LADWP – New Regulation for Procurement of Cyber Assets and Services

Dear vendors,

Effective October 1, 2020, LADWP is required to comply with North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standard-013. Pursuant to the CIP-013 Standard and LADWP's CIP-013 Supply Chain Cyber Security Risk Management Plan, LADWP must implement changes to its procurement process and **prequalify** vendors that participate in bidding opportunities for the procurement of cyber assets, equipment, software, or services supporting the Bulk Electric System.

> *A **Bulk Electric System** is defined as facilities and control systems necessary for operating an interconnected electric energy network including electrical generation, transmission, and interconnection systems and all associated software and equipment used to control and operate voltages of 100 kV or higher.*

To be prequalified by LADWP, vendors are required to provide a cybersecurity risk profile information that will be evaluated by LADWP – the evaluation includes an assessment of the vendor's organization, access control, technical controls, incident response, network security, and overall security posture.

All LADWP *Invitation for Bids* and *Request for Proposals* for the procurement of cyber assets, equipment, software, or services supporting the Bulk Electric System will be exclusively advertised to vendors that are on LADWP's Prequalified List of Cyber Vendors. Vendors that seek to be prequalified by LADWP shall **submit** a completed **CIP-013 Vendor Risk Assessment Questionnaire** form as follows:

1. Download a copy of LADWP's **CIP-013 Vendor Risk Assessment Questionnaire** form from:
   https://www.ladwp.com/CIP13scrm

2. Complete the **CIP-013 Vendor Risk Assessment Questionnaire** form

3. Submit a completed **CIP-013 Vendor Risk Assessment Questionnaire** form to the following email address:
   VendorCyberRisk@ladwp.com

As an alternative, vendors may submit any of the following documents in lieu of completing LADWP's CIP-013 Vendor Risk Assessment Questionnaire.

- **a.** Submit a nationally or internationally accepted "certification" to an established cyber security framework or standard such as IEC 62443 or ISO 27001 to VendorCyberRisk@ladwp.com; or
- **b.** Submit a completed copy of North American Transmission Forum (NATF) – **Energy Sector Supply Chain Risk Questionnaire** form to VendorCyberRisk@ladwp.com.The NATF form is located at:
  https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

If LADWP is unable to assess the Vendor's risk based on responses provided on the Vendor Risk Assessment Questionnaire or alternative documents, LADWP will return the incomplete response and request for more information. Once a cyber security risk assessment of a vendor is completed, LADWP will inform the vendor of the results.

LADWP will manage all inherent and residual risks based on established practices and in accordance with the CIP-013 Supply Chain Cyber Security Risk Management Plan. Thank you for your cooperation in supporting the security of LADWP's Bulk Electric System.

For questions, please contact VendorCyberRisk@ladwp.com.

LA DWP

Revision: 09/01/2020