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

NERC CIP-013
Supply Chain Cyber Security Risk Management Plan
Version 7.0

May 1, 2025

CIP Compliance Office

Regulatory Compliance Division

Table of Contents

LADWP CIP-013 Approval Page

Review and Approved by:

Name:	Tanesha Smith		
Title:	CIP Senior Manager Delegate		
Signature:	Tanesha Smith Digitally signed by Tanesha Smith Date: 2025.04.28 09:31:50 -07'00'	Date:	4/28/25

1.0 EXECUTIVE SUMMARY

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 Systems (BCS) and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that will require vendor cooperation and risk assessments to protect the security of the BCS 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.

As part of the Plan, LADWP will notify potential CIP-013 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 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 Enterprise Cybersecurity Services 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.

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.

Control Strength Rating – A measure of the effectiveness of a control in mitigating a risk based on the answers provided by a vendor to the questions in the questionnaire from LADWP. The rating can be Strong, Satisfactory, Insufficient, or Weak.

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.

Inherent Risk Rating – The level of risk to an entity before any controls are implemented to alter a risk's impact, likelihood, or both. The rating can be Low, Medium, High, or Critical.

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.

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 or Prequalified Vendor List – 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 or their associated EACMS and PACS 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:

Business Requestor – LADWP personnel responsible for initiating the Vendor Risk Assessment Process and coordinating between LADWP and the vendor for related mitigations, findings, or communications.

CIP Compliance Office – Responsible for providing guidance on regulatory standards, communicating regulatory updates to applicable business units, coordinating with external agencies for regulatory activities, and assisting with the determination of CIP-013 applicability.

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.

Enterprise Cybersecurity Services (ECS) – A division responsible for conducting risk assessments and working with subject matter experts on risk mitigation for third-party vendors on specific risk areas, including but not limited to, IT risk, OT risk, and general cybersecurity risk in collaboration with Supply Chain Services, and CIP Compliance Office.

Requestor – LADWP personnel (full time, part time, and temporary employees) that procure material or professional services associated with high or medium Impact BES Cyber Systems or their associated EACMS and PACS.

Risk Analyst – ECS personnel responsible for conducting the Vendor Risk Assessment.

Supply Chain Services (SCS) – Requirement Owner for CIP-013 R1, R2, and R3. A division responsible for maintaining the CIP-013 Supply Chain Cyber Security Risk Management Plan,

managing the procurement of materials and services for LADWP, managing and monitoring 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, monitoring prequalified vendors, and developing 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 or their associated EACMS and PACS 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. Unless an exception is made, 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 List of Vendors, potential vendors must perform the following steps:

1. Notify LADWP of the vendor's intent to participate in LADWP's CIP-013 procurement activities and request to be placed on LADWP's Prequalified List of Vendors.
2. Provide an appropriate Cyber Security certification or attestation or fill out security questionnaire(s), as detailed in Section 8.0. Vendor should complete the questionnaire(s) as accurately and comprehensively as possible and provide follow up information and responses as needed.
3. Register for a vendor profile within LADWP's procurement system.
4. 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

What: The scope encompasses LADWP High Impact BES Cyber Systems and their associated EACMS and PACS and Medium Impact BES Cyber Systems and their associated EACMS and PACS (including power projects operating within the LADWP CIP Program), pursuant to NERC Standard CIP-013-2.

Who: The scope also encompasses all LADWP personnel (full time, part time, and temporary employees), including Prime Contractors, consultants, volunteers, and vendors who purchase or install high or medium impact BES Cyber Systems or their associated EACMS and PACS.

When Invoked: This plan is invoked when equipment, software, or a service related to high or medium impact BES Cyber Systems or their associated EACMS and PACS is procured.

Intermountain Power Service Corporation (IPSC) utilizes LADWP's Supply Chain Cyber Security Risk Management Plan and Prequalified Vendor List. For the procurement of computing systems and industrial control system hardware, software, and computing and networking services associated with BES operations from a vendor not covered through LADWP's Prequalified Vendor List, IPSC utilizes a Supplemental Supply Chain Cyber Security Risk Management Procedure to mitigate cyber security risks to the reliable operation of the BES.

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 LADWP 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 LADWP 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

7.1 LADWP created a separate e-mail account, VendorCyberRisk@ladwp.com, to communicate with all CIP-013 applicable Vendors. This email is jointly managed by Supply Chain Services and the CIP Compliance Office.

7.2 Supply Chain Services coordinates with the Power System Divisions, and Information Technology Services Division to compile a list of CIP-013 applicable Vendors.

7.3 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.

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

- All vendors that currently provide and previously provided Cyber Assets and services to LADWP.
- All applicable vendors registered on LADWP's vendor data base.
- All applicable vendors registered on the City of Los Angeles - Business Assistance Virtual Network (BAVN) vendor database.
- All applicable Small Business and Disabled-Veteran Business Enterprise advocacy groups in the greater Los Angeles area.
- 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.

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

8.0 VENDOR RISK ASSESSMENT FOR PREQUALIFICATION

Vendors must undergo a vendor risk assessment and have an Acceptable Risk Level to be included on LADWP's CIP-013 Prequalified List of Vendors and to be eligible to participate in LADWP's CIP-013 procurement opportunities. Vendor risk assessments can be based on either one or more of the following actions:

8.1 Cyber Security Certification or Attestation

Vendor submits a nationally or internationally accepted "certification" or attestation to an established cyber security framework or standard, including but not limited to, IEC 62443, ISO 27001, or SOC 2/3.

8.1.1 Acceptance of the certification or attestation to nationally or internationally accepted frameworks is based on NERC recommendations. LADWP considers vendors that provide a certification or attestation as posing Acceptable Risk.

8.2 Vendor Risk Assessment Process

Vendor completes the Vendor Risk Assessment Process conducted by LADWP's ECS Risk Team (Risk Team). The following describes the process at a high level:

8.2.1 Risk Team receives a request from a Business Requestor (BR) to conduct a risk assessment on Vendor.

8.2.2 Risk Team sends a security questionnaire to Vendor. Risk Team uses a Governance Risk Compliance tool, including a scoring matrix, to conduct risk assessment to determine Vendor's risk rating. A Vendor's risk rating is based on the Vendor's Inherent Risk Rating and Control Strength Rating and may be rated as Low, Medium, High, or Critical.

8.2.2.1 Risk Team considers potential CIP vendors to have a High Inherent Risk Rating by default.

8.2.2.2 Risk Team reviews the Vendor's responses to the security questionnaire using predefined scoring criteria. Each response has an assigned score which is used in calculating the Vendor's Control Strength Rating.

8.2.3 ECS Executive Management or delegate reviews and acknowledges Vendor's risk rating.

8.2.3.1 If Vendor's risk rating is Low or Medium, they are considered to have Acceptable Risk, and the outcomes would be:

- Vendor will be added to the CIP-013 Prequalified List of Vendors.
- Therefore, Vendor may participate in future CIP-013 applicable procurement opportunities.

8.2.3.2 If Vendor's risk rating is High or Critical, they are considered to have Unacceptable Risk and the outcomes would be:

- Vendor will not be added to the CIP-013 Prequalified List of Vendors.
- Vendor may work with the BR to request reassessment.

8.3 Special Circumstances

The following considerations are also made regarding vendor risk assessments:

8.3.1 Banned/Sanctioned Entities and Equipment/Service

8.3.1.1 LADWP abides by laws, regulations, and orders set forth by other governmental agencies having jurisdiction that identify vendors with risk characteristics that could adversely impact the BES (e.g., Section 2 of the Secure and Trusted Communications Networks Act of 2019). Vendors banned or sanctioned by such governmental agencies, and vendors who rely on services or products from those banned or sanctioned vendors, shall not be included on the CIP-013 Prequalified List of Vendors.

8.3.2 Open-Source Software

8.3.2.1 The Requestor must perform due diligence regarding any security documentation available from the open-source software provider.

8.3.2.2 When possible, the open-source software provider will undergo the Vendor Risk Assessment Process or submit an eligible certification.

8.3.2.3 LADWP management will review for approval once risks have been identified and appropriate mitigations have been acknowledged.

8.3.3 Vendor Transitions

8.3.3.1 In the event of any change in vendor for a procurement, such as transitioning from one vendor to another, corporate mergers, or company acquisitions, the new vendor must undergo the Vendor Risk Assessment Process or submit an eligible certification or attestation.

8.3.4 Value-Added Reseller or Third-Party Procurements

8.3.4.1 When procuring a product through a value-added reseller (VAR) or third-party reseller, a risk assessment of the Original Equipment Manufacturer (OEM) vendor must be completed in addition to the VAR. If not feasible, the risk assessment will be based on available resources, such as external security rating tools, security documentation (e.g., security certification, industry standard security questionnaires, and security audit reports), and feedback from Subject Matter Experts.

8.3.5 Exceptions to Unacceptable Risk

8.3.5.1 In the event where a Vendor 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/or the CIP Senior Manager or delegate. Such an exception will require the Vendor and/or LADWP to develop and implement a mitigation plan(s). Consideration will be given regarding highly specialized and/or proprietary material/services. For procurements related to CIP Exceptional Circumstances, refer to Section 12.1.

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, that have been evaluated to pose an Acceptable Risk Level, and that have registered within LADWP's procurement system will be added to the Prequalified List of Vendors.

9.2 A Vendor's prequalification status shall be effective until the earliest of either one year after the risk assessment has been completed or the expiration of the accepted certification or attestation to nationally or internationally accepted frameworks.

9.3 Supply Chain Services will communicate the results of the Vendor Risk Assessment Process and will coordinate the renewal process with the Vendor.

9.4 Supply Chain Services will review and update the Prequalified List of Vendors. The updated Prequalified List of Vendors will be posted monthly.

10.0 PROCUREMENT PROCESS

All procurements that are subject to CIP-013 are to be made only from vendors on LADWP's Prequalified List of Vendors. The available procurement avenues for LADWP staff to purchase applicable equipment, software, or services from CIP-013 Prequalified vendors includes, but is not limited to, the following:

10.1 Electronic Request Solicit Procure (eRSP)

10.1.1 Requestor identifies if the procurement is subject to CIP-013 (high/medium impact BES Cyber Systems or their associated EACMS and PACS).

10.1.2 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.

10.1.3 Once the procurement requisition is completed and approved through the eRSP workflow, Supply Chain Services will finalize and publish the CIP-013 solicitation and send invites to applicable vendors via eRSP. Only vendors on LADWP's CIP-013 Prequalified List of Vendors will be allowed to submit a bid for CIP-013 applicable procurements.

10.1.4 Supply Chain Services works with the Requestor to complete the purchase request following standard LADWP procurement processes. Where applicable, provisions related to CIP-013 Requirement R1.2 Parts 1.2.1 through 1.2.6 are included.

10.2 Purchasing Card (P-Card)

10.2.1 CIP-013 applicable P-Card purchases can only be made with a designated CIP-013 P-Card. The Requestor must verify that the intended vendor is on the CIP-013 Prequalified List of Vendors prior to purchase.

10.2.2 A CIP-013 form is required to be submitted for all CIP-013 eligible P-Card purchases at the time of purchase request.

10.3 Procurement Contracts

10.3.1 CIP-013 applicable purchases can be made through existing contracts to streamline and expedite the procurement process for critical projects. An existing contract may be used if it meets at least one of the following criteria:

- Effective date prior to the effective date of the CIP-013-1 Reliability Standard of October 1, 2020.
- Processed through the eRSP procedure described in Section 10.1.
- Vendor is on the CIP-013 Prequalified List of Vendors and an exception with associated mitigation plan has been reviewed and approved by the Vendor Risk Committee, LADWP Subject Matter Experts, and/or the CIP Senior Manager or delegate.

11.0 VENDOR RISK MONITORING

Perform following steps to monitor Vendor risk:

11.1 Supply Chain Services and Enterprise Cybersecurity Services will establish a risk-based monitoring schedule for Vendors with contracts to supply equipment, software, and services related to CIP-013. Guidelines for this schedule are the following:

- Vendors will be notified of their CIP-013 prequalification expiration and be invited to reapply through the standard process.
- Reevaluation of vendor risk profiles will consider industry alerts and other utility feedback.
- Risk Team may use external risk scoring and reporting tools to monitor Vendors' overall security posture.
- Whenever a risk re-assessment is warranted from the above monitoring activities, the Vendor Risk Assessment Process on the vendor may be invoked manually.

12.0 MANAGING INHERENT AND RESIDUAL CYBER SECURITY RISKS

12.1 In the event where participating Vendors are evaluated to pose an Unacceptable Risk to LADWP; a critical Vendor is unable/unwilling to undergo the Vendor Risk Assessment Process; 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 the Vendor and/or LADWP to develop and implement a mitigation plan(s) to ensure risks are acceptable.

12.2 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.

12.3 During the procurement phase of the products or services, where applicable and depending on the nature of the procurement, LADWP includes CIP-013 provisions to address the 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.

12.4 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:

12.4.1 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.

12.4.2 Residual risks associated with coordination of responses between LADWP and the vendor to vendor-identified incidents under CIP-013 R1.2 Part1.2.2 will be mitigated by LADWP's CIP-008 Incident Reporting and Response processes, as applicable.

12.4.3 Residual risks associated with notifications to LADWP by vendors if remote or onsite access is no longer required by vendor representatives 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.

12.4.4 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.

12.4.5 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.

12.4.6 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:

- The CIP Senior Manager or delegate shall perform an annual review and approval of the Supply Chain Cyber Security Risk Management Plan.
- The Plan shall be reviewed by Supply Chain Services, Enterprise Cybersecurity Services Office, CIP Senior Manager or delegate, the CIP Compliance Office, and applicable Subject Matter Experts after the initial review and subsequent revisions. As part of the review process, the City Attorney's Office is requested to review the Plan before it is finalized.
- 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:

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

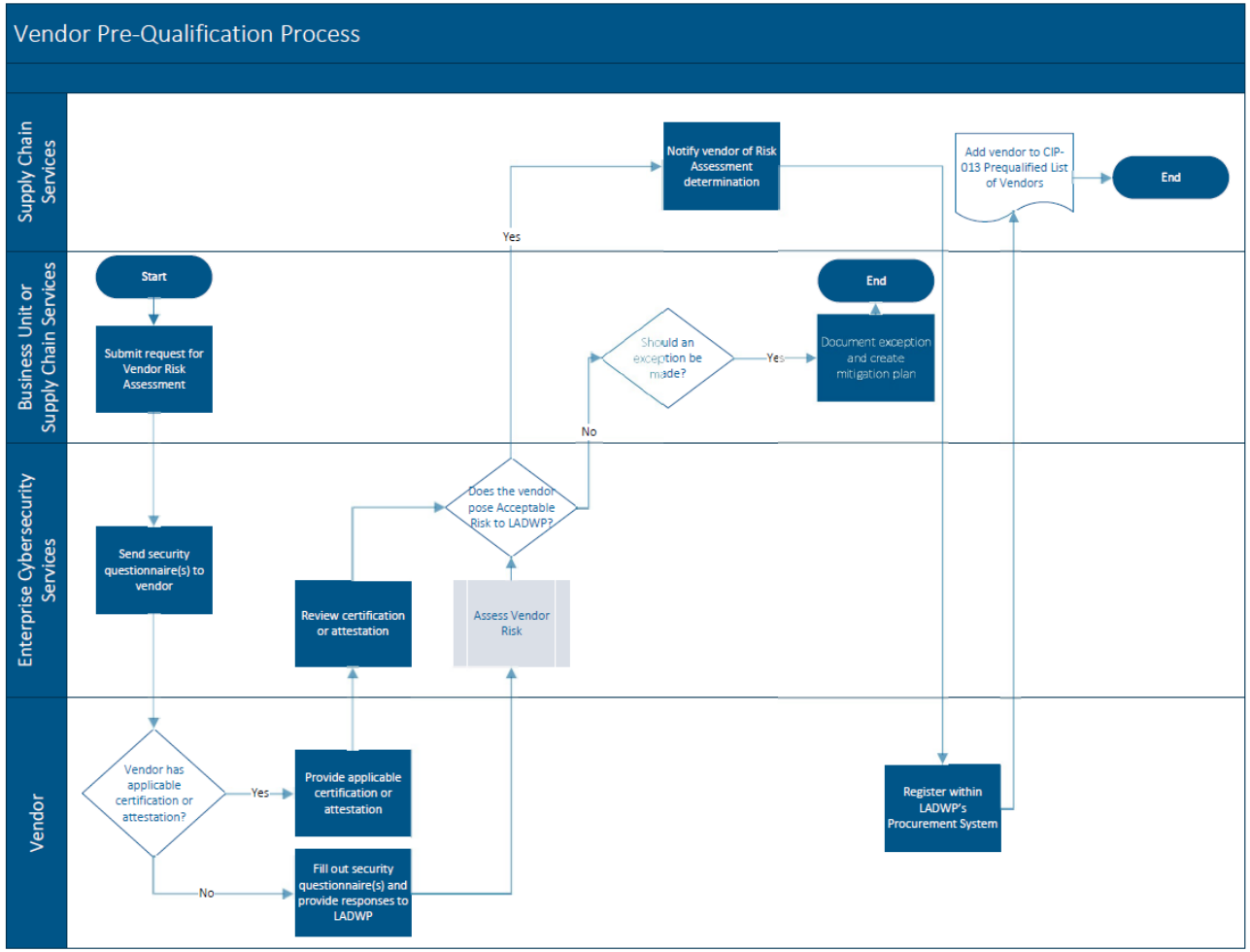
13.3 Maintenance of Compliance Evidence:

- 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 signed and dated documents indicating the Plan was approved by the CIP Senior Manager or delegate(s).

14.0 REFERENCES

- NERC Reliability Standard CIP-013-2
- NERC CIP-013 Implementation Guidance

15.0 ATTACHMENT A – VENDOR PREQUALIFICATION PROCESS



16.0 REVISION HISTORY

Version	Description of Change	Author	Date
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
6.2	Updates to Section 5.0 to include IPP reference Removal of “City Attorney’s Office” from Section 3.0 and 13.1.2.	Justin Aleman	02/07/2024
7.0	Annual Review Major updates to the Plan to reflect the Supply Chain Services Requirement Owner Transition, supporting business unit roles, and Enterprise Cybersecurity Services Vendor Risk Assessment Process Updates to Sections 8.0, 9.0, and 10.0 Modifications to Attachment A. Removal of Attachments B and C Formatting to the entire document	Justin Aleman	05/01/2025

Change history reflects changes to format or content.