North American Electric Reliability Corporation (NERC)
Critical Infrastructure Protection (CIP)
Reliability Standards

NERC CIP-013-2
Supply Chain Cyber Security Risk Management Plan
Version 6.1

Los Angeles Department of Water and Power
NERC CIP Compliance Program

January 31, 2023

CIP Compliance Office

Power System Regulatory and Innovation Division

Document Version Control

Revision History

Version	Description of Change	Date
1.0	Initial Supply Chain Cyber Security Risk Management Plan	06/01/2020
2.0	Minor updates made to Sections 7.3, 7.4.2, 7.4.3, 7.4.4, 8.1.1, 8.2, 10.2, 12.0, and 12.1	09/20/2020
3.0	• Minor updates to Sections 8, 10, 11, 12, 13, and 14 to provide clarity • Added Section 12.2 • Minor updates to Questionnaire	02/12/2021
4.0	• Added “Cyber Assets” definition to Section 2 • Revised Section 7 and 9 • Minor Formatting to the entire document	01/26/2022
5.0	• Updated SCRM Plan for CIP-013-2 revisions to include requirements for EACMS and PACS associated with BES Cyber Systems	09/30/2022
6.0	• Formatting to table of contents	1/31/2023
6.1	• Formatting Attachment A and Attachment B	4/24/2023

Change history reflects changes to format or content.

LA DWP Los Angeles Department of Water & Power

LADWP CIP-013 Approval Page

Reviewed and approved by:

Name: Glenn Barry

Tittle: CIP Senior Manager

Signature: Glenn T. Barry Digitally signed by Glenn T. Barry Date: 2023.04.25 20:21:54 -07'00' Date: 4/25/2023

Contents

1.0 EXECUTIVE SUMMARY

On October 18, 2018, the Federal Energy Regulatory Commission (FERC) approved the North American Electric Reliability Corporation (NERC) Reliability Standard CIP-013-1 (Cyber Security – Supply Chain Risk Management). The CIP-013-1 reliability standard supplemented the NERC Critical Infrastructure Protection (CIP) Standards to mitigate cyber security risks associated with the supply chain for grid-related cyber systems. The CIP-013-1 Reliability Standard became effective on October 1, 2020.

On March 18, 2021, FERC approved the NERC Reliability Standard CIP-013-2 (Cyber Security – Supply Chain Risk Management). The primary change for the new CIP-013-2 Reliability Standard added Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) associated with high and medium impact BES Cyber Systems (BCS) to the list of applicable systems. The CIP-013-2 Reliability Standard will become effective, and CIP-013-1 will be retired on October 1, 2022.

CIP-013-2 directs utilities to develop one or more documented supply chain cyber security risk management plan(s) that include processes for use in procurements of products (hardware or software) and services for Bulk Electric System (BES) cyber system and their associated EACMS and PACS that will require vendor cooperation and risk assessments to protect the security of the BES cyber system supply chain.

In response, the Los Angeles Department of Water and Power (LADWP) updated its Supply Chain Cyber Security Risk Management Plan (Plan) to comply with the CIP-013-2 requirements to assess, monitor, and mitigate supply chain risks related to vendors of applicable products and services.

To ensure that LADWP's CIP-013-2 implementation plan is based on general industry practices consistent with other utilities in North America, LADWP followed the Supplier Cyber Security Assessment documentation and guidance provided by the North American Transmission Forum (NATF) – an affiliate group that was requested by NERC to develop and share best and leading practices in cyber security supply chain risk management.

As part of the Plan, LADWP will notify all potential cyber asset Vendors of the new regulatory requirements and the CIP-013 supply chain cyber risk evaluation process. LADWP will continue to evaluate vendor risk using technical and procedural controls initially developed for CIP-013-1 that will help identify the security posture of vendors. In addition, LADWP established a CIP-013 Prequalified List of Vendors, monitors prequalified vendors on a continuous basis, and mitigates cyber security supply chain risks across LADWP's Bulk Electric System (BES).

In accordance with CIP-013-2 requirements, the Plan will be reviewed and approved by LADWP's CIP Senior Manager or delegate at least once every 15 calendar months.

2.0 DEFINITIONS

Acceptable Risk Level – An acceptable risk level means a Vendor poses a relatively low risk to LADWP as evaluated by the Cyber Vendor Risk Assessment Committee based on an assessment process that is consistent within the energy industry.

Bidder – Any person or entity that submits a bid or proposal to LADWP or has expressed interest in submitting a bid or proposal in response to a solicitation issued by the LADWP.

Bulk Electric System (BES) – Unless noted in the Inclusions and Exclusions in the NERC Glossary of Terms, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy.

CIP-013-2 – Revised NERC Supply Chain Risk Management Reliability Standard that requires all utilities operating the Bulk Electric System to develop and implement a supply chain cyber security risk management plan that includes processes that ensure security controls for supply chain risk management are applied to procurements of applicable systems.

CIP Exceptional Circumstance – A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large-scale workforce availability.

Cyber Assets – Programmable electronic devices, including hardware, software, and data in those devices. Some examples of Cyber Assets include, but not limited to, are Physical Access Control Systems [PACS], Electronic Access Control and Monitoring System [EACMS], Intermediate Systems [IS], Intrusion Detection Systems/Intrusion Protection Systems [IDS/IPS], Serial Gateways, Dial-up Gateways & Modems, Transient Cyber Assets [TCA], Removable Media [RM], and Relay Protection Devices

Contract – Any mutually binding legal obligation created to acquire goods and/or services from one or more firms, which is paid, or which will be paid, in whole or part, with funds from LADWP. In this context, the terms "contracting", "purchasing", and "procurement" are synonymous and refer to the process or processes under which the LADWP undertakes such acquisitions.

Electronic Access Control or Monitoring System (EACMS) – Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

High Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as high impact according to LADWP's CIP-002-5.1a R1 BES identification and BCS categorization processes.

Medium Impact BES Cyber Systems – Applies to BES Cyber Systems categorized as medium impact according to LADWP's CIP-002-5.1a R1 BES identification and BCS categorization processes.

North American Transmission Forum (NATF) – Affiliate group that includes members from investor-owned, state-authorized, municipal, corporative, U.S. federal, and Canadian provincial utilities to exchange information related to improving the reliability of the transmission systems in the U.S. and Canada.

Physical Access Control Systems (PACS) – Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

Prequalified List of Vendors – Group of Vendors that are allowed to receive solicitations and submit bids or proposals for procurement of cyber assets including hardware, software, and services subject to CIP-013. This list does not guarantee contract opportunities and does not give any exemptions from LADWP's purchasing protocols, terms and conditions, and requirements.

Prime Contractor – The Contractor or Consultant who enters into contract with the LADWP and who is primarily responsible for performance under such contract.

Subcontractor – An individual, firm or corporation having a direct contract with the Contractor for the performance of a part of work which is proposed to be constructed or performed under the contract or permit, including the furnishing of all labor, materials or equipment. A Subcontractor shall perform a commercially useful function.

Vendor – Persons, companies, or other organizations with which LADWP, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators. Vendors subject to CIP-013 are limited to Prime Contractors.

Refer to the NERC Glossary of Terms for other capitalized defined terms (www.nerc.com).

3.0 ROLES AND RESPONSIBILITIES

The following internal stakeholders have critical roles and responsibilities as part of the implementation of the Supply Chain Cyber Security Risk Management Plan:

CIP Compliance Office – Responsible for assisting in the assessment of risks posed by potential vendors, enforcing the Supply Chain Cyber Security Risk Management Plan, and tasked as the repository of evidence and supporting documents related to CIP-013.

CIP Senior Manager – A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.

City Attorney's Office – Provide guidance to Supply Chain Services in establishing contract agreements and when necessary, advise the Vendor Risk Committee on the evaluation and prequalification of potential vendors.

Enterprise Cybersecurity Services – Assist in performing Information Technology related vendor cyber risk assessment in collaboration with Supply Chain Services and CIP Compliance Office.

Requestor – LADWP personnel (full time, part time, and temporary employees) that procure and/or install High or Medium Impact BES Cyber Systems.

Supply Chain Services – A Division responsible for managing the procurement of materials and services for LADWP as well as posting the CIP-013 Vendor Risk Assessment Questionnaire to the vendor community, informing vendors that are evaluated as ACCEPTABLE RISK after a cyber risk assessment process, posting LADWP's Prequalified List of Vendors, and issuing or advertising applicable solicitations only to Prequalified Vendors.

Vendor Risk Committee – Responsible for evaluating risks posed by potential vendors, establishment of the CIP-013 prequalified list of vendors, monitor prequalified vendors, and develop mitigation measures for minimizing supply chain related cyber risks to LADWP's BES. The committee consists of members of the Enterprise Cybersecurity Services Office, CIP Compliance Office, and Supply Chain Services. Impacted internal stakeholders may be invited to provide technical advisory services as part of the evaluation process.

4.0 PURPOSE AND BACKGROUND

The purpose of LADWP's Supply Chain Cyber Security Risk Management Plan is to provide a mechanism to mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems as required by CIP-013.

Effective October 1, 2022, CIP-013-2 became enforceable for all utilities operating the BES in North America. This revised NERC CIP standard affects the changes to procurement of equipment, software, and services related to the BES and their associated EACMS and PACS that may pose cyber security risks to LADWP's power system. **Only** vendors that applied to partake in LADWP's CIP-013 risk management evaluation process, evaluated to pose an acceptable risk, and included on LADWP's Prequalified List of Vendors will be allowed to participate in LADWP's procurement opportunities for cyber assets and services related to the BES.

As part of the application to be placed on LADWP's Prequalified Vendor List, potential vendors have to perform the following steps:

1. Read the instructions and complete the CIP-013 Vendor Risk Assessment

Questionnaire as accurately and comprehensively as possible.

2. Send the completed response to VendorCyberRisk@ladwp.com.
3. Get a confirmation from LADWP that the vendor was evaluated to have an ACCEPTABLE RISK LEVEL and included in LADWP's Prequalified List of Vendors in order to conduct business with LADWP for CIP-013 purposes.

5.0 SCOPE

The scope of CIP-013 encompasses LADWP's High Impact BES Cyber Systems and Medium Impact BES Cyber Systems. The scope also includes all LADWP personnel (full time, part time, and temporary employees), including Prime Contractors, Subcontractors, consultants, volunteers, and vendors who purchase or install High or Medium Impact BES Cyber Systems. This plan is invoked when equipment, software, or a service related to High or Medium Impact BES Cyber Systems is procured.

6.0 STANDARD REQUIREMENTS

This plan addresses all the requirements under NERC's CIP-013-2 Reliability Standard.

6.1 Requirement #1 (R1) states:

" Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS)."

R1 requires utilities to develop and document one or more plans for high and medium impact BES Cyber Systems and their associated EACMS and PACS.

R1.1 describes planning processes for the procurement of applicable BES Cyber Systems and their associated EACMS and PACS that include the development of a vendor risk identification and assessment methodology to mitigate cyber security risks to the reliability and security of the BES. Such cyber security risks must be identified and assessed for procurements of "*vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).*"

R1.2 requires LADWP to develop one or more processes used in procuring BES Cyber Systems, and their associated EACMS and PACS to mitigate residual risks associated with vendor products or services that occur after the procurement process. These residual risks include six sub-parts that may or may not be present in each applicable procurement depending on the nature of the procurement.

- Part R1.2.1 addresses notifications to LADWP by the vendor of vendor-identified incidents related to products or services that may pose cyber security risks;
- Part R1.2.2 addresses coordination of responses between LADWP and the vendor to vendor-identified incidents;

- Part R1.2.3 addresses notifications to LADWP by vendors if remote or onsite access is no longer required by vendor representatives;
- Part R1.2.4 addresses disclosures and remediation to LADWP by vendors of any known vulnerabilities related to the vendor's products or services;
- Part R1.2.5 addresses verifications of software integrity and the authenticity of all software and patches provide by the vendor for use in LADWP's applicable BES Cyber Systems and their associated EACMS and PACS; and
- Part R1.2.6 addresses coordination of controls for vendor-initiated remote access sessions that connect to LADWP's applicable BES Cyber Systems and their associated EACMS and PACS.

6.2 **Requirement #2 (R2)** states:

"Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1."

R2 requires utilities to implement R1 for each applicable procurement of BES Cyber Systems and their associated EACMS and PACS after the effective date of CIP-013-2. As stated above, each provision of R1 may or may not be applicable for a given procurement, depending on the scope of the given procurement. However, the R1 plan must be broad enough and flexible to cover each potential procurement after the effective date of CIP-013-2.

6.3 **Requirement #3 (R3)** states:

"Each Responsible entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months."

R3 requires LADWP's CIP Senior Manager or delegate to review and approve the R1 plan initially on or before the effective date of CIP-013-1 and at least once every 15 calendar months thereafter. This periodic compliance task is similar to the 15-calendar month periodic review and approval process already in place for CIP-002-5.1a and will be subjected to the same LADWP internal controls to track and manage periodic activities as are used for those associated with existing NERC Standards to ensure compliance with this requirement.

7.0 VENDOR OUTREACH & COMMUNICATION

7.0 A separate e-mail account, VendorCyberRisk@ladwp.com, is created and used to communicate with all CIP-013 applicable Vendors.

7.1 CIP Compliance Office coordinates with Power System Divisions and Information Technology Services Division to compile a list of CIP-013 applicable Vendors.

7.2 CIP Compliance Office and Supply Chain Services collaborate to develop an outreach campaign to inform applicable vendors of upcoming supply chain process changes as a result of CIP-013 requirements.

7.3 The outreach campaign includes communication of LADWP's CIP-013 risk assessment requirements to:

7.3.1 All vendors that currently provide and previously provided cyber assets and services to LADWP.

7.3.2 All applicable vendors registered on LADWP's vendordatabase.

7.3.3 All applicable vendors registered on the City of Los Angeles - Business Assistance Virtual Network (BAVN) vendor database.

7.3.4 All applicable Small Business and Disabled-Veteran Business Enterprise advocacy groups in the greater Los Angeles area.

7.3.5 All Southern California business advocacy groups, associations, and Chambers of Commerce including the National Association of Women Business Owners, Greater Los Angeles African American Chamber of Commerce, Latin Business Association, Asian Business Association, Los Angeles Chamber of Commerce, South California Hispanic Chamber of Commerce, and Valley Industry and Commerce Association.

7.4 The Outreach Campaign will also include:

7.4.1 Posting of information about LADWP's CIP-013 Vendor Risk Assessment Program on Supply Chain Service's regular publications such as "SupplyLine Newsletter".

7.4.2 Posting of information about LADWP's CIP-013 Vendor Risk Assessment Program on the City of Los Angeles - Business Assistance Virtual Network (BAVN) portal to encourage potential vendors to apply and get placed on the Prequalified List of Vendors.

7.5 The Vendor Risk Committee will evaluate each Vendor based on an industry standard Vendor Risk Assessment process.

8.0 VENDOR RISK ASSESSMENT

8.1 Vendor risk assessments can be based on either one or more of the following actions:

8.1.1 Vendor submits a nationally or internationally accepted "certification" to an established cyber security framework or standard such as IEC 62443, ISO 27001.

OR

8.1.2 Vendor completes the online CIP-013 Vendor Risk Assessment Questionnaire found at www.ladwp.com/cip13scrm

8.1.2.1 In lieu of LADWP's CIP-013 Vendor Risk Assessment Questionnaire, the Vendor may send to LADWP their responses to the NATF Energy Sector Supply Chain Risk Questionnaire posted on Supply Chain Cyber Security Industry Coordination site: https://www.natf.net/industry-initiatives/supply-chain-industry-coordination.

8.1.2.2 If LADWP is unable to assess the Vendor risk based on the responses to the Vendor Risk Assessment Questionnaire, LADWP will return the incomplete response and request more information.

8.2 **Scoring Criteria:** The Vendor Risk Committee assesses Vendor risk based on responses provided on the Vendor Risk Assessment Questionnaire form using the Vendor Risk Assessment Calculator (VRAC) scores given by each member of the Vendor Risk Committee are averaged to reach a final score. There are two different question types on the Vendor Risk Questionnaire, which are scaled responses (0-3) and Y/N questions.

The following general guidance is used to determine scoring for each scaled question:

0 – No response, inadequate response, or response not related to the question

1 – Partially meets standard industry practices

2 – Adequately meets standard industry practices

3 – Exceeds standard industry practices

The scaled responses are customized for each applicable question to determine how the response fits into the general guidance above. The Y/N responses are evaluated on a case-by-case basis depending on the question. In general, a “Y” scores 5 points, while an “N” scores 0 points. In limited cases, a “N” response is evaluated as less risky than a “Y” response, but these cases are indicated in the VRAC Applicability (column L).

The Vendor Risk Assessment Calculator pulls the vendor responses for both question types from the Vendor Risk Questionnaire and applies the correct scoring criteria to derive an initial quantitative score. Vendors are requested to provide relevant qualifying information in the Notes column, which will be evaluated by the Vendor Risk Committee. Committee members may adjust the calculated score for a given question up or down based on the comment review. Higher final calculated scores indicate lower overall vendor supply chain risk.

8.3 **Risk Evaluation**: The Vendor is notified of the risk rating determination by Supply Chain Services.

8.3.1 Based on industry practice, a Vendor should receive an average score of 70% or above of the maximum score on the quantitative and qualitative evaluation of the vendor risk questionnaire to be considered as having Acceptable Risk. If the Vendor is evaluated to have an Acceptable Risk, the Vendor is added to LADWP’s Prequalified List of Vendors.

8.3.2 Vendors receiving an average score of below 70% on the vendor risk questionnaire are considered to pose Unacceptable Risk to LADWP. In such cases, the Vendor has the option to implement additional security controls for re-evaluation.

8.3.3 In the event where a Vendor that provides highly specialized and/or proprietary material/services is evaluated to pose an Unacceptable Risk to LADWP, an exception can be made through a review and approval process involving the Vendor Risk Committee, LADWP Subject Matter Experts, and the CIP Senior Manager or delegate. Such an exception will require LADWP to develop and implement a mitigation plan(s) to ensure risks are acceptable. Refer to Attachment A.

9.0 ADD VENDOR TO PREQUALIFIED LIST OF VENDORS

9.1 **Only** vendors that applied to partake in LADWP's CIP-013 risk management evaluation process, in accordance with Section 8.0, and evaluated to pose an acceptable risk level will be added to the Prequalified List of Vendors.

9.2 The Vendor Risk Committee will review and update the Prequalified Vendor List. The updated Prequalified Vendor List will be posted monthly.

10.0 PROCUREMENT PROCESS

Perform the following steps to purchase applicable equipment, software, or services from a Vendor:

10.1 Requestor identifies if the procurement is subject to CIP-013 (high/medium impact BES Cyber Systems).

10.2 If the procurement is subject to CIP-013, the Requestor uses the Cyber Asset project workflow in eRSP to create a CIP-013 procurement requisition.

10.3 Once the procurement requisition is completed and approved through the eRSP workflow, Supply Chain Services sends the solicitation only to businesses on LADWP's CIP-013 Prequalified List of Vendors.

10.4 Supply Chain Services works with the Requestor to complete the purchase request following normal LADWP procurement processes.

10.5 Requestor or authorized implementer installs the equipment, software, or receives the service from a Prime Contractor.

11.0 VENDOR RISK MONITORING

Perform the following steps to monitor Vendor risk:

11.1 The Enterprise Cybersecurity Services Office and CIP Compliance Office will establish a risk-based monitoring schedule for Vendors with contracts to supply equipment, software, and services related to CIP-013. Refer to Attachment B.

Guidelines for this schedule are the following:

11.1.1 Vendor surveys are sent to Prequalified CyberAsset Vendors annually.

11.1.2 Vendor responds to the request with updates.

11.1.3 Vendor Risk Committee assesses, and monitors risks based on updates provided by the vendor.

11.1.4 Reevaluation of vendorrisk profiles are based on industry alerts and other utility feedback

12.0 MANAGING INHERENT AND RESIDUAL CYBER SECURITY RISKS

12.0 In the event where participating Vendors are evaluated to pose an Unacceptable Risk to LADWP; a critical Vendor is unable/unwilling to complete the CIP-013 Vendor Risk Assessment Questionnaire; an exigent purchase is made to maintain the reliability of the BES; a purchase is made for urgent operational purposes; a purchase is made in response to an emergency; or a purchase is made for any other justifiable CIP Exceptional Circumstances, an exception can be made by the CIP Senior Manager or delegate(s). Such an exception will require LADWP to develop and implement a mitigation plan(s) to ensure risks are acceptable.

12.1 In the event a cyber asset is procured from a non-prequalified third-party vendor where the cyber asset is provided by a prequalified vendor/manufacturer, special instructions will be provided where the cyber asset will be shipped **directly** to LADWP by the prequalified vendor/manufacturer.

12.2 During the operations and maintenance phase of the procured products or services, to the extent there are residual cyber security risks associated with the implementation of the plan relative to CIP-013 for R1.2 Parts 1.2.1 through 1.2.6, LADWP will implement ongoing mitigating protective measures and controls based on CIP compliance programs and processes:

12.2.1 Residual risks associated with notifications to LADWP by the vendor of vendor-identified incidents under CIP-013 R1.2 Part 1.2.1 will be mitigated by LADWP’s CIP-008 Incident Reporting and Response processes, as applicable.

12.2.2 Residual risks associated with coordination of responses between LADWP and the vendor to vendor-identified incidents under CIP-013 R1.2 Part 1.2.2 will be mitigated by LADWP’s CIP-008 Incident Reporting and Response processes, as applicable.

12.3.3 Residual risks associated with notifications to LADWP by vendors if remote or onsite access is no longer required by vendorrepresentatives under CIP-013 R1.2 Part 1.2.3 will be mitigated by LADWP’s CIP-004

Account Management and Access Control processes, as applicable.

12.3.4 Residual risks associated with disclosures and remediation to LADWP by vendors of any known vulnerabilities related to the vendor's products or services under CIP-013 R1.2 Part 1.2.4 will be mitigated by LADWP's CIP-010 Vulnerability Assessment processes, as applicable.

12.3.5 Residual risks associated with verifications of software integrity and the authenticity of all software and patches provide by the vendor for use in LADWP's applicable BES Cyber Systems and their associated EACMS and PACS under CIP-013 R1.2 Part 1.2.5 will be mitigated by LADWP's CIP-007 Patch Management processes and CIP-010 Configuration Change Management processes, as applicable.

12.3.6 Residual risks associated with coordination of controls for vendor-initiated remote access sessions that connect to LADWP BES Cyber Systems and/or their associated EACMS and PACS under CIP-013 R1.2 Part 1.2.6 will be mitigated by LADWP's CIP-004 Access Control processes, CIP-005 Interactive Remote Access processes, and CIP-007 System Access Control processes, as applicable.

13.0 REVIEW AND APPROVAL

13.1 The Supply Chain Cyber Security Risk Management Plan review process will be as follows:

13.1.1 The CIP Senior Manager or delegate shall perform an initial review and approval of the Supply Chain Cyber Security Risk Management Plan on or before October 1, 2020.

13.1.2 The Plan shall be reviewed by Supply Chain Services, Enterprise Cybersecurity Services Office, City Attorney Office, CIP Senior Manager or delegate, the CIP Compliance Office, and applicable Subject Matter Experts after the initial review and subsequent revisions.

13.1.3 If any changes are identified during periodic reviews, the Plan shall be updated and submitted to the CIP Senior Manager or delegate for final review and approval.

13.2 Supply Chain Cyber Security Risk Management Plan Approvals:

13.2.1 The CIP Senior Manager or delegate shall review and approve this Plan at least once every fifteen (15) calendar months after the initial review.

13.3 Maintenance of Compliance Evidence:

13.3.1 The CIP Compliance Office shall maintain compliance evidence to demonstrate timely reviews of the Plan and documented approvals by the CIP Senior Manager or delegate occurred at least once every 15 calendar months, including:

13.3.1.1 Signed and dated documents indicating the Plan was approved by the CIP Senior Manager or delegate(s), and

13.3.1.2 Any additional CIP-013 compliance evidence, which may include, but is not limited to, policy documents, document updates, revision history, records of review, meeting minutes, vendor surveys and assessments, contract language, or workflow evidence from a document management system

14.0 EVIDENCE RETENTION

All evidence shall be retained in accordance with CIP-013 Standard Evidence Retention provisions.

15.0 ENFORCEMENT

All LADWP personnel (full time, part time, and temporary employees), including Prime Contractors, Subcontractors, consultants, volunteers, and vendors who purchase or install High or Medium Impact BES Cyber Systems and their associated EACMS and PACS affected by this procedure are subject to disciplinary action for failure to comply with its terms, up to and including discharge from employment or breach of contract. In addition, any violation may result in the loss of some or all access privileges (logical and physical). Furthermore, some violations may constitute a criminal offense, as outlined in local, State, and Federal laws.

16.0 REFERENCES

- NERC Reliability Standard CIP-013-2
- NERC CIP-013 Implementation Guidance
- NATF Supplier Cyber Security Assessment Model
- NATF Cyber Security Criteria for Suppliers
- NATF Energy Sector Supply Chain Risk Questionnaire

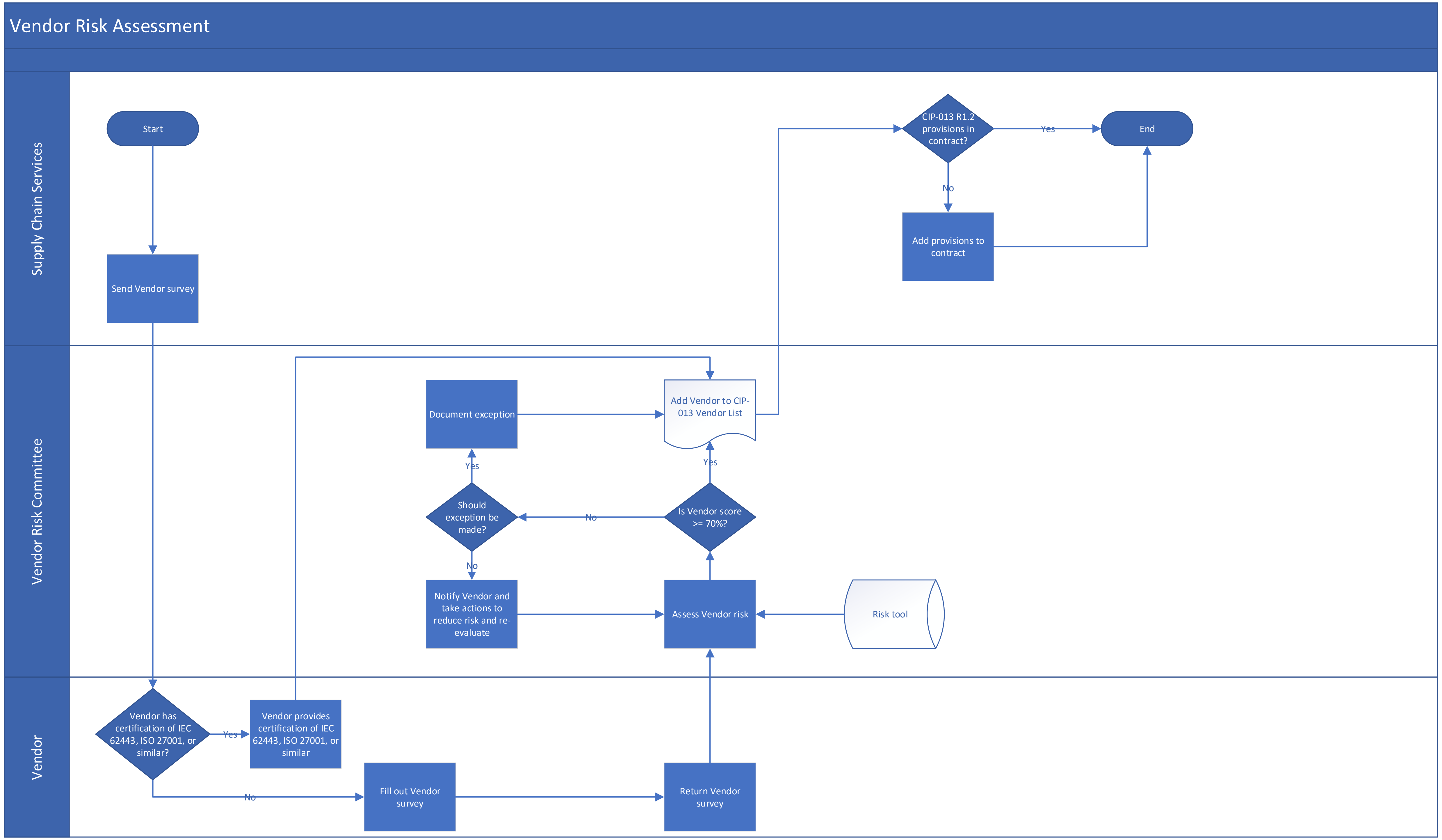
17.0 ATTACHMENTS

A. Vendor Risk Assessment Process

B. Vendor Risk Monitoring Process

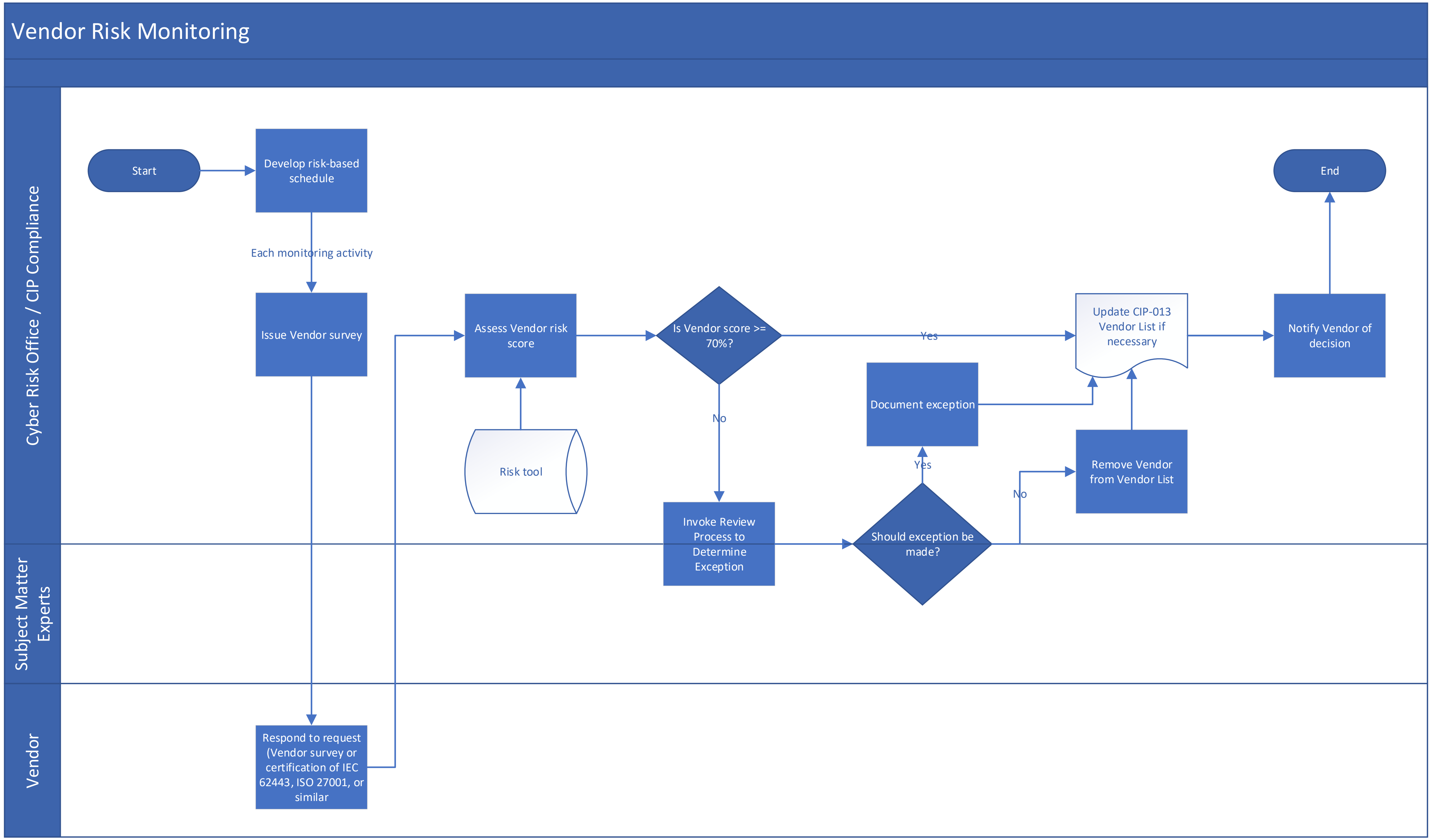
C. Vendor Risk Assessment Questionnaire

ATTACHMENT A – VENDOR RISK ASSESSMENT PROCESS



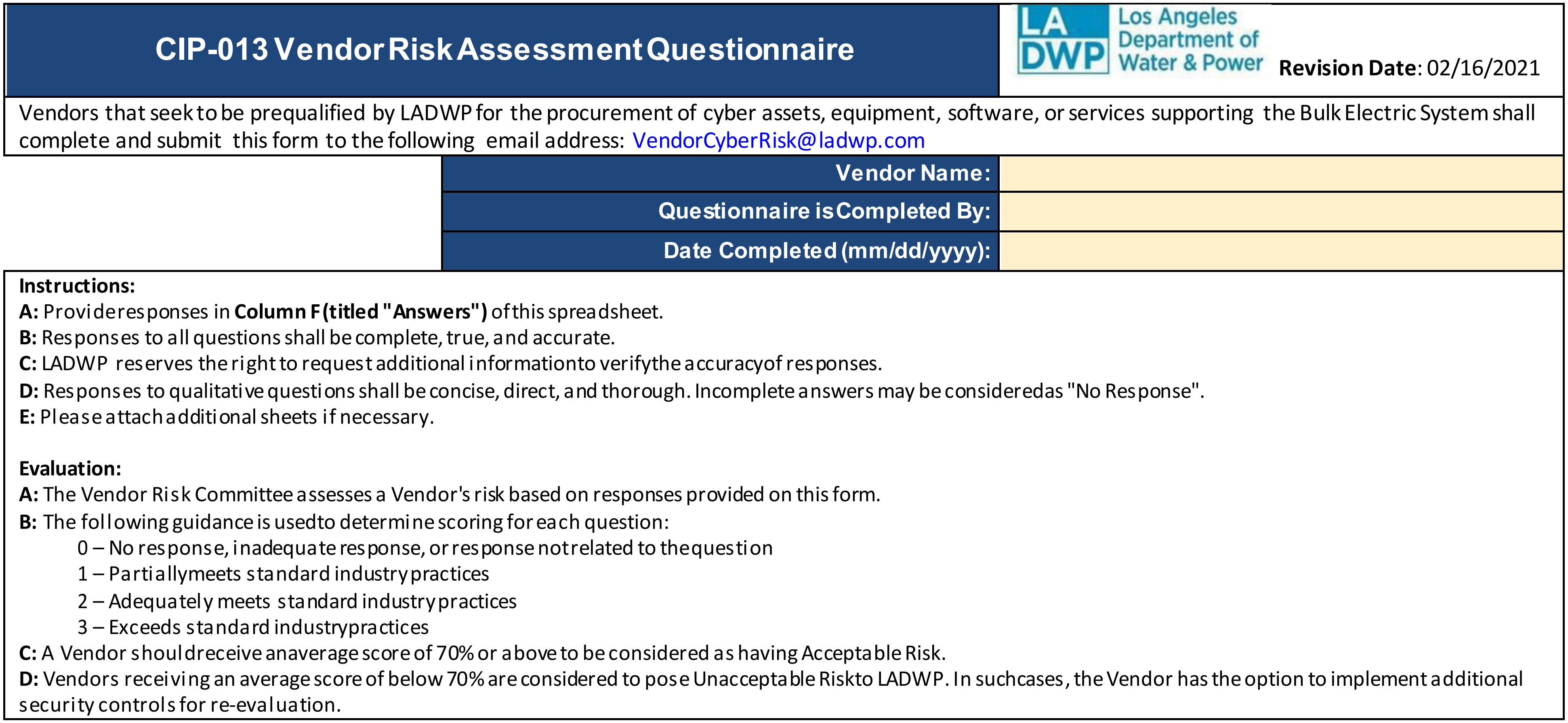
Vendor Risk Assessment
Supply Chain Services
Vendor Risk Committee
Vendor
Start
Send Vendor survey
Vendor has certification of IEC 62443, ISO 27001, or similar?
Yes
Vendor provides certification of IEC 62443, ISO 27001, or similar
No
Fill out Vendor survey
Return Vendor survey
Assess Vendor risk
Risk tool
Is Vendor score >= 70%?
Yes
Add Vendor to CIP-013 Vendor List
No
Should exception be made?
Yes
Document exception
No
Notify Vendor and take actions to reduce risk and re-evaluate
CIP-013 R1.2 provisions in contract?
Yes
End
No
Add provisions to contract

ATTACHMENT B – VENDOR RISK MONITORING PROCESS


Vendor Risk Monitoring
Cyber Risk Office / CIP Compliance
Subject Matter Experts
Vendor
Start
Develop risk-based schedule
Each monitoring activity
Issue Vendor survey
Respond to request (Vendor survey or certification of IEC 62443, ISO 27001, or similar
Assess Vendor risk score
Risk tool
Is Vendor score >= 70%?
Yes
No
Invoke Review Process to Determine Exception
Should exception be made?
Yes
No
Document exception
Remove Vendor from Vendor List
Update CIP-013 Vendor List if necessary
Notify Vendor of decision
End

ATTACHMENT C –VENDOR RISK ASSESSMENT QUESTIONNAIRE

The below questionnaire is currently aligned with utility industry practices across NERC jurisdiction; however, it is subject to change as the industry develops maturity in addressing supply chain cyber security risks.



CIP-013 Vendor Risk Assessment Questionnaire

LA DWP Los Angeles Department of Water & Power **Revision Date**: 02/16/2021

Vendors that seek to be prequalified by LADWP for the procurement of cyber assets, equipment, software, or services supporting the Bulk Electric System shall complete and submit this form to the following email address: VendorCyberRisk@ladwp.com

Vendor Name:	
Questionnaire is Completed By:	
Date Completed (mm/dd/yyyy):	

Instructions:

A: Provide responses in **Column F (titled "Answers")** of this spreadsheet.
B: Responses to all questions shall be complete, true, and accurate.
C: LADWP reserves the right to request additional information to verify the accuracy of responses.
D: Responses to qualitative questions shall be concise, direct, and thorough. Incomplete answers may be considered as "No Response".
E: Please attach additional sheets if necessary.

Evaluation:

A: The Vendor Risk Committee assesses a Vendor's risk based on responses provided on this form.
B: The following guidance is used to determine scoring for each question:

0 – No response, inadequate response, or response not related to the question
1 – Partially meets standard industry practices
2 – Adequately meets standard industry practices
3 – Exceeds standard industry practices

C: A Vendor should receive an average score of 70% or above to be considered as having Acceptable Risk.
D: Vendors receiving an average score of below 70% are considered to pose Unacceptable Risk to LADWP. In such cases, the Vendor has the option to implement additional security controls for re-evaluation.

No.	Area	Standard	Item	Answers
1	**Vendor Organization**	N/A	Vendor Name	
2	Vendor Organization	N/A	Vendor Website URL(s)	
3	Vendor Organization	N/A	Dun & Bradstreet Number	
4	Vendor Organization	N/A	Annual Gross Revenue	
5	Vendor Organization	N/A	Number of Contractors	
6	Vendor Organization	N/A	Product/Service Name	
7	Vendor Organization	N/A	Product/Service Description	
8	Vendor Organization	N/A	Web Link to Product Privacy Notice	
9	Vendor Organization	N/A	Vendor Corporate Headquarters Location	
10	Vendor Organization	N/A	Additional Countries with Vendor Presence	
11	Vendor Organization	N/A	Number of contractors the organization employs in countries other than the United States or Canada (indicate if none)	
12	Vendor Organization	N/A	Geolocation of Data Centers in which Utility Data will be stored	

No.	Area	Standard	Item	Answers
13	Vendor Organization	N/A	Vendor Subsidiaries	
14	Vendor Organization	N/A	Vendor Parent(s)	
15	Vendor Organization	N/A	Vendor Parent(s) Subsidiaries and Divisions	
16	Vendor Organization	N/A	Vendor Contact Name	
17	Vendor Organization	N/A	Vendor Contact Title	
18	Vendor Organization	N/A	Vendor Contact Email	
19	Vendor Organization	N/A	Vendor Contact Phone Number	
20	Vendor Organization	N/A	Please provide certifications that you have obtained related to industry standard security framework (NIST, Cybersecurity Framework, ISO 27001, etc.).	
21	Vendor Organization	N/A	Number of employees	

No.	Area	Standard	Item	Answers
22	Vendor Organization	N/A	Number of years your organization has been in business	
23	Vendor Organization	N/A	Provide the level of current cyber security risk insurance coverage your organization has in place (indicate if none)	
24	**Access Control**	CIP-004, NIST SP 800-53 AC-2	How do you manage electronic and physical access to your devices / software?	
25	Access Control	CIP-004, NIST SP 800-53 AC-2	Who is able to electronically access devices essential to providing the equipment, software, or services?	
26	Access Control	CIP-004, NIST SP 800-53 CM-5	How often do you review electronic access to devices essential to providing the equipment, software, or services?	

No.	Area	Standard	Item	Answers
27	Access Control	CIP-004, NIST SP 800-53 PS-3	Do you perform background checks on employees and contractors? If not, which employees undergo background checks?	
28	Access Control	CIP-004, NIST SP 800-53 PS-3	What do you look for when performing a background check?	
29	Access Control	CIP-004, NIST SP 800-53 PS-3	How often do you renew the background check of employees?	
30	Access Control	CIP-004, NIST SP 800-53 AT-3	For the following topics, identify which most closely represents the training you provided to employees: ▪ Cyber security policies ▪ Physical accesscontrols ▪ Electronic access controls ▪ Visitor control program ▪ Handling of sensitive information ▪ Identification and response to Cyber Security Incidents ▪ Recovery of critical systems ▪Cyber security risks associated with a logical connectivity with outside networks, portable devices, and removable media.	

No.	Area	Standard	Item	Answers
31	Access Control	CIP-004, NIST SP 800-53 AT-3	How often do employees take cybersecurity training?	
32	Access Control	CIP-004, NIST SP 800-53 AC-3	How soon after an employee is terminated is their access (physical or electronic) to devices/software removed?	
33	**CIP Supply Chain**	CIP-013 R1.2.1	Explain the extent to which you would follow a documented process for notifying LADWP of incidents related to products or services that would be provided?	
34	CIP Supply Chain	CIP-013 R1.2.2	Explain the extent to which you would follow a documented process to coordinate responses to incidents related to products or services that would be provided?	
35	CIP Supply Chain	CIP-013 R1.2.3	Explain the extent to which you would follow a documented process for disclosing known vulnerabilities to LADWP related to products or services that would be provided?	

No.	Area	Standard	Item	Answers
36	CIP Supply Chain	CIP-013 R1.2.4	Explain the extent to which you would provide a mechanism to verify the integrity of software provided to LADWP? Examples include file hash check, encryption in transit, and tamper-evident packaging during shipping.	
37	CIP Supply Chain	CIP-013 R1.2.5	Explain the extent to which you would provide a mechanism to verify software source authenticity? Examples include a pre-determined software repository and using trusted digital signatures.	
38	CIP Supply Chain	CIP-013 R1.2.6	If remote access would be required, explain the extent to which you would implement controls to secure Interactive Remote Access (Intermediate System, encryption, and 2-factor authentication) and system-to-system access (explicit access point access list and secure protocol).	
39	**Development Security**	NIST SP 800-161	How do you ensure the security of the software development life cycle?	

No.	Area	Standard	Item	Answers
40	Development Security	NIST SP 800-161	Who can accessthe code?	
41	Development Security	NIST SP 800-161	How do you trackcode updates?	
42	Development Security	NIST SP 800-161	Where are developers located?	
43	Development Security	NIST SP 800-161	Do you perform background checks on developers?	
44	**Incident Response**	CIP-008, NIST SP 800-53 IR-4	Do you have a documented Incident Response Plan for systems? If so, describe.	

No.	Area	Standard	Item	Answers
45	Incident Response	CIP-008, NIST SP 800-53 IR-3	How often do you perform an exercise of the Incident Response Plan for systems?	
46	Incident Response	CIP-008, NIST SP 800-53 IR-4	How often is the Incident Response Plan reviewed and updated for systems?	
47	**Information Protection**	CIP-011, NIST SP 800-53 MP-2	Is any sensitive information (defined as any information that would substantially aid at attacker in compromising systems) shared with 3rd parties?	
48	Information Protection	CIP-011, NIST SP 800-53 MP-2	If so, is this information encrypted at rest and in transit?	
49	Information Protection	CIP-011, NIST SP 800-53 MP-2	Is sensitive information encrypted at rest?	
50	Information Protection	CIP-011, NIST SP 800-53 MP-2	Is sensitive information encrypted in transit? (from your facility to LADWP and from your facility to other entities)	

No.	Area	Standard	Item	Answers
51	Information Protection	CIP-011, NIST SP 800-53 MP-6	How do you securely dispose of sensitive information when discarding or reusing a device?	
52	**Multiple Vendor Levels**		How many different vendors does your product/service rely on?	
53	Multiple Vendor Levels		Do you have any vendors that operate in US Government restricted countries?	
54	Multiple Vendor Levels		Do you have cyber security agreements with none of your vendors, some of your vendors, or all of your vendors?	
55	**Network Monitoring**	CIP-005, NIST SP 800-53 SI-3	How do you monitor your networks for malicious communications?	

No.	Area	Standard	Item	Answers
56	Network Monitoring	CIP-007, NIST SP 800-53 SI-04	Are you monitoring traffic outside your networks, such as threats communicated by your ISP?	
57	**Network Security**	CIP-005, NIST SP 800-53 PL-2	How do you control changes to firewall ACLs protecting your network containing devices essential to providing the equipment, software, or services?	
58	Network Security	CIP-005, NIST SP 800-53 AC-17	Do you allow remote access into your networks?	
59	Network Security	CIP-005, NIST SP 800-53 AC-17	If so, identify the extent to which remote access controls are in place.	
60	**Physical Security**	CIP-006, NIST SP 800-53 PE-3	Do you restrict physical access to your networks?	

No.	Area	Standard	Item	Answers
61	Physical Security	CIP-006, NIST SP 800-53 PE-3	If yes, please describe how you restrict physical access to your networks.	
62	Physical Security	CIP-006, NIST SP 800-53 PE-3	Is physical access monitored 24x7x365?	
63	Physical Security	CIP-006, NIST SP 800-53 PE-3	How are you protecting cabling outside the physically restricted area that connects to your protected networks?	
64	Physical Security	CIP-006, NIST SP 800-53 PE-3	How do you manage visitor physical access to restricted areas?	
65	**Risk Management**	NIST SP 800-39	How often do you perform a risk assessment of your operations to identify high, medium, and low risk?	

No.	Area	Standard	Item	Answers
66	**System Configuration**	CIP-007, NIST SP 800-53 CM-7	How do you limit logical network ports on systems?	
67	System Configuration	CIP-007, NIST SP 800-53 SC-7	How do you prevent the use of physical ports on systems?	
68	System Configuration	CIP-007, NIST SP 800-53 SI-2	How do you ensure security patchesare current on systems?	
69	System Configuration	CIP-007, NIST SP 800-53 SI-2	How often do you check for security patches on systems?	
70	System Configuration	CIP-007, NIST SP 800-53 SI-2	Do you test security patches before installing on systems?	

No.	Area	Standard	Item	Answers
71	System Configuration	CIP-007, NIST SP 800-53 SI-3	How do you prevent malicious code (i.e. anti-virus software) on systems?	
72	System Configuration	CIP-007, NIST SP 800-53 SI-3	How often do you update anti-virus signatures on systems?	
73	System Configuration	CIP-007, NIST SP 800-53 SI-3	Do you test anti-virus signatures before updating on systems?	
74	System Configuration	CIP-007, NIST SP 800-53 AU-2	How do you log security events on systems?	
75	System Configuration	CIP-007, NIST SP 800-53 AU-5	Do you alert based on security logs?	
76	System Configuration	CIP-007, NIST SP 800-53 AU-5	How often are security log alerts monitored on systems?	

No.	Area	Standard	Item	Answers
77	System Configuration	CIP-007, NIST SP 800-53 AU-5	Do you review security logs for systems?	
78	System Configuration	CIP-007, NIST SP 800-53 AU-5	How often are security logs reviewed for systems?	
79	System Configuration	CIP-007, NIST SP 800-53 AU-4	For how many days are security logs retained for systems?	
80	System Configuration	CIP-007, NIST SP 800-53 IA-02	Do you authenticate system accounts with 2-factor authentication for systems?	
81	System Configuration	CIP-007, NIST SP 800-53 AC-2	Do you track shared accounts and who has access to them for systems?	
82	System Configuration	CIP-007, NIST SP 800-53 IA-5	Describe the settings for default accounts on previously purchased systems.	

No.	Area	Standard	Item	Answers
83	System Configuration	CIP-007, NIST SP 800-53 IA-5	How many characters of password length do you enforce for systems?	
84	System Configuration	CIP-007, NIST SP 800-53 IA-5	How many different character classes do you enforce for passwords for systems?	
85	System Configuration	CIP-007, NIST SP 800-53 IA-5	How often must users change their passwords for systems?	
86	System Configuration	CIP-007, NIST SP 800-53 AC-7	Describe the settings for alerting or locking accounts on equipment or systems you provide?	
87	System Configuration	CIP-010, NIST SP 800-53 CM-2	Do you track system baselines for systems? If so, describe.	
88	System Configuration	CIP-010, NIST SP 800-53 CM-3	Describe your process for authorizing system changes for equipment or systems you provide?	

No.	Area	Standard	Item	Answers
89	System Configuration	CIP-010, NIST SP 800-53 CM-3	Do you test changes prior to implementing for systems? If so, describe.	
90	System Configuration	CIP-010, NIST SP 800-53 CM-3	Describe your process to monitor for baseline changes (manually or through an automated tool) for systems.	
91	System Configuration	CIP-010, NIST SP 800-53 RA-5	Do you conduct vulnerability assessments for systems? If so, how often?	
92	System Configuration	CIP-010, NIST SP 800-53 RA-5	If so, what is included in vulnerability assessments?	
93	System Configuration	CIP-010, NIST SP 800-53 AC-20	Do you allow any non-company equipment to be physically connected to systems?	
94	System Configuration	CIP-010, NIST SP 800-53 AC-20	If so, describe the protections in place to prevent malicious code	

No.	Area	Standard	Item	Answers
95	**System Recovery**	CIP-009, NIST SP 800-53 CP-2	Do you have a documented Recovery Plan for systems? If so, describe.	
96	System Recovery	CIP-009, NIST SP 800-53 CP-2	How often is recovery data backed up for systems?	
97	System Recovery	CIP-009, NIST SP 800-53 CP-4	How often do you perform an exercise of the Recovery Plan for systems?	
98	System Recovery	CIP-009, NIST SP 800-53 CP-2	How often is the Recovery Plan reviewed and updated for systems?	
99	**Other**		Describe any other security controls related to your operations that reduce cyber security risk	