controllers are proprietary physical devices that are part of the badge access system to control access to doors. When an individual presents a badge at the badge reader, a local database in the net controller is checked to verify whether it should grant access. The badge reader communicates with the net controller through a serial connection, and if the identity of the person presenting the badge matches with an approved person in the local net controller database, it then grants access. The net controller also communicates with a remote server using an IP protocol for updates to its local database. In its Mitigation Plan for a previous violation of CIP-006-1 R5, regarding a malfunctioning badge access system, RFC_URE2 committed to designating and protecting the net controllers as Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP). RFC_URE2 connected the badge access system for the electric system operations center racks located in the IT data center to a net controller that was not protected as a Cyber Asset. Once RFC_URE2 connected the badge access system to this net controller, this net controller became a Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter. RFC_URE2, however, had not afforded the requisite protections to this net controller. Specifically, RFC_URE2 failed to afford the protections of CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3c R5 and CIP-007-3 R6 and R8.	CIP-006-3c	R2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk was mitigated by the following factors. RFC_URE2 provided the protections of CIP-003-3, CIP-007-3 R2, R3, R4, R5, and R7, CIP-008-3, and CIP-009-3 for the net controller. The net controller is physically located inside the IT data center which is staffed 24-hours a day. RFC_URE2 restricts entry to the IT data center through a biometric man trap and badge access control system. The electric system operations center racks are located in the IT data center and are monitored by video. RFC_URE2 monitors and logs access to the Critical Cyber Assets located within the racks. In addition, the racks are protected using magnetic locks and a badge access system. Furthermore, a firewall continuously electronically protects the net controller and segregates the net controller from the general network. Only a limited number of IT associates with background checking have logical access to the firewall.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE2 installed the net controllers	when RFC_URE2 installed and commissioned a new net controller	$0	Self-Report	To mitigate this violation, RFC_URE2: 1) Installed a new net controller as part of the RFC_URE2 NERC CIP physical security access system to control access to the electric system operations center racks in the IT data center; and 2) Conducted a review of all other net controllers protecting CIP environments to determine if they were protected by the appropriate measures. The review determined that all installed net controllers had the appropriate protections.	5/11/2012	12/27/2012	Admits

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of the RFC_URE2's internal compliance program (ICP) as mitigating factors. ReliabilityFirst considered that the violation concerns RFC_URE2's logging procedures. ReliabilityFirst also considered that it discovered the violation through a Self-Report and applied mitigating credit. Effective oversight of the reliability of the BPS depends on robust and timely self-reporting by registered entities. RFC_URE2 promptly identified and reported the violation due to the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. As a result, ReliabilityFirst seeks to encourage this type of self-reporting, characterized by spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action, and imposed a zero dollar penalty for the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010101	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst identifying a violation of CIP-005-3a R5. RFC_URE2 utilizes two security monitoring tools for network devices to simultaneously log the events from its Cyber Assets within the Electronic Security Perimeter (ESP), Cyber Assets used in access control and/or monitoring of the ESPs, and access points to the ESP. RFC_URE2 configured numerous additional devices to send their events to the security monitoring tool for network devices. The quantity of logs was greater than what RFC_URE2 expected due to the amount of devices installed, and, as a result, some of the logs were overwritten to make space for the new log messages. RFC_URE2 discovered that only 81 days of logs were available on 12 access points to the ESPs, 14 Cyber Assets within the ESP, and 2 Cyber Assets used in access control and/or monitoring of the ESPs.	CIP-005-3a	R5

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower	Lower	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk was mitigated by the following factors: 1) Nine days of logs were missing for two months; 2) The security logs were alerting properly; 3) RFC_URE2 monitored the security logs daily during the time period of the violation; and 4) RFC_URE2 moved quickly to mitigate the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE2 did not retain logs for 90 calendar days	when RFC_URE2 retained 90 calendar days of logs	$0	Self-Report	To mitigate this violation, RFC_URE2: 1) Configured the log monitoring system to archive logs to external storage on a daily basis; 2) Manually extracted all available online logs to the external storage location; and 3) Ensured that the revised configuration was accumulating 90 days of logs.	3/29/2012	12/28/2012	Admits

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of the RFC_URE2's internal compliance program (ICP) as mitigating factors. ReliabilityFirst considered that the violation concerns RFC_URE2's logging procedures. ReliabilityFirst also considered that it discovered the violation through a Self-Report and applied mitigating credit. Effective oversight of the reliability of the BPS depends on robust and timely self-reporting by registered entities. RFC_URE2 promptly identified and reported the violation due to the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. As a result, ReliabilityFirst seeks to encourage this type of self-reporting, characterized by spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action, and imposed a zero dollar penalty for the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010419	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst identifying a violation of CIP-007-3 R6. In the Self-Report, RFC_URE2 also identified a violation of CIP-005-3a R3. Subsequently, RFC_URE2 self-certified that it was non-compliant with CIP-005-3a R3. When RFC_URE2 installed its new log monitoring system, a subset of the devices was not properly configured to send logs to the monitoring system or to capture the logs from all devices. RFC_URE2 uses a security monitoring tool for network device to store and monitor the access logs for Electronic Access and Monitoring (EACM) access points and network switches within the Electronic Security Perimeter (ESP). RFC_URE2 failed to configure one access point for the switching station ESP to send logging information to the security monitoring tool for network device. The Cyber Asset was sending its information to a server as well as to two inactive devices instead of sending it to the security monitoring tool for network device. The server maintained the logs and retained them for 90 calendar days. As a result, RFC_URE2 failed to ensure that this access point detected and alerted for attempts at or actual unauthorized access at least every 90 calendar days. RFC_URE2 also failed to review logs where alerting personnel was not feasible.	CIP-005-2a	R3

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk was mitigated by the following factors. The server to which the logs were being sent retained the logs for 90 calendar days, although the server did not provide alerting. In addition, there are ten Critical Cyber Assets at the switching station, including eight remote terminal units (RTUs). One of the Critical Cyber Assets, a separate front-end device that connects the RTU devices to the network, creates and retains logs for attempts to gain access to the RTUs or attempts for unauthorized access. The eight RTUs are the only devices behind the front-end device, and as a result, the RTUs are situated on a private subnet behind the front-end device. The communication ports for the RTUs are not directly accessible from any other network, including the network used to communicate with the energy management system. Furthermore, the protections provided to the Critical Cyber Assets within the ESPs were not compromised during the violation. The access point protections were operational and did not permit unauthorized traffic into the ESP. The 10 devices are located within a Physical Security Perimeter for which RFC_URE2 utilizes electronic badging to permit or deny entry.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE2 installed the new device	when RFC_URE2 configured all missed devices to send security and event logs to the log monitoring system	$0	Self-Report	To mitigate this violation, RFC_URE2: 1) Reviewed all devices that either formed the ESPs or were contained within the ESPs; 2) Configured the individual devices to create logs and send them to the log monitoring system; 3) Ensured the viability of the communications between the reporting devices and the log monitoring system; 4) Configured the log monitoring system to receive the logs; 5) Configured the configuration management system to report all deviations in the device configurations that would disrupt the delivery of logs to the log management system; and 6) Configured all devices to create periodic test log entries to ensure that the log management system is capturing logs from all devices.	10/28/2011	12/26/2012	Admits

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst considered certain aspects of the RFC_URE2's internal compliance program (ICP) as mitigating factors. ReliabilityFirst considered that the violation concerns RFC_URE2's logging procedures. ReliabilityFirst also considered that it discovered the violation through a Self-Report and applied mitigating credit. Effective oversight of the reliability of the BPS depends on robust and timely self-reporting by registered entities. RFC_URE2 promptly identified and reported the violation due to the effective execution of its ICP and the installation of internal controls that yielded identification of the issues prior to the occurrence of any harm. As a result, ReliabilityFirst seeks to encourage this type of self-reporting, characterized by spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action, and imposed a zero dollar penalty for the violation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100866	Settlement Agreement	RFC_URE3 self-certified non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE3 determined that they had not outfitted their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE3 had not outfitted the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system which RFC_URE3 has been assigned the responsibility to operate and maintain in compliance with NERC CIP Standards. The Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE3 do not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE3 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE3 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE3 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, RFC_URE3 monitored the operational status of the Panels in its systems network operations center.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE3	when RFC_URE3 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE3 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE3 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into RFC_URE3 recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst favorably considered certain aspects of RFC_URE3's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201100867	Settlement Agreement	RFC_URE4 self-certified non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE4 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE4 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system which RFC_URE4 has been assigned the responsibility to operate and maintain in compliance with NERC CIP Standards. The Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE4 does not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE4 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for which it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE4 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE4 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE4	when RFC_URE4 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE4 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE4 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE4's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100868	Settlement Agreement	RFC_URE5 self-certified non-compliance with Reliability Standard CIP-006-3c R2.2 to Reliability*First.* RFC_URE5 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c, R2.2. Specifically, RFC_URE5 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. RFC_URE5 replaced the Panels used in CIP related areas and replaced them with the Panels used by other entities. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system for RFC_URE5. The Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE5 does not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE5 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for which it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE5 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE5 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE5	when RFC_URE5 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE5 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE5 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE5's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC201100869	Settlement Agreement	RFC_URE6 self-certified non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE6 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE6 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. RFC_URE6 replaced the Panels used in CIP related areas and replaced them with the Panels used by other entities. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system for RFC_URE6. The Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE6 does not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE6 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for which it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE6 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE6 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE6	when RFC_URE6 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE6 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE6 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE6's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC201100870	Settlement Agreement	RFC_URE7 self-certified non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE7 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE7 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. RFC_URE7 replaced the Panels in CIP related areas and replaced them with the Panels used by other entities. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective Responsible Entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system for RFC_URE7. Therefore, the Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE7 does not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE7 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for which it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE7 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE7 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE7	when RFC_URE7 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE7 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE7 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE7's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 8 (RFC_URE8)	NCRXXXXX	RFC201100871	Settlement Agreement	RFC_URE8 self-certified non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE8 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE8 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. RFC_URE8 replaced the Panels used in CIP related areas and replaced them with the Panels used by other entities. The Panels serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system for RFC_URE8. Therefore, the Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE8 do not use the Panels to permanently retain log records of access. The number of Panels varied from an initial low of 22 to a high of 62 over the violation period. RFC_URE8 must be able to demonstrate individual compliance with CIP-006-3c R2.2 based on the respective functions for which it is registered on the NERC Compliance Registry.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE8 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE8 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE8	when RFC_URE8 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE8 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE8 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE8's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC2012009861	Settlement Agreement	RFC_URE9 self-certified or self-reported non-compliance with CIP-006-3c R2.2 to Reliability*First.* RFC_URE9 determined that they had not afforded their remote security system panels (Panels) with the protective measures required by CIP-006-3c R2.2. Specifically, RFC_URE9 had not afforded the Panels the protective measures that authorize and/or log access to physical security perimeters (PSPs), as prescribed in CIP-003-3 R6, CIP-007-3, and CIP-009-3. RFC_URE9 previously used Panels that, although from a different manufacturer than the Panels used by other entities, functionally operated in a similar manner. RFC_URE9 replaced the Panels used in CIP related areas and replaced them with the Panels used by each of the other entities. The Panels, serve as intermediary devices that convert and communicate programmed instructions from centralized servers to the respective entity's physical security access devices as part of the authorization process necessary to gain access to the PSPs. The Panels are part of an overall security system for RFC_URE9. The Panels qualify as Cyber Assets that authorize access to PSPs and should have received the protective measures described in CIP-006-3 R2.2. The Panels have limited storage capability, but RFC_URE9 does not use the Panels to permanently retain log records of access.	CIP-006-3c	R2.2

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	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 risk posed to the BPS was mitigated by the following factors. RFC_URE9 afforded the Panels with the protective measures specified by CIP-003-3 (with the exception of R6), CIP-004-3 R3, CIP-005-3 R2 and R3, CIP-006-3 R4 and R5, and CIP-008-3. Additionally, the Panels were within PSPs during the duration of the violations. Further, RFC_URE9 stored the Panels in locked or key carded cabinets with tamper alarms. Only CIP qualified personnel (those with CIP training and personnel risk assessments (PRAs) or individuals escorted by CIP qualified personnel) had access to the Panels. Finally, the operational status of the Panels in its systems network operations center were monitored.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE9	when RFC_URE9 afforded its Panels with all of the protective measures required by CIP-006-3c R2.2	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Certification	RFC_URE9 submitted a Mitigation Plan to address the violations of CIP-006-3 R2.2. RFC_URE9 completed the following mitigating actions: 1) Established and implemented a change control and configuration management process for the Panels per CIP-003 R6; 2) Completed Panel testing and associated documentation per CIP-007 R1; 3) Completed records and documentation per CIP-007 R2 and submitted the appropriate technical feasibility exception requests for the Panels per CIP-007 R4, R5 and R6; 4) Performed and documented vulnerability assessments on the Panels per CIP-007 R8; 5) Integrated fully the Panels into recovery plans per CIP-009 R1, R2, R3, R4 and R5; and 6) Replaced its existing Panels with a new upgraded model that includes upgraded security features.	12/31/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE9's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC2012001323	Settlement Agreement	RFC_URE7 self-reported possible non-compliance with CIP-007-3 R6 to Reliability*First*. RFC_URE7 discovered that it had not configured the security monitoring controls on one Critical Cyber Asset (CCA) to issue automated or manual alerts for detected Cyber Security Incidents. The CCA at issue was a Microsoft Windows server that RFC_URE7 uses to collect standard Windows event logs, such as application, system, and security, from other Windows servers at RFC_URE7. As a result of RFC_URE7's not properly configuring the CCA, one local interactive Windows account for this device could not automatically alert for detected Cyber Security Incidents. RFC_URE7 also did not have security monitoring controls in place for this CCA to provide manual alerts for detected Cyber Security Incidents. Further, RFC_URE7 did not review logs of system events related to the CCA at issue or maintain records documenting review of such logs until it discovered the possible violation of CIP-007-3 R6. RFC_URE7 reviewed local server and Windows Domain Control logs and found no evidence of system events associated with the CCA at issue during the duration of the violation. Upon discovery of the violation, RFC_URE7 manually reviewed the 90 days of logs available, but could not recover any logs older than 90 days. RFC_URE7 did not identify any Cyber Security Incidents from the manual review of the available logs.	CIP-007-3	R6

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The CCA at issue does not provide control capability for the BPS. Further, the CCA does not contain any data that could compromise or adversely affect the BPS.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when the Standard became mandatory and enforceable to RFC_URE7	when RFC_URE7 configured the affected CCA to issue automated alerts for detected Cyber Security Incidents pursuant to CIP-007-3 R6.2)	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Report	In its Self-Report, RFC_URE7 described the mitigating actions it took to address the violation of CIP-007-3 R6. RFC_URE7 configured the CCA at issue to automatically alert for detected Cyber Security Incidents. Additionally, RFC_URE7 implemented supplemental control processes to ensure that logging and monitoring configurations are completed when a device is put in service. Finally, RFC_URE7 implemented an additional daily control process to verify CIP devices are properly configured for logging and monitoring.	7/29/2011	9/4/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
ReliabilityFirst favorably considered certain aspects of RFC_URE7's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012009852	Settlement Agreement	RFC_URE3 self-reported possible non-compliance with CIP-004-3 R4 to Reliability*First*. RFC_URE3 added an employee (Employee 1), for whom it had not granted access rights, to the list of personnel with authorized unescorted physical access rights to one Physical Security Perimeter (PSP). Additionally, RFC_URE3 did not revoke the unescorted physical access rights of another employee (Employee 2) who no longer required such access within seven calendar days. Specifically, Employee 2 resigned on August 4, 2011, but RFC_URE3 did not revoke Employee 2's access rights until September 14, 2011.	CIP-004-3	R4

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower	Lower	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. Employee 1 completed CIP training and had a current personnel risk assessment prior to RFC_URE3 adding Employee 1 to its access list. Therefore, Employee 1 satisfied all the requirements for unescorted physical access to the PSP except an official grant of access by RFC_URE3. Also, RFC_URE3 collected Employee 2's access badge on the date of Employee 2's resignation. Therefore Employee 2 did not have the ability to physically access any RFC_URE3 PSPs during the duration of the violation. Further, Employee 2 did not have electronic access to any Critical Cyber Assets prior to, or following, Employee 2's resignation.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE3 should have removed Employee 2 from its access list when RFC_URE3 should have removed Employee 1 from the access list	when RFC_URE3 revoked Employee 2's unescorted physical access rights when RFC_URE3 revoked Employee 1's unescorted physical access rights	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Report	RFC_URE3 certified that it completed all necessary mitigating activities associated with the violation of CIP-004-3 R4. Upon discovery of the violation, RFC_URE3 revoked Employee 1 and Employee 2's access rights. Additionally, RFC_URE3 provided the individuals responsible for the violations with refresher training on properly granting access rights as well as feedback on improving performance.	10/18/2011	8/27/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE3's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 8 (RFC_URE8)	NCRXXXXX	RFC2012009907	Settlement Agreement	RFC_URE8 self-reported two occasions of possible non-compliance with CIP-004-3 R4 to Reliability*First* . First, RFC_URE8 added an employee (Employee 1) who had not completed CIP training to the list of personnel with unescorted physical access rights to the Physical Security Perimeters (PSPs) at two generation plants. Security personnel attempted to add a different employee to the list of individuals with unescorted physical access rights, but inadvertently added Employee 1's name to the list due to Employee 1's similar name to that of the intended employee. Specifically, Employee 1 and the intended employee have the same first and last name, but Employee 1 has the suffix "Junior" while the intended employee has the suffix "Senior." The intended employee and Employee 1 are related. Second, on RFC_URE8 added an employee (Employee 2) who had not completed CIP training to the list of personnel with authorized unescorted physical access to three generation plant PSPs.	CIP-004-3	R4

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Lower	Lower	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. Employee 1 and Employee 2 both had current personnel risk assessments prior to RFC_URE8 adding Employee 1 and Employee 2 to the respective access lists. Additionally, during the duration of the violation, neither Employee 1 nor Employee 2 attempted to access the PSPs to which RFC_URE8 granted them access.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE8 added Employee 1 to its access list when RFC_URE8 added Employee 2 to the list of personnel with authorized unescorted physical access to PSPs	when RFC_URE8 removed Employee 1 from its access list when RFC_URE8 removed Employee 2 from its access list to three generation plant PSPs	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Report	In its Self-Report, RFC_URE8 described the mitigating actions it took to address the violation of CIP-004-3 R4. Upon discovery of the violation, RFC_URE8 revoked Employee 1 and Employee 2's access rights. Additionally, RFC_URE8 provided the individuals responsible for the violations with additional training on properly granting access as well as feedback on improving performance.	1/22/2012	8/27/2012	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE8's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012009859	Settlement Agreement	RFC_URE3 self-reported possible non-compliance with the CIP-006-3c R1 to Reliability*First* . RFC_URE3 self-reported possible non-compliance with CIP-006-3c R1 when it discovered it had not properly logged access to physical security perimeters (PSPs) at a single facility. Specifically, RFC_URE3 logged visitor access to a facility which contained several PSPs, but did not log visitor access to the individual PSPs within the facility pursuant to CIP-006-3c R1. The PSPs at issue protected non-dispatcher energy management system (EMS) workstations. The EMS workstations were used for management oversight, IT support, and distribution operations. RFC_URE3 provided evidence of additional occurrences of possible non-compliance with CIP-006-3c R1. Reliability*First* determined the additional information expanded the scope of RFC_URE3's self-reported violation of CIP-006-3c R1 and was nota new possible violation. RFC_URE3 stated that two employees (Employee 1 and Employee 2) inappropriately used physical access controls and were unescorted in the PSP for approximately three minutes in violation of CIP-006-3c R1.4 and R1.6. Specifically, Employee 1 and Employee 2 used a key to enter a PSP for which neither had received authorization from RFC_URE3 and were unescorted in the PSP until security personnel arrived and escorted them out of the PSP.	CIP-006-3c	R1

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. Although RFC_URE3 did not properly log access to each specific PSP in the facility at issue, RFC_URE3 did log access for all visitors into and out of the facility which housed the PSPs . Further, all visitors were continuously escorted by a qualified and approved RFC_URE3 employee while inside the PSPs during the duration of the violation. Also, Employee 1 and Employee 2 completed CIP training and received personnel risk assessments prior to entering the specific PSP at issue. RFC_URE3 granted Employee 1 and Employee 2 access to other PSPs within the same facility prior to the violation. Upon using the key to enter the PSP, an alarm alerted RFC_URE3 security personnel that someone had bypassed the normal entry procedure. RFC_URE3 security personnel located Employee 1 and Employee 2 and escorted them out of the PSP within approximately three minutes.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE3 first did not properly log access to its PSPs at the facility at issue	when RFC_URE3 first did not continuously escort a contractor while inside the PSP	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Report	RFC_URE3 submitted its Mitigation Plan to address its alleged violation of CIP-006-3c, R1 to Reliability*First* . To mitigate the violation of CIP-006-3c R1.4 RFC_URE3 established a more stringent key control policy at facility where the PSP is located that limits access and use of the key. Specifically, the key control policy allows only a supervisor to have possession of a key and the use of the key is restricted to emergency situations and requires notification of the RFC_URE3 control center prior to use of the key. To mitigate the violation of CIP-006-3c R1.6, RFC_URE3 implemented a new electronic logging system that electronically logs the entrance and exit of each visitor to individual PSPs within the facility. The electronic logging is performed by a security officer or a designee authorized by RFC_URE3's corporate physical security. RFC_URE3 continues to investigate the arrangement of individual PSPs within the facility and will determine whether to rearrange and/or consolidate PSPs in order to reduce the administrative burden of logging movements of visitors among separate PSPs within the facility.	11/7/2012	1/30/2013	Neither Admits nor Denies

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE3's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012009860	Settlement Agreement	RFC_URE4 self-reported possible non-compliance with CIP-006-3c R1 to Reliability*First*. Specifically, RFC_URE4 discovered that in one instance, it did not continuously escort a contractor while inside a physical security perimeter (PSP). The PSP at issue contained two Critical Cyber Assets (CCAs), a dial-up device and a network and data communications device. RFC_URE4 also did not properly log the contractor's access to the PSP.	CIP-006-3c	R1
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012010776	Settlement Agreement	WECC_URE1 submitted a Self-Report to WECC stating that it was in violation of CIP-005-3a R1.5. WECC_URE1 discovered that it had failed to assess available patches as described in CIP-007-3 R3 and required by CIP-005-3a R1.5. The following devices, which encompass the scope of the equipment affected in this violation, were located in two of WECC_URE1's control centers: 1) Three servers which are authentication devices used for access, control and monitoring (ACM); 2) Three RSA SecurID two factor authentication (RSA) appliances used for ACM; and 3) Four firewalls access points used for ACM.	CIP-005-3a	R1; R1.5

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. Prior to the violation, RFC_URE4 completed a personnel risk assessment for the contractor which revealed no criminal or identity issues. Also, RFC_URE4 did provide an escort for the contractor who, although not continuously escorting the contractor, remained in the proximity of the contractor and periodically observed the contractor during the duration of the violation.
Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE1 assessed the potential impact to the BPS as minimal because all network devices in scope are protected from unauthorized physical access behind Physical Security Perimeters and unauthorized access attempts would have triggered alarms alerting personnel. Authorized access to these devices is limited to a very small group comprised of five individuals who all completed Personnel Risk Assessments and CIP training. Also, all electronic access was controlled, logged and monitored. In addition, out of 25 requirements, WECC_URE1 only failed to meet one. All other CIP requirements were met for these devices.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when RFC_URE4 did not continuously escort a contractor while inside the Physical Security Perimeter (PSP)	when RFC_URE4 did not continuously escort a contractor while inside the PSP	$0 (for RFC201100866, RFC201100867, RFC201100868, RFC201100869, RFC201100870, RFC201100871, RFC2012001323, RFC2012009852, RFC2012009859, RFC2012009860, RFC2012009861, and RFC2012009907)	Self-Report	RFC_URE4 described the mitigating actions it took to address the violation of CIP-006-3c R1.6. RFC_URE4 conducted refresher training with the individual responsible for the violation. Specifically, RFC_URE4 emphasized its Corporate Policy on visitors which states the escort must keep the visitor within sight at all times except when the visitor is in the lavatory. RFC_URE4 also emphasized the need to document the entry and exit of visitors.	12/20/2011	8/27/2012	Neither Admits nor Denies
when WECC_URE1 should have begun assessing the devices in scope for available patches	Mitigation Plan completion	$10,000	Self-Report	In accordance with its Mitigation Plan, a WECC_URE1 team assessed posted security patches for the network devices that were in production within the Energy Management System environment, as well as the RSA and server devices located in the energy network. Once the assessments were complete, the team began upgrading the control center devices first, with new security patches where applicable. Once that was complete, WECC_URE1's Information Technology security scanned each device to document its security posture. The same process was applied to the other control center devices at issue. WECC_URE1 also conducted training for all applicable personnel to reinforce familiarity with its patch management process.	8/31/2012	10/8/2012	Does Not Contest

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* favorably considered certain aspects of RFC_URE4's compliance program as a mitigating factor in the penalty assessment. ReliabilityFirst considers the fact that entity self-reported six of the violations described in this Agreement as a mitigating factor. ReliabilityFirst also considered that the discovery of all these violations was not prompted by any intervention on the part of ReliabilityFirst. ReliabilityFirst encourages such self-assessment and self-disclosure because these behaviors assist ReliabilityFirst in carrying out its mission to preserve and protect the reliability of the BPS. Taking all the facts and circumstances, as well as aggravating and mitigating factors into consideration, ReliabilityFirst determined a zero dollar penalty was appropriate.
WECC reviewed WECC_URE1's Internal Compliance Program (ICP) and considered it a mitigating factor during the penalty determination.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Standard	Req.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102933	Settlement Agreement	WECC conducted a Compliance Audit of WECC_URE2. WECC determined that WECC_URE2 was in violation of CIP-002-3 R1 because its Critical Asset identification methodology (Methodology) did not include a risk-based assessment component. WECC_URE2 created the Methodology and associated documentation, which included a statement that WECC_URE2 subject matter experts (SMEs) would apply the Methodology to WECC_URE2's list of assets. WECC_URE2 created this Methodology based on threshold values drawn from CIP-002-4 and NERC's Security Guideline for the Electricity Sector on Identifying Critical Assets (dated November 19, 2009). However, WECC determined that WECC_URE2's Methodology did not identify the specific factors that WECC_URE2's SMEs should consider as they applied the criteria set forth in the Methodology. WECC_URE2's previous asset identification methodology demonstrated compliance with CIP-002 R1.	CIP-002-3	R1; R1.1

Seattle City Light

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Violation Risk Factor	Violation Severity Level	Risk Assessment
Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC determined that the violation posed a moderate risk because WECC_URE2's noncompliance could have resulted in misidentified or unidentified Critical Assets and over-reporting, under-reporting, or misreporting of associated Critical Cyber Assets (CCAs). Furthermore, given the cross-cutting nature of networked technology, malicious attack or intentional or unintentional misuse may impact multiple assets at once. Therefore, failure to identify, protect, and secure CCAs and Critical Assets may pose a risk and jeopardize BPS reliability by rendering one or a number of Critical Assets vulnerable to misuse or malicious attack. However, WECC_URE2's corporate security policy provides protections that constitute compensating measures, thereby reducing the risk to the BPS. WECC_URE2's corporate security program includes maintaining security staff, overseeing physical facility protections, and responding to alarms. Additionally, the risk was mitigated by the fact that WECC_URE2 based its Methodology on criteria developed in support of Version 4 of the CIP Reliability Standards (i.e., expertise on the Standards drafting team and vetted and pooled industry comment and knowledge), and approved by both NERC and FERC. Furthermore, although application of WECC_URE2's Methodology ultimately reduced WECC_URE2's list of Critical Assets and list of associated CCAs, WECC_URE2 did not remove existing CIP-003 through CIP-009 protections from the assets that were not identified by application of the Methodology. Finally, WECC_URE2's Methodology explicitly states that WECC_URE2 SMEs are to apply WECC_URE2's criteria to WECC_URE2's asset lists. In practice, WECC_URE2 accomplishes this by reviewing its assets and criteria in meetings with SMEs responsible for and knowledgeable about WECC_URE2's system.

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

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, "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not
when WECC_URE2 modified its Methodology in a manner that did not comply with CIP-002-3 R1.1	Mitigation Plan completion	$15,000	Compliance Audit	To mitigate this violation, WECC_URE2 updated its risk-based assessment methodology to include clearer, more specific documentation requirements for its annual execution and update.	9/4/2012	10/5/2012	Agrees/ Stipulates

Attachment A-2

January 31, 2013 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
WECC reviewed WECC_URE2's internal compliance program (ICP), which was in place at the time of the violation, and determined it to be a mitigating factor in the penalty determination.

Document Accession #: 20130131-5371 Filed Date: 01/31/2013

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 31, 2013

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP13-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A regarding 22 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

The Spreadsheet NOP resolves 50 violations[5] of 13 Reliability Standards. In order to be a candidate for inclusion in the Spreadsheet NOP, the violations are those that had a minimal or moderate impact on the reliability of the bulk power system (BPS). In all cases, the NOP sets forth whether the violations have been mitigated, certified by the respective Registered Entities as mitigated, and verified by the Regional Entity as having been mitigated.

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.
[3] Attachment A is an excel spreadsheet.
[4] *See* 18 C.F.R § 39.7(c)(2).
[5] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. As designated in the attached spreadsheet, some of the Registered Entities have admitted to the violations, while the others have indicated that they neither admit nor deny the violations and have agreed to the proposed penalty as stated in Attachment A or did not dispute the violations and proposed penalty amount stated in Attachment A, in addition to other remedies and mitigation actions to mitigate the instant violations and ensure future compliance with the Reliability Standards. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

As discussed below, this Spreadsheet NOP resolves 50 violations. NERC respectfully requests that the Commission accept this Spreadsheet NOP.

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Text of the Reliability Standards at issue in the Spreadsheet NOP may be found on NERC's web site at http://www.nerc.com/page.php?cid=2|20. For each respective violation, the Reliability Standard Requirement at issue and the applicable Violation Risk Factor are set forth in Attachment A.

Unless otherwise detailed within the Spreadsheet NOP, the Registered Entities were cooperative throughout the compliance enforcement process; there was no evidence of any attempt to conceal a violation or evidence of intent to do so. In accordance with the Guidance Order issued by FERC concerning treatment of repeat violations and violations of corporate affiliates, the violation history for the Registered Entities and affiliated entities who share a common corporate compliance program is detailed in Attachment A when that history includes violations of the same or similar Standard. Additional mitigating, aggravating, or extenuating circumstances beyond those listed above are detailed in Attachment A.

Status of Mitigation[6]

The mitigation activities are described in Attachment A for each respective violation. Information also is provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[7]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order, the August 27, 2010 Guidance Order and the March 15, 2011 Compliance Enforcement Initiative Order,[8] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee. Such considerations include the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, the NERC Enforcement staff's review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the violations at issue.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[6] *See* 18 C.F.R § 39.7(d)(7).
[7] *See* 18 C.F.R § 39.7(d)(4).
[8] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A;

b) Additions to the service list, included as Attachment B; and

c) Violation Risk Factor Revision History Applicable to the Spreadsheet Notice of Penalty, included as Attachment C.

A Form of Notice Suitable for Publication[9]

A copy of a notice suitable for publication is included in Attachment D.

[9] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
rebecca.michael@nerc.net

cc: Entities listed in Attachment B

Document Accession #: 20130131-5371 Filed Date: 01/31/2013

Document Content(s)