We recommend that LSST adopt the OpenID Connect (OIDC) standard for Web Single Sign-On (SSO). NCSA's CILogon service provides an OIDC-compliant Web SSO service that is available for testing and integration. See http://www.cilogon.org/oidc for details. Choosing CILogon's LSST "skin" will include the LSST logo on the login page.

The CILogon endpoints are:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration</td>
<td><a href="https://cilogon.org/oauth2/register">https://cilogon.org/oauth2/register</a></td>
</tr>
<tr>
<td>Authorization</td>
<td><a href="https://cilogon.org/authorize?skin=LSST">https://cilogon.org/authorize?skin=LSST</a></td>
</tr>
<tr>
<td>Token</td>
<td><a href="https://cilogon.org/oauth2/token">https://cilogon.org/oauth2/token</a></td>
</tr>
<tr>
<td>User Info</td>
<td><a href="https://cilogon.org/oauth2/userinfo">https://cilogon.org/oauth2/userinfo</a></td>
</tr>
<tr>
<td>X.509 Certificate</td>
<td><a href="https://cilogon.org/oauth2/getcert">https://cilogon.org/oauth2/getcert</a></td>
</tr>
</tbody>
</table>

The User Info endpoint will return a JSON structure containing claims matching the following example:

```json
{
  "sub": "http://cilogon.org/serverA/users/534",
  "given_name": "James",
  "family_name": "Basney",
  "email": "jbasney@illinois.edu",
  "voPersonExternalID": "148492@github.com",
  "idp_name": "GitHub",
  "idp": "http://github.com/login/oauth/authorize",
  "uid": "jbasney",
  "uidNumber": "25555",
  "isMemberOf": [
    {"name": "lsst_users", "id": 1363},
    {"name": "lsst_int_lspdev", "id": 1618}
  ]
}
```

The `sub` claim is the user's unique subject identifier. Please use it to uniquely identify the user in your web application.

The `isMemberOf` claim contains the user's group memberships which convey authorization in LSST.

The `uid` and `uidNumber` claims contain the user's NCSA username and user IDs.

The `voPersonExternalID` claim contains the external identity linked to the user's NCSA identity (if the user logged in with an external identity provider using Federated Identity).

Any questions/comments? Please post to our https://lists.lsst.org/mailman/listinfo/iam email list.