NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NP10-138
Duke Energy Co.

July 6, 2010

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

Re: NERC Non-Public Notices of Penalty, FERC Docket No. NP10-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1], which includes one (1) Non-Public Exhibit pertaining to a NERC Registered Entity. The Notice of Penalty set forth in the Non-Public Exhibit contains, in whole or in part, violations of the CIP-002 through CIP-009 Reliability Standards that were resolved by Settlement Agreement. The Registered Entity admits to the violation and agrees to the penalty. This filing is submitted 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)).[2]

The Non-Public Exhibit identifies the Reliability Standards at issue, the basis for the violation and the impact to reliability, and the ultimate disposition. A summary is set forth below:

[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 (2008). *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).

[2] *See* 18 C.F.R § 39.7(c)(2).

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

NERC Violation ID*	Reliability Std.	Req. (R)	Approved VRF[3]	Basis for Violation	Total Penalty ($)
RFC200900134	CIP-004-1	4.2	Medium	The Registered Entity did not revoke physical access rights to Critical Cyber Assets within seven days for personnel who no longer required access. The Registered Entity discovered seven instances where records could not be located to demonstrate badge deactivations occurred in a timely manner for personnel who no longer required access to Critical Cyber Assets. Subsequently, the Registered Entity submitted a letter in which it identified two additional instances in which revocation was similarly delayed and occurred in the same time frame as the original seven. Therefore, the Registered Entity self-reported a total of nine instances where access badges were not deactivated in a timely manner, following termination of those employees. Specifically, the Registered Entity historically relied on the submittal of an electronic form to the badge office as the primary means of requesting revocation of badge access. It also permitted requests via telephone or e-mail, instead of the electronic form, to the badge office. In the incidents discovered during the audit, the responsible supervisors for the affected personnel failed to notify the badge office via any of the above mentioned methods that the badge access should be revoked. Additionally, at the time of the occurrences, the Registered Entity utilized an automated program designed to run once every 24 hours, extracting termination information from the Human Resources (HR) data mart and passing that data to its badge system. This process resulted in the automatic revocation of physical access privileges for terminated employees. This method served as a back-up to the process of submitting an electronic form, e-mail or	5,000

[3] Violation Risk Factors (VRF) are the current FERC approved assignments for the Reliability Standards.

				telephone call to the badge office requesting physical access revocation.[4] Also according to the Mitigation Plan, the investigation performed by the Registered Entity revealed two time periods, April 2, 2008 through August 15, 2008 and November 20, 2008 through January 9, 2009, when the HR to badge system interface was not synchronizing. As a result, there were no automatic physical access revocations or electronic access revocation forms submitted for the nine cases identified during these two time periods. Specifically, the earliest date it failed to terminate physical access to Critical Cyber Assets was identified as May 26, 2008, and instead of access being removed within seven days, access was removed on July 8, 2008. The last date it failed to terminate physical access to Critical Cyber Assets was identified as December 29, 2008, and instead of access being removed within seven days, access was removed on January 8, 2009. According to a subsequent letter, there were additional instances, not mentioned in the Mitigation Plan, in which it failed to revoke physical access in a timely manner. The Registered Entity failed to terminate access to Critical Cyber Assets on November 30, 2008, and instead of access being removed within seven days, access was removed on January 14, 2008.[5] Electronic access rights were not at issue in this instance as the employees in question never had electronic access to Critical Cyber Assets. The Registered Entity mitigated this violation by implementing an independent process for the reconciliation of terminations or transfers of employees with access to Critical Cyber Assets	

[4] This system covered the revocation of access for employees, contractors, terminations and transfers.

[5] In the Mitigation Plan submitted and completed by the Registered Entity, efforts to retrain and reinforce the need for timely access removal was performed. The Registered Entity also implemented additional procedures to correct the syncing problems between HR and the badging system. Both of the additional incidents reported in the October 19, 2009 letter occurred during the same timeframe of the initially self-reported items. The Registered Entity reported that the mitigating activities that have been completed also addressed the cause of these newly discovered incidents. No additional instances have been identified since the completion of the Mitigation Plan.

				against changes to the maintained lists of employees with physical and electronic access to Critical Cyber Assets. Also it committed to removing all inappropriate employee access and to correct its HR practices so that its badge access lists are synchronized with HR records twice daily. The Registered Entity: 1. provided additional training for managers regarding proper procedures for removing access to relevant cyber assets; 2. changed internal process to notify an administrator and other personnel of changes processed by HR regarding personnel with access to critical cyber assets; 3. removed access for terminated or transferred employees as determined by internal investigation or audit action; 4. implemented a program change to migrate employee termination processing from a legacy mainframe application to its workforce hub; 5. changed the synchronization of HR and badging system records from once daily to twice daily; 6. reiterated to managers the need for timely access revocation; 7. created automatic triggering of follow-up actions for identified anomalies; 8. reduced the number of personnel authorized to access the restricted area; and 9. enhanced the presentations and materials used by managers in the hiring, termination and transfer processes.	

				Additionally, it took the following additional actions: 1. monitoring of the HR and badging system synchronization process to ensure proper and timely operation; and 2. daily termination reports are generated for use by access control personnels.	

*Due to the confidential nature of the CIP-002 through CIP-009 violations, the Registered Entity's name is not identified.

Request for Confidential Treatment

Information in and certain attachments to the instant Notice of Penalty include privileged and confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed "confidential" by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721 (609)452-8060 (609) 452-9550 – facsimile gerry.cauley@nerc.net david.cook@nerc.net Timothy R. Gallagher* President and Chief Executive Officer Reliability*First* Corporation 320 Springside Drive, Suite 320 Akron, Ohio 44333 (330) 456-2488 tim.gallagher@rfirst.org Raymond J. Palmieri* Vice President and Director of Compliance Reliability*First* Corporation 320 Springside Drive, Suite 320 Akron, Ohio 44333 (330) 456-2488 ray.palmieri@rfirst.org *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* Assistant General Counsel Holly A. Hawkins* Attorney V. Davis Smith* Attorney (admitted in IN; not admitted in D.C. or NJ) North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net holly.hawkins@nerc.net davis.smith@nerc.net Robert K. Wargo* Manager of Compliance Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 320 Akron, Ohio 44333 (330) 456-2488 bob.wargo@rfirst.org Michael D. Austin* Compliance Enforcement Specialist Reliability*First* Corporation 320 Springside Drive, Suite 320 Akron, Ohio 44333 (330) 456-2488 mike.austin@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this 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
David N. Cook
Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
gerry.cauley@nerc.net
david.cook@nerc.net

Rebecca J. Michael
Assistant General Counsel
Holly A. Hawkins
Attorney
V. Davis Smith
Attorney (admitted in IN;
not admitted in D.C. or NJ)
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
holly.hawkins@nerc.net
davis.smith@nerc.net