MEMORANDUM OF UNDERSTANDING
BETWEEN
THE U.S. NUCLEAR REGULATORY COMMISSION
AND
THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

I. Purpose:

1. This Memorandum of Understanding (MOU) is entered into by the U.S. Nuclear Regulatory Commission (NRC) and the North American Electric Reliability Corporation (NERC) (hereafter "Party" or "Parties").

2. Consistent with their statutory authority and regulations, the NRC and NERC each have responsibility for establishing and enforcing cyber security requirements at commercial nuclear power plants operating in the United States of America (USA). The NRC's primary focus is on the prevention of radiological sabotage (*i.e.*, significant core damage) that could result in harm to public health and safety or the environment or have an adverse impact upon the common defense and security of the USA. NERC's primary focus is on the reliability of the bulk power system (BPS). It accomplishes this in part by enforcing compliance with applicable NERC Reliability Standards, including, but not limited to, the Critical Infrastructure Protection (CIP) Reliability Standards.

3. The purpose of this MOU is to set forth and coordinate the roles and responsibilities of each organization as they relate to the application of their respective cyber security requirements for the protection of digital assets at commercial nuclear power plants operating in the USA. This cooperation will ensure that the common responsibilities of each organization are achieved in the most efficient and effective manner without diminishing or interfering with their respective responsibilities and authorities. The goal of this cooperation is to maintain the safety and security of commercial nuclear power plants operating in the USA while optimizing the reliability of the BPS to the maximum extent possible.

4. This memorandum supplements an existing Memorandum of Agreement (MOA) between the NRC and NERC dated July 10, 2007.

II. Roles and Responsibilities:

1. NRC:

   a. The NRC has statutory responsibility for licensing and regulating commercial nuclear facilities operating in the USA as well as the civilian use of byproduct, source, and special nuclear materials in order to protect public health and safety, promote the common defense and security, and protect the environment. Pub. L 93-438, 88 Stat. 1233 (42 U.S.C. 5801 *et seq.*).

b. The NRC carries out its statutory responsibilities by promulgating regulations and issuing licenses, certificates and orders for commercial nuclear power plants and other nuclear facilities and materials in the USA.

c. The NRC has issued orders and promulgated regulations imposing cyber security requirements on commercial nuclear power plants under its jurisdiction. Portions of these facilities also fall under the concurrent jurisdiction of NERC's CIP reliability standards.

d. The NRC's cyber security regulations set forth at 10 C.F.R. § 73.54 govern digital systems and networks that can affect commercial nuclear power reactor safety, security, and emergency preparedness functions. Those regulations do not govern systems within nuclear facilities, such as those related to continuity of power, that could not have an adverse impact on safety, security, or emergency preparedness functions.

2. NERC:

a. NERC has statutory responsibility for improving the reliability and security of the BPS in the United States. NERC conducts equivalent activities in Canada. NERC's authority and jurisdiction in the USA is set forth in the Federal Power Act pursuant to Title XII of the Energy Policy Act of 2005, FERC's implementing regulations at 18 C.F.R. Part 39, and applicable FERC Orders, including but not limited to, the Electric Reliability Organization (ERO) Certification Order, Order Nos. 672, 693, 706 and 706-B. NERC is a not-for-profit, self-regulatory corporation.

b. NERC develops and enforces reliability standards; monitors the BPS; analyzes BPS events; assesses the adequacy of the BPS annually via a 10-year forecast and winter and summer forecasts; audits owners, operators, and users of the BPS; and educates and trains industry personnel.

III. NRC/NERC Consultations on the FERC Order 706-B Exception Process:

1. On January 18, 2008, FERC issued Order No. 706 imposing eight NERC-developed cyber security CIP reliability standards on BPS owners, operators, and users. This Order exempted facilities regulated by the NRC from compliance with NERC's CIP standards.

2. On March 19, 2009, FERC issued Order No. 706-B, significantly narrowing the nuclear facilities exemptions from NERC's CIP standards in order to ensure comprehensive cyber security protection of appropriate digital assets at nuclear power plants. Order No. 706-B allows nuclear facilities to seek exceptions from NERC's CIP standards on a case-by-case basis for those digital assets subject to the NRC's cyber security requirements.

3. The NRC and NERC agree to cooperate regarding NERC's disposition of exception requests received from nuclear facilities subject to NERC's CIP standards. NERC agrees to consult with the NRC on each request for an exception from NERC's CIP

standards that NERC receives from a nuclear facility also regulated by the NRC. This cooperation and consultation will facilitate the proper characterization of digital assets as subject to either the NRC's cyber security requirements or NERC's CIP standards.

IV. Cyber Security Inspection Protocol:

1. The NRC has regulatory responsibility for inspecting those digital assets, including digital control and data acquisition systems and networks, which can affect safety, security, and emergency preparedness functions of a nuclear power plant. The NRC will inspect such systems to ensure compliance with the NRC's cyber security requirements.

2. The NRC does not have regulatory responsibility to inspect those digital assets unrelated to the safety, security or emergency preparedness functions of a nuclear power plant, such as those digital control and data acquisition systems related to continuity of power, unless those systems can have an adverse impact on safety, security, or emergency preparedness functions.

3. NERC has regulatory responsibility for inspecting digital assets related to continuity of power for compliance with NERC's CIP standards.

4. The NRC and NERC agree to share any information discovered during the course of their respective inspections that they believe may be relevant to or have an adverse impact on any digital asset governed by the other Party's cyber security requirements.

5. The NRC and NERC agree to consult and coordinate to the maximum extent practicable on the process for conducting inspections to carry out activities contemplated under this MOU.

V. Information Sharing:

1. The NRC and NERC recognize that the sharing of relevant information between the Parties may be necessary to implement the provisions of this MOU. Consistent with applicable laws and regulations, the NRC and NERC support the sharing of all information necessary to carry out the intent of this MOU. Accordingly, all relevant information will be shared with the other Party in a timely manner so that each Party can take appropriate action.

2. The NRC and NERC recognize that this MOU may require the sharing of sensitive information up to and including Safeguards Information (SGI) as defined in 10 C.F.R. § 73.2. The NRC and NERC agree to protect sensitive information received from the other party in accordance with all applicable laws and requirements, including all requirements governing access to and protection of SGI. NERC further agrees that it will not transmit any SGI received from the NRC to any third party, except for its Regional Entities pursuant to V.4 below, without the written consent of the NRC.

3. NERC agrees to adhere to procedures governing the sharing, possession and handling of SGI under this MOU in accordance with the Appendix to this MOU, entitled, "Procedures Governing Access to and Possession of Safeguards Information." NERC

further agrees to develop, implement, and maintain an SGI program in accordance with applicable requirements and the Appendix to this MOU.

4. NRC and NERC recognize that NERC has delegated, by contract, certain authority to eight Regional Entities to assist NERC in carrying out NERC's compliance and enforcement program and that it may be necessary for NERC to share certain sensitive information with those Regional Entities in the process of carrying out the compliance and enforcement program. With respect to access to and protection of SGI, those eight Regional Entities will be considered to be contractors of NERC. NERC agrees that it will adhere to the procedures governing the sharing, possession and handling of SGI in accordance with the Appendix to this MOU entitled, "Procedures Governing Access to and Possession of Safeguards Information" for any SGI to which Regional Entities are given access.

VI. Enforcement Actions:

1. Nothing in this MOU is intended to limit the authority of the NRC or NERC to take enforcement action consistent with their statutory authority and regulations.

2. The NRC and NERC agree that the NRC will have sole responsibility for taking enforcement action because of a violation involving a digital asset subject to the NRC's cyber security requirements. The NRC shall inform NERC of any enforcement actions that it plans to take as a result of a violation of NRC cyber security requirements.

3. The NRC and NERC agree that NERC will have sole responsibility for taking enforcement action because of a violation involving a digital asset subject to NERC's CIP standards. NERC shall inform the NRC of any enforcement actions that it plans to take as a result of a violation of NERC's CIP standards.

4. In those situations where a cyber security incident at a nuclear power plant results in violations of both the NRC's and NERC's requirements, the NRC and NERC agree to consult and coordinate on any enforcement actions to be taken.

5. If NERC considers imposing remedial action directives or sanctions on a nuclear power plant, NERC agrees to consult in advance with the NRC to ensure that the proposed action will not adversely affect nuclear safety, security or emergency preparedness.

6. The NRC and NERC agree to coordinate on any public announcements of enforcement actions taken as a result of any violation of their respective cyber security requirements.

VII. Points of Contact:

The following are designated points of contact for carrying out the routine administration of matters arising under this MOU:

1. The resolution of policy issues concerning organizational jurisdiction and operational relations will be coordinated by the NRC's Executive Director for Operations and NERC's Chief Executive Officer. Appropriate points of contact will be established.

2. The NRC's Office of Enforcement (OE) and NERC's Compliance Department shall coordinate the resolution of issues involving enforcement actions taken by one or both parties at an NRC-licensed nuclear power plant. Appropriate OE and Compliance Program points of contact will be established.

VIII. Administrative Matters:

1. This MOU shall become effective upon signing by all of the Parties and shall remain in effect for five years from the date of signing unless terminated in accordance with the procedures set forth below.

2. This MOU may be modified or amended by written mutual agreement of the Parties.

3. Any Party may terminate this MOU by providing written notice of its intent to terminate the MOU to the other Party at least 180 days in advance of the effective date of termination.

4. This MOU shall not be construed to be or create a private right of action for or by any person or entity.

5. This MOU does not commit or obligate appropriated funds. All activities undertaken to implement any responsibilities carried out pursuant to this MOU shall be subject to the availability of appropriated funds.

6. If any provision(s) of this MOU, or the application of any provision(s) to any person or entity, is held to be invalid, the remainder of this MOU and the application of any remaining provision(s) to any person or entity shall not be affected.

FOR THE NUCLEAR REGULATORY COMMISSION

12/30/09

R. W. Borchardt
Executive Director for Operations

FOR THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

12/30/09

Rick Sergel
Chief Executive Officer and President

Appendix

Procedures Governing Access to and Possession of Safeguards Information

It is possible that both the NRC and NERC may require access to Safeguards Information (SGI) to carry out their respective responsibilities under this Memorandum of Understanding (MOU). The NRC has promulgated detailed regulations in 10 C.F.R. Part 73 governing access to and the handling of SGI. The definition of SGI is set forth at 10 C.F.R. § 73.2. This Appendix sets forth general principles and procedures governing access to and the handling of SGI for purposes of carrying out this MOU. To the extent that any of the principles and procedures set forth in this Appendix conflict with the requirements set forth in 10 C.F.R. Part 73, the NRC and NERC agree that the regulatory requirements set forth in Part 73 shall take precedence over this MOU.

SGI is a special category of sensitive unclassified information protected from unauthorized disclosure under Section 147 of the Atomic Energy Act of 1954 (AEA), as amended. Although SGI is sensitive unclassified information, it is handled and protected more like Classified National Security Information than like other sensitive unclassified information. Information designated as SGI must be withheld from public disclosure and must be physically controlled and protected to prevent any unauthorized disclosure. The requirements set forth in 10 C.F.R. Part 73 applies to any person, whether or not a licensee of the NRC, who produces, receives or acquires SGI.

All persons who have or have had access to SGI have a continuing obligation to protect SGI in order to prevent its inadvertent release and/or unauthorized disclosure. Violations of SGI handling and protection requirements, including the unauthorized disclosure of SGI, may result in the imposition of applicable civil and criminal penalties.

Information to be Protected as Safeguards Information:

Any documents provided to NERC by NRC that contain SGI will be designated in accordance with 10 C.F.R. § 73.22. Documents developed by NERC that contain SGI must also be designated and protected as SGI in accordance with 10 C.F.R. § 73.22. The NRC and NERC agree to comply with the requirements for protecting all information designated as SGI as set forth in 10 C.F.R. § 73.22(a).

Access to Safeguards Information:

Generally, no person may have access to SGI unless the person has an established "need to know" for the information and has been determined to be "trustworthy and reliable." Typically, a determination of trustworthiness and reliability is based upon a background check, including at a minimum, a Federal Bureau of Investigation (FBI) criminal history records check (including verification of identity based on fingerprinting), employment history, education and personal references. The terms "background check," "need to know" and "trustworthy and reliable" are defined in 10 C.F.R. § 73.2. The NRC and NERC agree to comply with the requirements for access to SGI set forth in 10 C.F.R. § 73.22(b) and 10 C.F.R. § 73.57.

Reviewing Official:

The determination that a NERC employee, consultant or contractor has a need for access to SGI (established "need to know" and is "trustworthy and reliable") must initially be made by an individual already authorized access to SGI. Accordingly, the NRC and NERC agree to implement the following procedures for granting NERC employees, consultants and contractors access to SGI for the purpose of carrying out this MOU.

NERC shall submit the name and fingerprints of at least one individual to the NRC who NERC has determined to be trustworthy and reliable and has a need to know SGI. NERC's trustworthiness and reliability determination shall be based, at a minimum, on all elements of a background check except for each individual's criminal history record. The NRC will conduct a criminal history record check based on each individual's fingerprints. Based upon the outcome of the criminal history record check, the NRC shall determine if the individual (or individuals if more than one name is submitted and approved) may have access to SGI and can serve as a reviewing official under this MOU. Upon approval by the NRC, this individual (or individuals if more than one name is submitted and approved) may serve as a reviewing official authorized to make SGI access authorization determinations for other NERC employees, consultants and contractors.

Individuals possessing an active Federal security clearance require no additional fingerprinting or background check for access to SGI, as this clearance meets the fingerprinting requirement and other elements of the background check, as prescribed in 10 C.F.R. § 73.22(b)(1). Such individuals must still meet the need to know requirement for access to SGI. However, when relying upon an existing active Federal security clearance to meet the SGI access requirements (except for the need to know determination), NERC should obtain and maintain a record of official notification stating that the individual possesses such a clearance.

Only NRC-approved reviewing officials shall be authorized to make SGI access determinations for other individuals who have been identified by NERC as having a need to know SGI. The reviewing official shall be responsible for determining that these individuals have a "need to know" for access to SGI to carry out their official duties under this MOU and for determining that these individuals are trustworthy and reliable. The reviewing official's determination of trustworthiness and reliability shall be based upon an adequate background check, including, at a minimum, an FBI criminal history records checks and fingerprinting. The reviewing official can only make SGI access determinations for other individuals, but cannot approve other individuals to act as reviewing officials.

NERC agrees that the reviewing official shall maintain secure and adequate records of each SGI access authorization determination. Such records shall be available to the NRC for inspection upon request.

Protection of Safeguards Information While in Use or Storage:

SGI must be adequately protected while in use or storage to prevent its unauthorized release or disclosure. The NRC and NERC agree to comply with the requirements for protection of SGI while in use or storage set forth in 10 C.F.R. § 73.22(c).

Preparation and Marking of Documents or Other Matter:

Documents and other matter must be prepared and conspicuously marked as SGI to ensure against unauthorized release or disclosure. The NRC and NERC agree to comply with the requirements for preparation and marking of documents and other material as set forth in 10 C.F.R. § 73.22(d).

Reproduction of Matter Containing Safeguards Information:

SGI may be reproduced to the minimum extent necessary consistent with need without permission of the originator. The NRC and NERC agree to comply with the requirements for reproduction of documents and other material containing SGI as set forth in 10 C.F.R. § 73.22(e).

External Transmission of Documents and Material:

Documents or other matter containing SGI when transmitted outside an authorized place of use or storage shall be enclosed in two sealed envelopes or wrappers and must not bear any markings or indication that the document contains SGI. The NRC and NERC agree to comply with the requirements for the external transmission of documents and other material containing SGI as set forth in 10 C.F.R. § 73.22(f).

Processing of Safeguards Information on Electronic Systems:

SGI may not be transmitted by unprotected telecommunications circuits except under emergency or extraordinary conditions. SGI must be processed or produced on an electronic system that ensures the integrity of the information and prevents the unauthorized release or disclosure of SGI. The NRC and NERC agree to comply with the requirements for the processing of SGI on electronic systems as set forth in 10 C.F.R. § 73.22(g).

Removal from Safeguards Information Category:

Documents containing SGI shall be removed from the SGI category (decontrolled) only after the NRC determines that the information no longer meets the criteria for designation as SGI. Organizations have the authority to make determinations that specific documents which they created no longer contain SGI and may be decontrolled. The NRC and NERC agree to comply with the requirements for removing information from the SGI category as set forth in 10 C.F.R. § 73.22(h).

Destruction of Matter Containing Safeguards Information:

Documents containing SGI should be destroyed when no longer needed. The NRC and NERC agree to comply with the requirements for the destruction of documents and other material containing SGI as set forth in 10 C.F.R. § 73.22(i).