**DISCUSSION DRAFT of Cybersecurity Information Reporting Guidelines**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Standard Practice | Cyber Event | Rate Recovery |
| Content | In a regular report, the utility should provide high-level, non-confidential information on:   * updates to cybersecurity policies or organizational structure; * cybersecurity budgets; * the date of the most recent internal and external vulnerability assessment and resulting actions; * the date of the most recent penetration test and resulting actions; * the date of the next planned vulnerability assessment and penetration test; * collaboration efforts with other utilities, industry groups or government bodies; * mandatory and voluntary compliance status regarding federal and state standards; and * a compilation of all cyber incident reports (see next column) since the last report and resulting actions. | If a cybersecurity event leads to:   * a loss of service; * breach of sensitive customer information; * serious financial harm; * involvement of the FBI/DHS/Military Dept.; or * reporting of the incident to a law enforcement or another regulatory body;   the utility should notify the Commission:   * that an event has occurred; * whether outside organizations (FBI/DHS/Military Dept., etc.) are involved; * what other organizations the utility has notified of the breach; * a non-confidential and non-sensitive description of the nature of the event and its impact; and * the date the incident was resolved, if applicable. | If a utility requests recovery of specific costs associated with cybersecurity efforts, consistent with Commission practice it should provide in testimony:   * its most recent cybersecurity report to the Commission; * information regarding the nature of the costs to be recovered; * description and contemporaneous documentation of the company’s internal evaluation of the investments (similar to information provided for resource acquisition and RFP analysis); * description of how capital and O&M costs related to cybersecurity are accounted for; and * other information as requested by Commission staff.   Should any of that information be confidential or sensitive, a protective order may be utilized. |
| Timeframe | Could be annual, semiannual, biennial, etc. | Similar to Outage or Incident reports (immediately or within 30-60 days). | As requested in rate cases. |
| Format | Similar to, or as a part of the utility’s annual Reliability Report. | Similar to Outage or Incident Report. | Rate case testimony, site visits. |
| Process options | Revision to reliability rules for electric companies (WAC 480-100-398), requirements agreed to in settlement stipulations, orders, new rules. | Revision to reliability rules, stipulations, orders, new rules. | For discussion. |