**ERCOT Nodal Protocols**

**Section 23**

**Form O: Notice of Cybersecurity Incident**

**March 13, 2020**

**NOTICE OF CYBERSECURITY INCIDENT**

A Market Participant shall use this form to notify ERCOT of a Cybersecurity Incident. Market Participant shall fill out this form with as much information as is available upon the time of reporting. Market Participant shall also use this form to provide ERCOT with updated/supplemental information concerning the Cybersecurity Incident as information becomes available.

This Notice of Cybersecurity Incident form shall be submitted to NCSI@ercot.com by the Market Participant’s Authorized Representative, Cybersecurity Contact, or an officer of the company. If, as a result of the Cybersecurity Incident, a Market Participant is unable to securely send the Notice of Cybersecurity Incident form to ERCOT, the Market Participant will call the ERCOT HelpDesk at (512) 248-6800 and/or its Client Service Representative to request a secure means for sending the Notice of Cybersecurity Incident to ERCOT.

|  |
| --- |
| **Market Participant** |
| Market Participant Account Name(s): |       |
| DUNS Number(s): |       |
| Market Participant Type(s): | [ ]  CP [ ]  CRRAH [ ]  IMRE [ ]  LSE [ ]  QSE/Sub-QSE[ ]  RE [ ]  TSP and/or DSP |
| Impacted Market Participant Agent Name(s), *if applicable*: |       |
| Impacted Market Participant Agent Contact Information, *if applicable*: |       |

|  |
| --- |
| **Submitter** |
| Authorized Representative (AR), Backup AR, Cybersecurity Contact, or Officer: |       |
| Signature: |  |
| Email: |       |
| Phone Number: |       |

|  |
| --- |
| **Temporary Cybersecurity Contact Information for this Cybersecurity Incident**(if different from Cybersecurity Contact information contained in ERCOT’s registration files) |
| Name: |       |
| Primary Phone: |       |
| Email Address: |       |
| Other: |       |

|  |
| --- |
| **Cybersecurity Incident**  |

|  |
| --- |
| **Details** |
| Date and Time the Cybersecurity Incident was determined: |       |
| Has the Cybersecurity Incident been resolved? |       |
| Physical location of affected network(s), system(s) &/or application(s): |       |
| Have governmental authorities been notified of the Cybersecurity Incident? If so, please identify the notified entities. |       |

|  |
| --- |
| **Description**  |
| Provide a description of the Cybersecurity Incident:       |
| Provide a description of the type of information/data that may have been compromised:       |

|  |
| --- |
| **Impact/Potential Impacts** |
| **To Notifying Market Participant:**Check all that apply:[ ]  Loss/Compromise of Data [ ]  Damage to Systems/Networks/Applications[ ]  System/Network/Application Downtime[ ]  Other Impacted Systems[ ]  UnknownProvide a description of impacts/potential impacts:       |
| **To ERCOT:**Check all that apply:[ ]  Loss/Compromise of Data[ ]  Damage to Systems/Networks/Applications[ ]  System/Network/Application Downtime[ ]  Other Impacted Systems[ ]  UnknownProvide a description of impacts/potential impacts:       |

|  |
| --- |
| **To Other Market Participants:**Check all that apply:[ ]  Loss/Compromise of Data[ ]  Damage to Systems/Networks/Applications[ ]  System/Network/Application Downtime[ ]  Other Impacted Systems[ ]  UnknownProvide a description of impacts/potential impacts:       |

|  |
| --- |
| **Incident Response**  |
| Please provide a description of steps that have been taken to remediate the Cybersecurity Incident (e.g., no action taken; system disconnected from network; log files examined; etc.):       |
| Please provide an ongoing log of activities taken during the Cybersecurity Incident response process: |
| Date | Activity |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |

|  |
| --- |
| **Additional/Supplemental Information** |
|       |