WIRAB Comments on PingThings
Request for Data from Peak Reliability

November 10, 2015

The Western Interconnection Regional Advisory Body (“WIRAB”) appreciates the opportunity to comment on PingThings request for data from Peak Reliability.

WIRAB recommends that the Peak Board of Directors:

1. Approve the PingThings request for Phasor Measurement Unit (PMU) data that has been archived and masked by Peak Reliability;

2. Direct the Peak Staff to make an independent recommendation (either to approve or not approve) to the Peak Board on all future third party data requests; and

3. Direct the Peak Staff to provide a detailed accounting of the estimated $10,000 cost of fulfilling the PingThings request.

WIRAB has evaluated the PingThings request using the Peak Data Sharing Review Process that has been proposed by WIRAB staff, Western Resource Advocates, Natural Resources Defense Council, and Western Grid Group (“The Joint Commenters”) as a permanent review process for third party data requests. This proposed review process is attached to these comments.

Under this proposed review process, whether to release the requested data is based on three factors: (1) the sensitivity level of the data; (2) the validity of the request; and (3) the viability of the Data Requestor.

Sensitivity Level of the Data

PingThings is requesting Phasor Measurement Unit (PMU) data that has been archived and masked by Peak. The data is to be delivered in unaltered form without any averaging or data reduction techniques being applied. PingThings understands the sensitive nature of the data and will accept data that does not allow the identification of any specific location, vendor or other identifying information that might be considered sensitive information.

The Joint Commenters have proposed the following data categories under its Alternative Data Sharing Review Process:

- **Restricted Data:** Restricted Data are data that: (1) are not available from public sources; (2) could be directly used to impact the operation of the Bulk Electric System (BES); and (3) if inadvertently released, pose a significant threat to the reliability of the BES.
• **Sensitive Data**: Sensitive Data are data that: (1) are not available from public sources; (2) are Confidential Data as defined in the NERC Rules of Procedure; or (3) are Transmission Function Information as defined by the FERC Standards of Conduct.

• **Non-Sensitive Data**: Non-sensitive Data are data that: (1) are available from public sources; (2) are not Restricted Data; and (3) are not Sensitive Data.

Using these criteria, the data requested by PingThings is appropriately categorized as Non-Sensitive Data which is consistent with Peak Staff’s determination. In its initial review of the PingThings request, the Peak Staff made a similar finding. The Peak Staff categorized the requested data as Non-Sensitive Data “because it is masked to the extent that no individual entity’s data is identifiable.”

**Under the Alternative Data Sharing Review Process, if the request is for Non-Sensitive Data, then Peak’s initial recommendation should be to approve the data request. The validity of the request and the viability of the requestor are not factors relevant to the release of Non-Sensitive Data.**

We believe this data cannot be categorized as restricted data. The masked data cannot be directly used to impact the operation of the BES and an inadvertent release of the data does not pose a significant threat to the reliability of the BES.

Further, we believe that this data cannot be categorized as Sensitive Data. The data is sufficiently masked so that it cannot be considered Confidential Data as defined in the NERC Rules of Procedure or as Transmission Function Information as defined by the FERC Standards of Conduct.

**Validity of the Request**

PingThings data request has the potential to lead to the production of a cost-effective solution for Geomagnetic Disturbance (GMD) monitoring. GMD monitoring has been proposed by FERC to be added to the TPL-007-01 standard via the recent Notice of Proposed Rulemaking in Docket # RM15-11-000. PingThings will use the provided data for identification of signatures from known geomagnetic storm activity. The signatures constitute the continued enhancement of PingThings’ PredictiveGrid™ Geomagnetically Induced Current (GIC) system. The PredictiveGrid™ GIC system has already identified known signatures and manifestations of GMD and PingThings seeks to extend the system’s abilities.

The Joint Commenters have proposed that a request for data be considered valid if: (1) the objective of the data request is to conduct research or develop tools or technologies that have the potential to enhance the reliability of the Western Interconnection; and (2) the requested data and the proposed research methodology are reasonably aligned to achieve the proposed objective.

It is clear that the objective of the PingThings request is to conduct research and develop tools that have the potential to enhance the reliability of the Western Interconnection. Further, the request for data is consistent with its stated objectives. In its initial review of the PingThings
request, Peak Staff made a similar finding. The Peak Staff concluded that PingThings analytic techniques are “promising for the identification of patterns and signatures in Synchrophasor data” and that these types of analytics “could prove to be valuable.” Based on the evidence, PingThings’ request is valid.

Again, under the proposed Alternative Data Sharing Review Process, once data is considered non-sensitive that alone is sufficient grounds for an initial recommendation to approve a data request. An entity objecting to the release of Non-Sensitive Data carries the burden of demonstrating that the request is for invalid purposes.

**Viability of the Requestor**

PingThings has agreed to the terms of the Data License Agreement. Peak and PingThings have negotiated a limited indemnity clause, wherein PingThings will indemnify for acts that are negligent or fraudulent. Peak and PingThings have also negotiated a limited liability clause, wherein PingThings will maintain liability only for acts that are negligent or fraudulent.

Under Joint Commenters proposed review process, there is a rebuttable presumption that the Data Requestor is viable if one of the following conditions are met:

- The Data Requestor is a Department of Energy (DOE) Laboratory;
- The Data Requestor is a research institution that has previously undertaken research for the National Security Agency, Department of Defense, or DOE related to national security, with its security clearances still in force;
- The Data Requestor has received appropriate clearance from FERC, with its security clearance still in force;
- The Data Requestor has met or has the ability to meet the then current NERC Cyber Security Requirements and has processes in place to comply with the then current FERC Rules of Procedure;
- The Data Requestor has at least $2 million in liability insurance from an insurance provider reasonably acceptable to Peak, thereby, demonstrating that the Data Requestor has been vetted by the insurance provider and is considered viable by the provider.

Based on these criteria, we believe that PingThings is a Viable Requestor. It has completed the Cyber Security Checklist and has the necessary insurance coverage in place. In the Data Licensing Agreement, PingThings has agreed to have at least $2,000,000 in liability insurance to cover any breach of confidential information, data breach, or other loss or unauthorized acquisition of data. Additionally, PingThings agrees to have general liability insurance coverage of at least $1,000,000.
For all of the reasons stated above WIRAB recommends that the Peak Board approve the PingThings request for archived and masked Phasor Measurement Unit (PMU) data.

**Peak’s Recommendation**

We note that the Peak Staff has not made a recommendation to the Peak Board on the PingThings request. The Peak Staff has identified the benefits, safeguards, risks, and cost, and posted the request for comments.

Peak Staff is best situated to make an unbiased review of a third party data request. It should have an active and independent role in confirming the data categorization and evaluating the validity of a third party request and the viability of the requestor. After conducting its review, staff should make a recommendation.

WIRAB recommends that Peak Board direct the Peak Staff to make an independent recommendation to the Board on future third party data requests.

**Estimated Cost of Fulfilling the Request**

It is PingThings obligation to cover the costs Peak incurs for fulfilling the data request, but to ensure that all data requestors are treated equally when it comes to the cost of fulfilling a data request, Peak should provide a detailed accounting of its best estimate of the actual cost of meeting a request.

WIRAB recommends that the Peak Board direct the Peak Staff to provide a more detailed accounting of $10,000 estimated cost of fulfilling the PingThings request.

The Alternative Exhibit A – Peak Data Sharing Review Process, proposed by WIRAB staff, Western Resource Advocates, Natural Resources Defense Council, and Western Grid Group is attached to these comments.
I. Overview of Data Request Review Process

- **Initial Review:** Once a Data Requestor submits a completed Application Package, Peak Reliability conducts an initial review process in which it (1) confirms the level of data sensitivity being requested, (2) determines the validity of the request, (3) evaluates the viability of the requestor, and (4) issues and posts for comment an initial recommendation to approve or disapprove the data request.

- **Notice and Comment Process:** Following the issuance of Peak’s initial recommendation, parties have 30 days to provide comments to Peak. During the 30-day period, a Data Sharing Review Group (DSRG) will be convened to serve in the event that it is needed. If no comments opposing Peak’s initial recommendation are received, the DSRG is disbanded, and Peak’s initial recommendation becomes its final determination.

- **Data Sharing Review Group:** If comments opposing Peak’s initial recommendation are received, the DSRG will become active. It will review the written comments, consult with the commenters to receive clarification or to obtain their reaction to the comments of other parties; advise Peak on whether comments are reasoned and supported by facts, and advise Peak on its final determination on the data request. The DSRG will submit its advice to Peak on its final determination no later than 30 days following the end of the comment period.

- **Peak Final Determination:** Within 30 days of receiving the DSRG advice, Peak will issue its final determination regarding the approval or disapproval of a data request.

- **Appeal Process:** Following the issuance of Peak’s final determination, a party receiving an adverse decision has 30 days to submit an appeal. If an appeal is received, the Data Request Appeal Panel (DRAP) will be convened and given 45 days to render a decision. The Appeal Panel’s decision is final.

II. Initial Application

Peak will dedicate a section of its website to the provision of data-request-related information. Information will include: (1) a data categorization document identifying the data collected by Peak and its level of sensitivity; (2) a listing of information that must be provided to receive Restricted and/or Sensitive data; (3) criteria for evaluating whether a data request is viable; (4) criteria for evaluating whether a requesting entity is viable; and (5) the required application fee.

Data Requestors will submit a completed application and data request package to Peak including the specified initial application fee. The request will include information required to establish the sensitivity of the data (e.g. the type, periodicity, and timeframe of the data desired); information
required to establish the Data Request as valid (e.g., establishing the potential benefit to the interconnection from granting the request); and information required to establish the Data Requestor as viable.

III. Initial Review

Peak’s initial recommendation regarding the release of the requested data will be based on three factors: (1) the sensitivity level of the data; (2) the validity of the request; and (3) the viability of the Data Requestor.

Data Sensitivity Level

Peak must first determine the sensitivity level of the requested data. Data is categorized as follows:

- **Restricted Data**: Restricted Data are data that: (1) are not available from public sources; (2) could be directly used to impact the operation of the Bulk Electric System (BES); and (3) if inadvertently released, pose a significant threat to the reliability of the BES.

- **Sensitive Data**: Sensitive Data are data that: (1) are not available from public sources; (2) are Confidential Data as defined in the NERC Rules of Procedure; or (3) are Transmission Function Information as defined by the FERC Standards of Conduct.

- **Non-Sensitive Data**: Non-sensitive Data are data that: (1) are available from public sources; (2) are not Restricted Data; and (3) are not Sensitive Data.

If the request is for Non-Sensitive Data, then Peak’s initial recommendation will be to approve the data request. The validity of the request and the viability of the requestor are not factors relevant to the release of Non-Sensitive Data. If the request is for Sensitive or Restricted Data, then Peak must evaluate the validity of the request and the viability of the requestor.

Valid Request

A request for data will be considered valid if: (1) the objective of the data request is to conduct research or develop tools or technologies that have the potential to enhance the reliability of the Western Interconnection; and (2) the requested data and the proposed research methodology are reasonably aligned to achieve the proposed objective.

If Peak determines that the proposed use of Sensitive or Restricted Data does not have the potential to enhance the reliability of the Western Interconnection, or the requested data is not reasonably aligned with the research objective, then Peak’s initial recommendation will be to deny the data request. Requests for Sensitive or Restricted Data will be denied if the request is invalid, regardless of the viability of the requestor. If the request is found to be valid, then Peak must evaluate the viability of the requestor.

Viable Requestor

There will be a rebuttable presumption that the Data Requestor is viable if one of the following conditions are met:
• The Data Requestor is a Department of Energy (DOE) Laboratory;
• The Data Requestor is a research institution that has previously undertaken research for the National Security Agency, Department of Defense, or DOE related to national security, with its security clearances still in force;
• The Data Requestor has received appropriate clearance from FERC, with its security clearance still in force;
• The Data Requestor has met or has the ability to meet the then current NERC Cyber Security Requirements and has processes in place to comply with the then current FERC Rules of Procedure;
• The Data Requestor has at least $2 million in liability insurance from an insurance provider reasonably acceptable to Peak, thereby, demonstrating that the Data Requestor has been vetted by the insurance provider and is considered viable by the provider.

Peak’s Initial Recommendation

Peak’s initial recommendation will be to approve the data request if:

• The request is for Non-Sensitive Data; or
• The request is for Sensitive or Restricted Data and the request is valid and the requestor is viable.

Peak’s initial recommendation will be to deny the request for Sensitive or Restricted Data if:

• The request is invalid; or
• The requestor is not viable.

Peak will post its initial recommendation with an explanation of its decision and supporting information on its website. Peak will notify the Data Requestor, designated Data Providers, other Peak Members, and any interested stakeholders of the posting of its initial recommendation. If Peak’s initial recommendation is to approve the request, Peak will also provide an estimate of the fee to be charged to the Data Requestor if the request is ultimately granted.

VI. Comment Period and Convening of the DSRG

Following Peak’s issuance of its initial recommendation, the Data Requestor, Data Providers, and other interested parties will have 30 days to comment. Comments will be posted on the Peak website.

In anticipation that objections to Peak’s initial recommendation may be received, concurrent with the posting of Peak’s initial recommendation, Peak will convene a Data Sharing Review Group and organize a first meeting to be held soon after the closing of the 30-day comment window.

If no comments opposing Peak’s initial recommendation are received, the DSRG members will be alerted that their services are not needed, and Peak’s initial recommendation will become its final determination.
V. Data Sharing Review Group Process

If comments opposing Peak’s initial recommendation are received—either from Data Providers or other stakeholders objecting to the approval of a request or from non-data-providing members or stakeholders objecting to the denial of a request—the DSRG process will be mobilized.

The DSRG will consist of either (1) one representatives from Class 1, one representatives from Class 2 and one representative from Peak’s non-data-providing membership classes, or (2) two representatives from Class 1, two representatives from Class 2, and three representatives from Peak’s non-data-providing membership classes. Classes 1 and 2 will be responsible for selecting their representative(s), and the non-data-providing membership classes will be responsible for selecting their representative(s).

The DSRG will serve as advisor to Peak. It will review comments and determine whether they are well reasoned and supported by facts. It will consult with the commenters to receive clarification or to obtain their reaction to the comments of other parties. Finally, the DSRG will advise Peak on its final determination to approve or deny the request. The DSRG will submit its advice to Peak within 30 days of the close of the comment period.

The DSRG will conduct itself in an open and transparent manner, and all meeting of the DSRG will be public. Peak Reliability is incorporated in Utah, which has strict rules regarding the closure of public meetings. Under Utah law, closing a public meeting to facilitate discussion is not lawful; the only legitimate reason to close a meeting of the DSRG would be to protect confidential information. However, since the role of the DSRG is to address the issues associated with data release rather than a review of the data itself, closing a meeting to review confidential data appears avoidable.

VI. Peak Final Determination

Within 30 days of receiving the advice of the DSRG, Peak will issue its final determination regarding the approval or denial of a data request. In reaching its final determination, Peak will give considerable weight to the recommendation of the DSRG.

Peak’s final determination will be to approve the data request if:

- The request is for Non-Sensitive Data; or
- The request is for Sensitive or Restricted Data and the request is valid and the requestor is viable.

Peak’s final determination will be to deny the request for Sensitive or Restricted Data if:

- The request is invalid; or
- The requestor is not viable.

Peak will post its final determination with an explanation of its decision on its website and issue a notice of the posting. Peak will retain a record of its final determinations on its data-sharing website to document its decisions and to assist other data requestors in preparing initial data request applications.
VII. Appeal Process

Data Requestors or affected Data Providers may appeal an adverse decision. The appeal process is as follows.

- Within 30 days of the posting of Peak’s final determination, a party receiving an adverse decision may submit a written appeal stating their case. The written appeal must clearly explain how Peak’s final determination was based either on an error of fact or the misapplication of the vetting process. Assertions of misapplication of the vetting process must relate to Peak’s determination of the sensitivity level of the requested data, Peak’s determination of the validity of the request, or Peak’s determination of the viability of the requestor.

- Upon receipt of the written appeal, Peak will convene a Data Request Appeal Panel (DRAP). The DRAP will consist of one representative selected by the Data Providers, one representative selected by the non-data-providing members, and one member of the Board of Directors. The representatives of the Data Providers and the non-data providing members should be selected from senior management and may not have been involved in any Peak decision to deny or modify the request and shall not have served on any DSRG that reviewed the request.

- Peak will submit the written appeal to DRAP. If a Data Requestor and one or more affected Data Providers appeal a decision regarding the same data request, the Panel shall consider the appeals together.

- The Panel shall conduct its business in an open and transparent manner, and meetings of the DRAP will be public. Peak Reliability is incorporated in Utah, which has strict rules regarding the closure of public meetings. Under Utah law, the only legitimate reason to close a meeting of the DRAP would be to protect confidential information. However, the role of the DRAP is not to review actual data, but to address whether Peak’s final determination was appropriate and not based on an error of fact or the misapplication of the vetting process, therefore, closing a meeting to review confidential data appears avoidable.

- All decisions of the DRAP must be unanimous. If unanimous decisions cannot be reached, the appeal will be denied.

- The DRAP may overturn Peak’s final determination either approving or denying a data request only if it first determines that Peak’s final determination was based on an error of fact or a misapplication of the vetting process.

- If the DRAP concludes that Peak’s final determination was based on an error of fact or the misapplication of the vetting process, then the DRAP may vote to overturn Peak’s final determination. If the Panel votes unanimously to overturn Peak’s final determination, the determination is overturned and the outcome final. If Peak’s final
determination was to approve the data request, the request is denied. If Peak’s final determination was to deny the data request, the request is approved.