ISO User Access Administrator (UAA)
Establishment and Requirements

Purpose

The purpose of this document is to define User Access Administrator (UAA) responsibilities, so there is an understanding of the functions the UAA performs.

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

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 UAAs may be required. When this is the case, clear delineation of UAA areas will need to be defined with ISO.
3) When one external entity requests user access to another entity's data, the entity owning the data is required to submit/approve the user access request. It is assumed that coordination between the two entities will occur to validate the user's identity and access requirements.

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.

Establishment of External UAAs

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. The establishment of UAAs must be made by an individual at the external entity that has an appropriate level of authority to designate UAAs. For scheduling coordinators (SCs), UAAs must be identified in the initial certification contract established with ISO's Customer Service department. All other companies will need to identify their UAAs using the "ISO Application Access UAA Establishment and Change Agreement". Any business changes that impact the scope, areas of responsibility, or individuals assigned as UAAs must be communicated to ISO by one of the UAAs or another authorized company representative.

UAA Requirements

1) All CAISO application access requests will be submitted from established UAAs based on their area of responsibility.
2) UAAs must warrant the identity of users requesting access to CAISO systems through means agreeable with their company's practices.

3) UAAs must warrant that users requesting access to ISO systems are authorized for the applications and permissions being requested.
4) UAAs must warrant all data on the ISO Application Access Request Form or Device Certificate Request form is accurate and valid.
5) When any company changes occur which will impact the designated UAAs, an established UAA or other authorized representative of the company must notify ISO with enough advance notice to make any required changes.
6) UAAs must notify ISO immediately when a user's access to ISO applications is no longer required due to termination or a change in job responsibilities.
7) UAAs must understand the requirements of utilizing ISO certificates, which is defined in ISO's Certificate Policies and Certification Practice Statements, including the requirement that all transactions occurring under a user's certificate are the responsibility of that user, and that sharing certificates is not allowable.
8) If a user or UAA suspect a user's certificate (private key) has been compromised, the UAA must contact ISO immediately to revoke the suspect certificate.

Contact Information

For further information, please email UAARequests@caiso.com or contact your Client Representative. To designate or change UAAs, please refer to the "ISO External Application Access User Access Administrator (UAA) Establishment and Change Agreement" document.