Cross-team features and capabilities list

Registries work stream

- Support identity data workflow: Load, Validate, Normalize, Standardize, Reconcile (Identity Match)
- Standardized APIs for registry to consumer system provisioning
- Change-log and event-driven endpoints for provisioning and integration
- Interfaces to support self-service identity data management
- Delegated admin of identity workflow: Merge/split identities, early onboarding, audit & reporting
- Allow choice of databases
- Scale from small to large deployments
- Supports HA and DR deployments
- Provide monitoring hooks

Provisioning and Integration work stream

- RESTful APIs for Registry-to-Consumer system (de-)provisioning
  - event-driven push style
  - consumer-initiated pull
    - per user id
  - bulk provisioning
  - SCIM binding (defined SCIM schema extension for CIFER registry to consumer data model (users, groups, entitlements)
- Event-driven notification endpoint provided by Registry (JMS, XMPP)
- Configurable Diff-based provisioning engine
  - E.g., consumers request all user/group changes
    - that have occurred since their last request
    - that have occurred since a given point in time
    - that have occurred since a given change log rowId
- Configurable flat-file (re)generation utility
  - configurable population filter
  - configurable selection of data fields
- Support for data routing, transformation and connectors per standard enterprise integration patterns
- Provide monitoring hooks

Authentication work stream

- Multi-factor AuthN integrated into packages commonly used by CIFER-adopting institutions (namely Shib and CAS)
- Social2SAML so that SAML-protected web apps and relying parties have the option of serving populations who authenticate via a social IdP of their choice
- Account lifecycle management: From identity proofing through credential issuance to password management and Identity Assurance Profile support
  - Account claim/activation process
  - Password sync
- Self-service account linking (associate multiple log-in credentials with a single person identity)
- Authentication to native mobile apps
- Support for delegation scenarios (avoiding the impersonation model via technologies like SAML Enhanced Client or Proxy)
- Process authentication (How can services authenticate for, say, access to protected APIs)
- Provisioning of account information into other systems (Radius, Cloud services…)
- Provide monitoring hooks

Access Management work stream

- Management services for group, role and privilege-based access control,
- Management services for creation and deployment of authorization policies and permissions
- Standardized representations for permissions and their atoms (Subjects, Actions, Resources, Limits)
- APIs for access management services
- UIs for access management services
- Monitoring hooks

Identity Console work stream

- Self-service UI for identity-related actions
- Access request administration
- Password strength and reset policy configuration
- Admin UI for monitoring, configuring IAM services and flows
  - cross-function log and audit tools