



Project Name	IAM Program – IAM Lifecycle Committee		
Meeting Date	July 21, 2014	Meeting Time	10:30 – 12:00
Location/ Conference #	Smith Campus Center 561	Meeting Host	Jane Hill

**Invitees**

Mike Burke	
Teresa Butler	X
Julie Broad	
Peggy Callinan	X
Ann-Marie Costa	X
Courtney Harwood	X
Michael Humphreys	X
Tom Mayhew	X

Isabelle Modiano	X
Susan Richelson	
Susan Vomacka	
Kwok Yu	X
Jennifer Ryan	X
Gretchen Grozier	X

**Agenda and Notes**

July meeting opened at 10:35 a.m. and concluded at 12:05.

Agenda Items:

1. POI – Is a category of affiliated member of the community who is not an employee, not a traditional student (including class participants) or a library borrower – “they are something else” Discussion of what it means to be an employee turned to the unpaid appointee, and the confusions, and sometimes issues around when these appointments should be in the HR system and when they should not. There are defined rules for academic appointments, but some categories off affiliates like Fellows (including Post Doctoral Fellows) can even raise compliance issues for HR policy. It is clear that student fellowships paid through PeopleSoft (PS)(because it is expedient to do so) are not employees.
  - a. With the exception of student fellowships, all paid and unpaid roles that originate in PS are lumped under the umbrella role category of “employee” and historically are accorded online access as “employees” for services like library e-resources, or other web access
  - b. Isabelle says ideally, for an unpaid appointment in PS, an appointment letter will exist. The policies governing the academic appointments are domain of Academic Affairs. There is a body of University guidance that is published by the Provost’s Office
  - c. Some persons’ appointments as “Fellows” or “Visiting Fellows” will use the POI role type. This is not an issue on the surface, but it is noted that as non-employees they will not have the same access privileges, in general.
  - d. The group agreed that there is reason to believe that the general motivation for appointing individuals via the HR system include:
    - i. Ability to obtain employee verification (proof that the person was at Harvard)
    - ii. Online and also physical access
  - e. Training is required (HIPAA, OSHA) for lab workers and others, and although tracking of the training is done in PeopleSoft, the POIs are tracked in spreadsheets in a more cumbersome way. XID are used as well, which is even more difficult and concerning, as these are un-validated identities.
2. Due to the increase in tracking of digital identity to enable access to online resources, and the trend towards shared services (like Office 365 in the cloud) the population of users who are being tracked in the Identity and access management system is increasing. More categories of user types are being incorporated into the identity registry. This is due to the demand by campus service providers as well as other enterprise systems (like SIS) being interested in allowing online access to their users.
3. Discussion turned to “who should get an HUID” and whether the community is still equating having an HUID with more stature within the community. There are a handful of systems that are doing that, but in general, there is wider understanding that a HUID is just a business identifier.
4. SIS would like to have HUIDS for all the people they are tracking in their system in order to have consistency with their data model. However, they do not want to signal an intent to enable these users

to Authenticate.

- a. Some SIS schools are interested in issuing HUIDs to waitlisted students
  - b. Some are interested in issuing HUIDs to all admitted students
5. Kwok spoke of FAS intent to assign HUIDs to employees in Aurora. Isabelle pointed out that if they have the HUID in advance, it will constrain their ability to feed data to PS.
6. Discussion turned to sponsored accounts and their relationship to POIs. The conclusion was that the concepts should be combined into one over time.
- a. Sponsored Account is a good descriptive name for what they are. Even POIs today are "Sponsored"
  - b. The process of requesting a sponsored account should be distributed so that users can kick off the request directly. There was no discussion of the approval requirements, or policy around who should be able to request. (Future Topic)
  - c. Identities should be associated with different role(s).
  - d. Roles can be associated with differing levels of access
  - e. There should be as much focus on how roles are ended (what process, what tools) as there is on how they are created!
  - f. There will need to be a structure within the tool that constrains what type of role holders a particular user can set up. For example, only a select few would set up an overseer. However, a the ability to authorize a sponsored collaborator account (as FAS employs it today) would be widely available.
  - g. Tools need to ensure that sponsors are held accountable for their actions
  - h. PeopleSoft distributes access to employee and unpaid appointee creation, and requires people to sign-off on an affidavit before authorizing use.
  - i. The ramifications for Authorization Proxy need to be considered as this is an extremely important service to the community. New roles imply additional rules and roles need to be incorporated into the Authorization Service offerings. (Isabelle)
  - j. Jennifer pointed out that these changes may require assigning new role types to existing users as part of the migration to new systems.
7. Topics for next meeting:
- a. Roles Matrix
  - b. Role of authorized approval in creation of Sponsored Accounts and POIs

#### Action Items

1. Matrix of role types being considered for review (Jane)
2. Preliminary thinking around requirements for approval policies and rules for who can sponsor for review by the group (Jane)

#### Next Meeting

1. Review matrix of role types for sponsored accounts
2. Discussion around approval policies
3. More on role of self-registered guests

#### Archived Document