

July 6, 2010

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

**Re: NERC Notice of Penalty,  
FERC Docket No. NP10- \_000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty,<sup>1</sup> 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 a Settlement Agreement. The Registered Entity admitted to the violations and agreed 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)).<sup>2</sup>

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:

NERC Violation ID*	Reliability Std.	Req. (R)	Approved VRF	Basis for Violation	Total Penalty (\$)
SERC200800211	CIP-004-1	4	Lower	The Registered Entity failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access rights to Critical Cyber Assets and failed to remove access within seven days for personnel who no longer required such access. Specifically, the Registered Entity failed to identify one person who had physical	5,000

<sup>1</sup> *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 (2010). *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).

<sup>2</sup> See 18 C.F.R. § 39.7(c)(2).

**PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

				<p>access to its physical security perimeter, but did not have a current personnel risk assessment. In the spring and summer of 2008, the Registered Entity was working to update its software to implement controls necessary to comply with physical security requirements. To implement this change, the Registered Entity continued to run its existing access control system in production, while the upgraded access control system, was being run in a test environment. While both versions were running in parallel, changes to the access lists needed to be made in both systems. The violation occurred when access authorization was removed for the subject individual in the production system, but was not removed in the test system.</p> <p>When the upgraded version V4.0 was placed into production on May 27, 2008, the individual regained authorization to access the physical security perimeter. This error was not immediately identified because a flawed report failed to identify an access point into the physical security perimeter, and this individual had authorization to access the physical security perimeter through that point.<sup>3</sup> Once security fixed the flawed report, on September 24, 2008, the report then listed the one individual who did not have a personnel risk assessment.</p> <p>On September 26, 2008, control center personnel responsible for authorizing access to the physical security perimeter reviewed the corrected report, identified the issue and immediately removed the individual's access authorization. The Registered Entity's records show that at no time did the individual attempt or gain access to the physical security perimeter during the period when the standard became applicable until September 26, 2008, when the access was again revoked.</p> <p>On November 13, 2008, the Registered Entity submitted two additional self-reports highlighting two additional potential violations, discovered as a result of the corporate-wide review of its access control systems.</p> <p>The Registered Entity's internal investigation and Mitigation Plan implementation following the initial self-report uncovered an additional</p>	
--	--	--	--	--	--

<sup>3</sup> Had the access point been included in the report or had the individual had access through other physical security parameter points, the error would likely have been identified prior to the system being put into production, and the authorization removed at that time.

**PRIVILEGED AND CONFIDENTIAL INFORMATION  
HAS BEEN REMOVED FROM THIS PUBLIC VERSION**

				<p>individual who had physical access to Critical Cyber Assets, but did not have the required training or personnel risk assessment. It explained that this additional individual had not shown up in the original reports because the individual had not been granted access through the physical security perimeter, but did have authorization to access interior areas of the physical security perimeter. Upon discovery, the Registered Entity terminated the access authorization, and its records showed that this additional individual did not have unescorted access to the physical security perimeter at any time after the standard became mandatory and enforceable.</p> <p>In addition, a security guard at its affiliate determined that security staff had unescorted access to the primary and back-up control centers. As a result of the experience of its affiliate, the Registered Entity reviewed its own controls and discovered that certain members of its security staff unintentionally had unescorted access to its back-up control center. Based on this, the Registered Entity took additional actions to secure its back-up control center by limiting access and inserting additional controls around emergency access.</p> <p>The Registered Entity took the following actions to mitigate these issues: (1) immediately terminated access and completed the personnel risk assessment; (2) immediately replaced the existing key core for the access point where the violation occurred; (3) validated all success lists; (4) reviewed the Critical Cyber Asset physical access report design; (5) revised procedures to reflect control measures to ensure key hierarchy is replaced; (6) upgraded access control software and database structure; and (7) created a new position and hired a person with enterprise-wide responsibility for managing the access control system.</p>	
--	--	--	--	---	--

\*Due to the confidential nature of the CIP-002 through CIP-009 violations, the Registered Entity 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:

<p>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</p> <p>Marisa A. Sifontes* Compliance Legal Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org</p> <p>*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.</p>	<p>Rebecca J. Michael* Assistant General Counsel Holly 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</p> <p>Kenneth B. Keels, Jr.* Manager of Compliance Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive Charlotte, NC 28217 (704) 940-8214 (704) 357-7914 – facsimile kkeels@serc1.org</p>
---	--

**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 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