Print Form

# NERC Cyber Security Standards & Requirements

National Grid ("Company") is required to comply with the North American Electric Reliability Corporation ("NERC") Reliability Standards, specifically Cyber Security Standards CIP-002 through CIP009 in order to provide a security framework for the protection of critical cyber assets that support the reliable operation of the bulk electric system.

The services covered by this Request for Proposal have been identified as services requiring the Contractor's compliance with these NERC Standards. Accordingly, you will be required to:

1. Review the attached document entitled "National Grid Contractor Requirements for Compliance with NERC Cyber Security Standards CIP-002 through CIP-009."

2. Complete the document entitled "NERC Cyber Security Standards" and include it with your Proposal – Attachment – NERC A.

If awarded a contract, as a result of this RFP, you will be required to perform the required background checks and training, for all employees who will be performing this work or have access to protected documents. The following documents (included in the RFP) will need to be completed, signed and returned to the responsible Manager, for the work, prior to the commencement of these services:

1. Contractor Background Check Validation Statement: Attachment - NERC B

2. Training Completion Record: Attachment – NERC C

# National Grid Contractor Requirements for Compliance with NERC Cyber Security Standards CIP-002 through CIP-009

**1. Definition of "Contractor" and "Contractor Employees"**

The entity or entities engaged or to be engaged under this contract to perform services for National Grid are referred to throughout this document as "Contractor." The individuals who will perform work for National Grid ("Company") under a contract, including employees, principals, sole proprietors, or contingent staff provided by the Contractor, are referred to as "Contractor Employees**."**

**1.1 (b) "NERC CIP Protected Information"** – All material marked as such by Company, or which should reasonably be understood to be NERC CIP Protected Information by Service Firm, including, without limitation, the items defined by NERC CIP 003, latest revision which includes, any drawings, configurations, Critical Assets (CA's), Critical Cyber Assets (CCA's) and/or other information identified in the bulleted list below, as NERC CIP Protected Information which is furnished or disclosed by the Company or its affiliates (or its or its affiliates' agents, servants, representatives, or employees) to Contractor, whether provided orally, in writing, or by electronic means, and any memoranda, notes, reports, files, copies, extracts, inventions, discoveries, improvements or any other thing prepared or derived there from. Without limiting the foregoing, all NERC CIP Protected Information shall be Confidential Information.

- Operational procedures related to CCA's
- Lists of CA's and CCA's identified in CIP002
- Network topology or similar diagrams
- Floor plans of computing centers containing CCA's
- Equipment layouts of CCA's
- Disaster Recovery plans for CCA's created as part of CIP009
- Incident response plans for CCA's created as part of CIP008
- Security configuration information that if exposed could put CCA's at risk

**2. NERC Cyber Security Standards CIP-002 through CIP-009**

National Grid must comply with the North American Electric Reliability Corporation (NERC) Cyber Security Standards CIP-002 – CIP-009. To comply with these standards, Company must require Contractor and Contractor Employees who require authorized cyber access and/or unescorted physical access to identified CCA's or who require access to protected information falling under the NERC requirements to meet the mandated criteria contained in the CIP Standards. The requirements are as follows:

- Cyber Security Training – Company must maintain and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCA's. Company must maintain documentation that training is conducted annually, including the date the training was completed and attendance records.

- Personnel Risk Assessment (PRA) Program – Company must have a documented personnel risk assessment program in accordance with federal, state, provincial, and local laws and subject to existing collective bargaining agreements for personnel having authorized cyber or authorized unescorted physical access to CCA. The PRA must include, at a minimum, identification verification and legal eligibility to work in the United States (verified via a Social Security Number trace) and seven-year criminal history check. The PRA must be updated at least every seven years after the initial PRA or for cause. Company must document that the PRA of Contractor Employees with such access is conducted pursuant to Standard CIP-004.

- Company must maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCA, including their specific electronic and physical access rights to CCA. Company must validate the lists of personnel who have such access quarterly. The list(s) must be updated within seven calendar days of any change of personnel with such access to CCA, or any change in the access rights of such personnel. Company must ensure that access list(s) for Contractors and service vendors are properly maintained.

- Company must revoke authorized cyber access and authorized unescorted physical access to CCA within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to CCA.

**3. Contractor Responsibilities**

National Grid contract administrators will identify those Contractors subject to the NERC requirements. Such Contractors shall ensure compliance with the NERC requirements as contained in the above section by providing appropriate documentation and notifications as follows:

- Cyber Security Training – Company will provide the required training either through an e-learning computer-based training module or by providing a DVD training program. All Contractor Employees identified as requiring authorized cyber access and/or authorized unescorted physical access must successfully complete the training program prior to being approved for access. The contractor must provide a Contractor NERC Cyber Security Training Validation Statement (Attachment A) to the Company contract administrator listing the names of the Contractor Employees who have completed the initial training and the date the training was completed. The Contractor shall ensure training is updated annually for those Contractor Employees requiring continued access through training programs and validation statement forms provided by Company.

- Personnel Risk Assessment – Contractor shall ensure that PRA consisting of identification verification, legal eligibility to work in the United States (validated via a Social Security number trace) and seven-year criminal history check is completed on all Contractor Employees identified as requiring authorized cyber access and/or authorized unescorted physical access to CCA. Contractor must provide a Contractor Background Check Validation Statement (Attachment B) to the Company contract administrator listing the names of the Contractor

Employees who have satisfactorily met the criteria and qualifications as required by Company, the date the check was completed and identification information from a Government Issued ID (e.g. Valid State Drivers License, Passport, etc.). The PRA must be updated at least every seven years after the initial PRA or for cause (as identified by the Contractor or Company).

- Revocation of Access – Contractor shall immediately notify Company Security and the appropriate Company contract administrator whenever any previously identified Contractor Employee either (1) no longer requires authorized cyber access and/or authorized unescorted physical access to Company CCA or (2) is terminated for cause. Contractor shall ensure that this notification is timely in both events. In the case of Contractor Employees who no longer require access, Contractor shall ensure that notification is given no later than the seven calendar day requirement for revocation of access. In the case of Contractor Employees terminated for cause, Contractor shall **immediately** notify Company Security and the appropriate Company contract administrator and Contractor shall ensure that this notification in no event extends beyond the 24 hour requirement for revocation of access following a termination for cause. Contractor is required to make these notifications by calling the Company Security Control Center (SCC) at 516-545-5000 and the Enterprise Support Center at 1-877-373-1112. The SCC and the Enterprise Support Center are manned 24/7/365.

**4. Conflicts**

To the extent the Contractor finds that any of the NERC Cyber Security Standard requirements are in conflict with Federal, State or local statutes, or its collective bargaining agreements, or identifies other issues that would prohibit compliance, the Contractor should notify the Company contract administrator for guidance and resolution.

**5. Retention and Access to Contractor Records**

Contractor must maintain a record of the NERC Cyber Security Training and Personnel Risk Assessments performed during the term of the contract and shall make all records and correspondence available to National Grid or its agent upon reasonable notice. National Grid may perform audits of Contractor's training and PRA records and all supporting documents and records as they relate to Contractor Employees performing work for National Grid. National Grid's direct costs and the cost for any contracted audit services will be at the expense of National Grid.

**Attachment – NERC A**
**NERC Cyber Security Standards**

National Grid is required to comply with the North American Electric Reliability Corporation ("NERC") Cyber Security Standards CIP-002 – CIP-009 and has established a new policy entitled, "National Grid Contractor Requirements for Compliance with NERC Cyber Security Standards CIP-002 – CIP-009," latest revision ("Cyber Security – Contractor Requirements");

National Grid Contractors are required to comply with the Cyber Security – Contractor Requirements;

Contractor agrees to comply the Cyber Security – Contractor Requirements; and National Grid and Contractor hereby agree to incorporate into resulting purchase orders (The "Purchase Order") and any associated agreements between Contractor and the National Grid affiliate(s) Identified in the Purchase Order as "Owner" or "Company" (The National Grid Entity") as follows:

1. "National Grid Contractor Requirements for Compliance with NERC Cyber Security Standards CIP-002 – CIP-009," latest revision, is incorporated in the Purchase Order and made a part thereof. .

2. The following provision is incorporated in the Purchase Order and made a part thereof:

   "Contractor shall, and shall require its Subcontractors to, comply with National Grid's Contractor Requirements for Compliance with NERC Cyber Security Standards CIP-002 through CIP-009 as set forth in The Purchase Order or Agreement and as may be amended from time to time. In the event of non-compliance on the part of Contractor with any or all of these requirements, the National Grid Entity may cancel its Purchase Order or Agreement for its convenience pursuant to the termination provisions contained herein, except that in no event shall the National Grid Entity or any of its affiliates be liable for any termination cost/charges to Contractor beyond compensation for goods or services provided up to the date of such cancellation."

**ACCEPTED & AGREED TO:**

| | |
|---|---|
| _____ | _____ |
| **Signature** | **Name** |
| _____ | _____ |
| **Title** | **Date** |
| _____ | |
| **Company Name** | |

nationalgrid

**Attachment - NERC B**
**CONTRACTOR BACKGROUND CHECK VALIDATION STATEMENT**

Personal Risk Assessments (PRA) consisting of identification verification, legal eligibility to work in the U.S., and a criminal history check are required pursuant to NERC Cyber Security Standard CIP-004. These checks have been conducted on the following listed contractor employees:

| **Name** (Please Print) | **Date PRA Completed** | **Government Issued ID** (See Below Instruction*) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

The stated checks have been completed pursuant to National Grid guidelines contained in Background Check Requirements for Contracted Service Providers (NGSP6), and all employees listed above have satisfactorily met the criteria and qualifications as required by National Grid.

Company Name: _____

Company Management Representative (Print)_____

Title:_____

Signature:_____ Date:_____

***** Include in this section unique identifying information from a Government issued ID including type and number. Some examples are: last four digits of SS#, Driver's license # (include State), passport #, work visa #, etc.

nationalgrid

**Attachment - NERC C**
**National Grid – Learning and Development Training Record**

All employees who have completed the NERC CIP – Cyber Security Training must print their name below, so that completed training can be entered into the appropriate training records.

| **Name** (Please Print) | **Date Training Completed** | **Government Issued ID** (See Below Instruction*) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Company Name: _____

Company Management Representative (Print)_____

Title:_____

Signature:_____ Date:_____

- Include in this section unique identifying information from a Government issued ID including type and number. Some examples are: last four digits of SS#, Driver's license # (include State), passport #, work visa #, etc.