Unofficial Nomination Form
Project 2020-03 Supply Chain Low Impact Revisions

**Do not** use this form for submitting nominations. Use the [electronic form](https://nerc.checkboxonline.com/6FE1FEA4-9103-4DDC-9A12-A1C6C09E86E0) to submit nominations for **Project 2020-03** **Supply Chain Low Impact Revisions** drafting team members by **8 p.m. Eastern, Wednesday, May 6, 2020.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Additional information about this project is available on the [project page](https://www.nerc.com/pa/Stand/Pages/Project_2020-03_Supply_Chain_Low_Impact_Revisions.aspx). If you have questions, contact Senior Standards Developer, Alison Oswald (via email), or at 404-446-9668.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in face-to-face meetings and conference calls.

Previous drafting or review team experience is beneficial, but not required. A brief description of the desired qualifications, expected commitment, and other pertinent information is included below.

Supply Chain Low Impact Revisions
In adopting the Supply Chain Standards in August 2017, the NERC Board concurrently adopted additional resolutions related to implementation and risk evaluation. These resolutions included preparation of a study of cyber security supply chain risks. FERC approved the Supply Chain Standards with directives for additional modifications to address electronic access or control monitoring systems (EACMS) in Order No. 850, issued October 18, 2018. In its final report accepted by the NERC Board in May 2019, NERC documented the results of the evaluation of supply chain risks associated with certain categories of assets not currently subject to the Supply Chain Standards and recommended actions to address those risks.[[1]](#footnote-1) NERC staff recommended further study to determine whether new information supports modifying the standards to include low impact BES Cyber Systems with external connectivity by issuing a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure.

The Board approved the formal issuance of this data request on August 15, 2019. NERC collected the data from August 19 through October 3, 2019. A final report, *Supply Chain Risk Assessment*, was published in December 2019. The report recommended the modification of the Supply Chain Standards to include low impact BES Cyber Systems with remote electronic access connectivity. Further, industry feedback was received regarding this recommendation at the February 2020 NERC Board meeting through [MRC Policy Input](https://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Policy-Input-Package-February-2020-PUBLIC-POSTING.pdf).

After considering policy input, the NERC Board adopted a resolution to initiate a project to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary.

**Standards affected: CIP-003-8**

The time commitment for these projects is expected to be up to two face-to-face meetings per quarter (on average two and a half full working days each meeting) with conference calls scheduled as needed to meet the agreed-upon timeline the review or drafting team sets forth. Team members may also have side projects, either individually or by subgroup, to present to the larger team for discussion and review. Lastly, an important component of the review and drafting team effort is outreach. Members of the team will be expected to conduct industry outreach during the development process to support a successful project outcome. NERC is seeking individuals who have significiant subject matter expertise with the Critical Infrastructure Protection (“CIP) family of Reliability Standards and Cyber Asset and BES Cyber Asset definitions. Expertise with of remote access or network design is needed.

|  |  |
| --- | --- |
| Name:  |  |
| Organization: |  |
| Address: |  |
| Telephone: |  |
| E-mail: |  |
| Please briefly describe your experience and qualifications to serve on the requested Standard Drafting Team (Bio): |
| **If you are currently a member of any NERC drafting team, please list each team here:**[ ]  Not currently on any active SAR or standard drafting team. [ ]  Currently a member of the following SAR or standard drafting team(s): |
| **If you previously worked on any NERC drafting team please identify the team(s):** [ ]  No prior NERC SAR or standard drafting team.[ ]  Prior experience on the following team(s): |
| **Acknowledgement that the nominee has read and understands both the *NERC Participant Conduct Policy* and the *Standard Drafting Team Scope* documents, available on NERC Standards Resources.**[ ]  Yes, the nominee has read and understands these documents. |
| Select each NERC Region in which you have experience relevant to the Project for which you are volunteering: |
| [ ]  MRO[ ]  NPCC[ ]  RF | [ ]  SERC[ ]  Texas RE [ ]  WECC | [ ]  NA – Not Applicable |

|  |
| --- |
| **Select each Industry Segment that you represent:** |
| [ ]  | 1 — Transmission Owners |
| [ ]  | 2 — RTOs, ISOs |
| [ ]  | 3 — Load-serving Entities |
| [ ]  | 4 — Transmission-dependent Utilities |
| [ ]  | 5 — Electric Generators |
| [ ]  | 6 — Electricity Brokers, Aggregators, and Marketers |
| [ ]  | 7 — Large Electricity End Users |
| [ ]  | 8 — Small Electricity End Users |
| [ ]  | 9 — Federal, State, and Provincial Regulatory or other Government Entities |
| [ ]  | 10 — Regional Reliability Organizations and Regional Entities |
| [ ]  | NA – Not Applicable |

|  |
| --- |
| Select each Function**[[2]](#footnote-2)** in which you have current or prior expertise:  |
| [ ]  Balancing Authority[ ]  Compliance Enforcement Authority[ ]  Distribution Provider[ ]  Generator Operator[ ]  Generator Owner[ ]  Interchange Authority[ ]  Load-serving Entity [ ]  Market Operator[ ]  Planning Coordinator | [ ]  Transmission Operator [ ]  Transmission Owner[ ]  Transmission Planner[ ]  Transmission Service Provider [ ]  Purchasing-selling Entity[ ]  Reliability Coordinator [ ]  Reliability Assurer[ ]  Resource Planner |

|  |
| --- |
| Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group: |
| Name: |  | Telephone: |  |
| Organization: |  | E-mail: |  |
| Name: |  | Telephone: |  |
| Organization: |  | E-mail: |  |

|  |
| --- |
| Provide the name and contact information of your immediate supervisor or a member of your management who can confirm your organization’s willingness to support your active participation. |
| Name: |  | Telephone: |  |
| Title: |  | Email: |  |

1. *See* NERC, *Cyber Security Supply Chain Risks: Staff Report and Recommended Actions* (May 17, 2019). This report, and the other materials referenced in this item, are available on NERC’s Supply Chain Risk Mitigation Program page at https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx. [↑](#footnote-ref-1)
2. These functions are defined in the NERC [Functional Model](http://www.nerc.com/pa/Stand/Functional%20Model%20Advisory%20Group%20DL/FMAG_Inf_Functional%20Model%20v6%20%28clean%29.pdf), which is available on the NERC web site. [↑](#footnote-ref-2)