Identity & Access Management
Lifecycle Committee

April 13, 2015
Monday
Smith Center 561
Agenda

• Special Guests: Employee IAM Lifecycle
  – Onboarding Workflow
    • Early Entry Into PeopleSoft, I-9 Process
  – Special Challenges
    • Transfers
    • Leaves
    • “Silent” Organization Affiliations
    • Emeritus “Active” and Honorary Emeritus Status
    • POI-to-Employee and Employee-to-POI Transitions

• Recap POI Affiliations
  – Sponsored Affiliations and Sponsored POI Roles
  – POI Role Types
Onboarding and the I-9 Process
Amy G. Esposito & Joanne Jordan
Employee Lifecycle Issues

Amy Esposito / Joanne Jordan / Mary Beth Johnson
Central Payroll / Financial Systems Solutions
Topics Impacting Payroll

- Form I-9 processing *
- Electronic W-2 forms *
- Direct Deposit

* topics for today
Form I-9 Processing
Current Process Concerns

• Forms are completed locally and mailed or dropped off at Central Payroll
  – Delays in processing caused by delivery delays
  – Risk of lost or miss directed mail
  – Requires manual review for compliance

• No current restriction on who can complete I-9 on behalf of the University
  – Forms not completed in a timely manner
  – Forms completed incorrectly putting the University at a compliance risk (Fine up to $1100 per incorrect form)
  – No mechanism to delete forms that are no longer required to be maintained, increasing our risk in the event of an audit
Electronic I-9 Processing

• Benefits
  – Forms are completed online and submitted/stored electronically so can be easily deleted when hold requirement is met
  – Most programs have built in safe guards to ensure compliance
  – No risk of lost mail
  – Access can be limited to select individuals in the University, training could be required for access

• Concerns
  – Would likely require centralization of the I-9 process
  – Vendor concerns – if not PeopleSoft, would we need a feed?
  – If PeopleSoft how would it work- typically HUID needed for self-service, currently HUID created upon hire
Electronic I-9 Processing in PS
Electronic I-9 Processing in PS
Electronic I-9 Processing in PS
Electronic I-9 Processing in PS
Electronic I-9 Processing in PS

To be completed and signed by the employer. Examine one document from List A OR examine one document from List B and one from List C, as listed in the instructions, and record the title, number and expiration date, if any, of the document(s).

To open the Handbook for Employers in a separate browser window, select I-9 Instructions.

List A

Document Title:  
Issuing Authority:  
Document Number:  
Receipt Doc Nbr:  
Doc Exp Date (if any):  
Rec Exp Date (if any):  

Document Title:  
Issuing Authority:  
Document Number:  
Receipt Doc Nbr:  
Doc Exp Date (if any):  
Rec Exp Date (if any):  

Document Title:  
Issuing Authority:  
Document Number:  
Receipt Doc Nbr:  
Doc Exp Date (if any):  
Rec Exp Date (if any):  

List B and List C

Document Title:  
Issuing Authority:  
Document Number:  
Receipt Doc Nbr:  
Doc Exp Date (if any):  
Rec Exp Date (if any):  

Document Title:  
Issuing Authority:  
Document Number:  
Receipt Doc Nbr:  
Doc Exp Date (if any):  
Rec Exp Date (if any):  

Employer Representative Details

Name:  
Title:  
Address:  

I attest under penalty of perjury, that I have examined the document(s) presented by the above-named employee, that the above-listed document(s) appear to be genuine and to relate to the employee named that the employee began employment on (month/day/year) 04/07/1989 and that to the best of my knowledge the employee is authorized to work in the United States. (State employment agencies may omit the date the employee began employment.)
Electronic W-2 Forms
Current Process Concerns

• Paper W-2 forms
  – Cost of postage for mailing approximately 35,000 forms from outside vendor
  – Significant number of forms returned due to incorrect address
  – Specialty paper/envelopes required to create mail/reprints
  – Large number of reprint requests require significant resources to process from February to April

• Electronic through PeopleSoft
  – Currently only available to active employees
  – Form does not look like the printed version we send, employees reluctant to accept
Electronic W-2s

• Benefits
  – Forms are available electronically, likely earlier than printed copies would arrive
  – No risk of lost mail
  – No postage costs
  – Limited manual reprints required

• Concerns
  – Employees need to opt in to received form electronically rather than hard copy (can this be part of on-boarding?)
  – Currently terminated employees can’t access PeopleSoft
  – If outside Vendor – can we do a single sign on so that HUID/Pin would work
1. Dr. Pat Patricks accepts an offer for an assistant professorship. Pat’s start date is Sept. 1.

2. Pat’s department admin sponsors an account for Pat — even though it’s only April. This includes details like birthdate, personal email, start/end dates, and affiliation type.

3. An identity for Pat — including a HUID — is created in the Harvard Identity Registry (IdDB).

4. HR sends Pat an email with an invitation to claim a new Harvard account.

5. Pat claims an account using name, date of birth, and the code from the email. Then, Pat chooses a username from a list of options, sets a strong password, and adds a recovery email in case a password reset is ever necessary.

6. Account Management flips Pat’s status in SailPoint IIQ to “Claimed.”

7. Accounts are provisioned for Pat in the appropriate targets for an Incoming Faculty role — in this case, HarvardKey LDAP, University AD, 0365, FAS AD, FAS LDAP, Kerberos, and Google.

8. By August, HR job data for Pat is fully complete in PeopleSoft, and PeopleSoft submits this data to IdDB.

9. A future-effective dated employee role update results in some provisioning to downstream systems.

10. On Sept. 1, when Pat’s Incoming Employee role ends and the Employee role starts, additional attributes are updated in LDAP — Pat’s data have “aged,” and the passage of time automatically results in additional provisioning.

11. Pat comes to campus to start the new appointment! Pat already has access to all the apps and services needed for day-to-day life at Harvard — including the Athletic Office site, where Pat buys a pool sticker for a workout after a great first day on the job.
Employee Lifecycle Topics: Special Challenges

• Transfers
  – Difficult to detect transfers in the HR data at times
  – Automatically cancelling prior departmental access the right move?

• Leaves
  – Related HR changes trigger deprovisioning of email, etc., because person appears to have lost departmental affiliation

• “Silent” organization affiliations
  – Individual’s HR data may say OPR, but the job is at HMS

• Emeritus ‘Active’ and Honorary Emeritus status
  – Library access often desired, but licensing and other issues

• POI-to-employee and employee-to-POI transitions
  – Although individual stays on the same HUID, there can be differences in what people are automatically eligible for
Person-of-Interest (POI) Affiliation

The POI category includes all affiliations which are not classified as student, faculty, staff, library borrower or alumni.

- Has the most variation of uses
- Potential for misunderstanding and misuse
- Important to understand the reason, know the person, and control their access
- Most POIs require a sponsor
- Implemented and managed through HUIT’s MIDAS system
Sponsored Affiliations = Sponsored POI Roles

Sponsored affiliations allow Harvard faculty and staff to give individuals outside of their School or organization — or outside of Harvard itself — temporary access to resources.

• Sponsored affiliations are implemented via POI roles that require a Harvard sponsor ("sponsored POI roles")
• Sponsors may be held accountable for how resources are used
• Sponsors may delegate administration of the sponsorship to a Sponsor Admin
• Sponsored POI roles must be renewed on a periodic basis
• If the person being sponsored doesn’t already exist in the identity registry, the system will create an identity record for them — this requires a minimum of first name, last name, and date of birth
Roles are the means within the HUIT identity registry of defining an individual’s affiliation(s) with Harvard.

- Included as part of a person’s HarvardKey
- A person may have multiple roles (e.g. student and employee)
- Role types are generic (e.g. student), but a person’s instance of a particular role also relates to a specific School or organization (e.g. FAS Student)
- Roles control access to a School or organization’s resources
## POI Role Types

<table>
<thead>
<tr>
<th>Current</th>
<th>Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sponsored Affiliations</strong></td>
<td><strong>Sponsored Affiliations</strong></td>
</tr>
<tr>
<td>• Consultant</td>
<td>• Incoming Employee/Transfer</td>
</tr>
<tr>
<td>• Contractor</td>
<td>• Collaborator</td>
</tr>
<tr>
<td>• Vendor</td>
<td>• Inter-school Affiliated</td>
</tr>
<tr>
<td>• Security</td>
<td>• Short-Term Visitor or Guest</td>
</tr>
<tr>
<td>• Family Member</td>
<td>• Volunteer</td>
</tr>
<tr>
<td>• Tenant</td>
<td>• Hospital Employee</td>
</tr>
<tr>
<td>• Smithsonian Employee</td>
<td>• Field Education Supervisor</td>
</tr>
<tr>
<td>• Harvard Management Co. Employee</td>
<td>• Academic Advisor</td>
</tr>
<tr>
<td>• Other</td>
<td></td>
</tr>
<tr>
<td><strong>Non-sponsored Affiliations</strong></td>
<td></td>
</tr>
<tr>
<td>• Overseer</td>
<td></td>
</tr>
<tr>
<td>• Retiree</td>
<td></td>
</tr>
<tr>
<td>• Spouse of Deceased Retiree</td>
<td></td>
</tr>
<tr>
<td>• Retired Hospital Affiliate</td>
<td></td>
</tr>
<tr>
<td>• Spouse of Deceased Hospital Affiliate</td>
<td></td>
</tr>
</tbody>
</table>
Any questions?
Thank you!
## Vocabulary Quiz

Do you know the difference between the key terms below?

<table>
<thead>
<tr>
<th>Term</th>
<th>How Used</th>
<th>Examples</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Login name            | Used as the login ID Expected to be the Harvard email address, can be another for Alumni or sponsored accounts | Email-eligible user: jay_hill@sph.harvard.edu  
Sponsored collaborator: jayhill@stanford.edu  
Alumnus/alumna: coolguyjay@comcast.net | When a user logs in using HarvardKey, the system will expect the user to enter this login name and its related password |
| User ID               | System-assigned identifier                                               | Sam Account: ADID = jeh454  
UNIX LDAP: UID = jeh454                                                   | Permanently assigned value enables prestaging                                                                                      |
| Harvard email address | Harvard-assigned email                                                    | username@optionalsubdomain.harvard.edu                                   | Users chooses value on left of @ sign as part of self-service account claim & onboarding process                                  |
| FAS name              | Legacy username for FAS person                                            | jayhill                                                                  | Former names will exist as mapped attributes                                                                                     |
| Google name           | Google username                                                          | jayhill@g.harvard.edu (always scoped)                                    | Since Google accounts can’t be changed without content loss, some will keep accessing via old names                             |
| {School} name         | Local username(s)                                                       | [we want to accomodate values when necessary]                             | Local usernames are mapped to identity as additional attributes                                                                 |

25