California ISO

ISO User Access Administrator (UAA) Establishment and Requirements

Purpose

The purpose of this document is to define User Access Administrator (UAA) responsibilities to ensure appropriate access to the systems and data for which the UAA performs the provisioning of access duties

Benefits

The benefits incurred by external companies by assigning a UAA include the following:

- Greater control over access to company data
- Better position to meet regulatory/audit requirements
- Greater accuracy in requests, which correlates to faster access provisioning

Scope

- The scope of established UAA responsibilities will be across all ISO applications for all user access requirements related to the UAA's area of responsibility.
- The understanding that the UAA for the company will adhere to and abide by data security for their own company as well as other companies under the endorsement access process.

Assumptions

1) Minimally, a primary and secondary UAA will be established for each external company for all ISO application access purposes.
2) For larger organizations, multiple UAA(s) may be required. It is the responsibility of the organization to determine if any of their designated UAA(s) should have a more limited capacity to provisioning access from other UAA(s).
3) When one external entity requests user access to another entity's data, the requesting entity endorses specified users to the other entity requesting the entity owning the data provision the access to specified date.

IMPORTANT: It is the responsibility of each entity's UAA to coordinate and validate the user's identity and access requirements.

Establishment of External UAAs

1) Before establishing a UAA, all companies must review the "ISO User Access Administrator Establishment and Requirements" document and understand the requirements of utilizing ISO certificates. This includes the requirement that all transactions occurring under a user's certificate are the responsibility of that user. Sharing certificates is not allowable. This information is provided to the organizations during the registration or certification process after obtaining an agreement from the ISO website.
2) The establishment of UAA(s) must be made by an individual at the external entity that has an appropriate level of authority to designate UAA(s).

3) Minimally, a primary and secondary UAA must be established for each company. This allows the ISO to continue communications with an entity regarding user access requests when one UAA is not available.

UAA Requirements/Responsibilities

1) All ISO application access requests will be submitted from established UAA(s) based on the user area of responsibility.
2) UAA(s) must validate the identity of users requesting access to ISO systems through means agreeable within their company's practices.
3) UAA(s) must validate:
   - User's job role for requesting access to ISO systems and
   - User must be authorized for the specified applications and permissions being requested.
4) UAA(s) must certify that all data on the Access Request is accurate and valid.
5) Any known changes within a company that will impact the established UAA(s), the UAA or other authorized representative of the company must notify the ISO of those changes by submitting an updated User Access Administrator Agreement form. This form is done through the DocuSign process; therefore, a digital signature is required.
6) UAA(s) must immediately take action in the AIM tool when a user's access to ISO applications is no longer required due to termination or a change in job responsibilities.
7) If a user or UAA suspects that a user's certificate (private key) has been compromised, the UAA must revoke the suspect certificate immediately and notify the ISO of any probably breach of data.
8) Before the UAA(s) can complete the submission request for endorsing ISO application access to user(s) outside of their organization, the UAA must check the ''The information contained herein is Confidential and subject to the FERC Standards of Conduct' acknowledgement box in the AIM application.
9) **Important**: Endorsement of users across ISO applications using the Access Control List (ACL) process **must** be paid particular attention in order to not provision access to unauthorized or users not permitted to have access (i.e. merchant versus regulatory organization in the AIM tool for the same company.
10) Creation of ACL groups can only be created for the following applications: CMRI, MRI-S meter data, WebOMS, and ADS.

Contact Information

- For further information, please email UAARequests@caiso.com or contact your Client Representative.