# E-Enterprise Federated Identity Management

## Identity Provider Policy Guide Outline DRAFT

## Sections Needing Governance Decisions

### Identity Provider Registration/Adoption

The identity provider services must be able to dependably meet the assurance needs of relying parties who will trust the identities provided by identity providers. The processes by which identity providers will be approved and integrated into EFIM are key to establishing and maintaining trust among the partner organizations.

**Necessary Processes:**

* Establishment of identity provider application
* Determination of identity provider assurance level
* Approval/Denial of identity provider application

**Existing Resources:**

* Identity Federation and Trust Network [[Link](https://usepa.sharepoint.com/:b:/r/sites/OCFO_Work/E_Enterprise/EEnterprise%20Federated%20Identity%20Management/Background%20EFIM%20Documents/Identity_Federation_and_Trust_Framework_Specifications_V3.pdf?csf=1&web=1&e=gc5ghP)]

### Determine Identity Provider Assurance Level

Closely related to its parent governance area, Identity Provider Registration/Adoption, this area of governance includes all processes that support the determination of level of assurance that an identity provider is able to support.

**Necessary Processes:**

* Adoption of standard level of assurance definitions for EFIM
* Leverage the Identity Bridge for this

**Existing Resources:**

* OpenID Connect Compliance [[Link](https://openid.net/wordpress-content/uploads/2019/03/OpenID-Certification-Terms-and-Conditions.pdf)]
* CROMERR Compliance [[Link](https://www.epa.gov/cromerr/cromerr-application-tools-and-templates#Application%20forms)]
* NIST Guidance – 3 attributes
  + CROMERR fits between NIST Assurance levels – not quite what we need
  + More research into NIST required
* Auth0?

### Identity Provider Policy Conformance Auditing

This governance area includes processes for ensuring that identity providers that are participating in the EFIM service maintain the necessary requirements to continue participation in EFIM and to verify that their assigned level of assurance remains appropriate. Identity provider policies, processes, and controls may change over time. This area of governance exists to maintain trust within the enterprise by continually confirming that identity providers conform to all EFIM requirements.

**Necessary Processes:**

* Auditing identity providers after registration to ensure that they continue to comply/conform with all required policies and security requirements
* Ongoing attestation that the IdP is the LoA that they state
* Identity provider reporting processes that allow identity providers to report changes that might impact their level of assurance and/or eligibility to participate in the enterprise
* Leverage the Bridge to track IdP annual compliance – allow the RP to have access to this info