HARVARD UNIVERSITY
Information Technology

Identity and Access Management

Technical Oversight Committee

July 31, 2014 | Thursday | 3-4 P.M. | 6 Story Street, Ground Floor

Agenda

- Meeting Purpose and Intended Outcome
- Approval of Previous Minutes
- Chair’s Report
- Shared Topics of Interest: SailPoint IIQ Technical Overview
- Shared Topics of Interest: Revised IAM Password Policy
- Survey Results: Technical Oversight Committee Meeting Topics
- General Discussion

Meeting Purpose and Intended Outcome

Purpose

- Present latest status of program plan adjustments resulting from changes to the Collaboration Program/Office 365 and revised SailPoint foundation release date
- Present and discuss a technical overview of SailPoint IIQ
- Present changes to IAM password policy

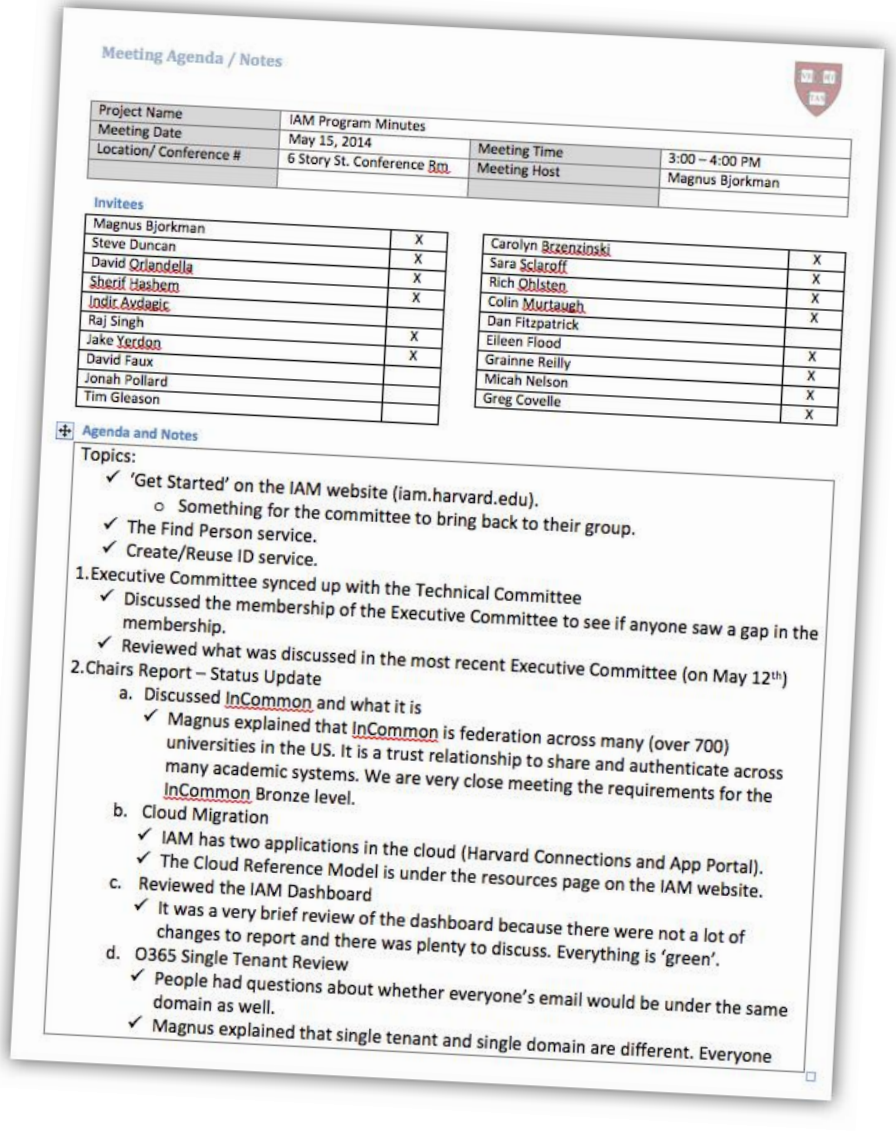
Intended Outcome

- An understanding of SailPoint IIQ to bring back to your organizations
- Familiarity with changes to IAM password policy

Approval of Previous Minutes

May 15 Meeting

- Status updates: InCommon, cloud migration, dashboard review, O365 single-tenant review
- “Get Started” section on IAM site
- Find Person and Create/Manage ID
- Team priorities shifted toward accelerated provisioning
- **Action Item:** App portal is available and deployed internally; need to implement additional security and audit requirements before piloting
- **Action Item:** Committee materials distributed prior to meetings



Meeting Agenda / Notes

Project Name	IAM Program Minutes		
Meeting Date	May 15, 2014	Meeting Time	3:00 – 4:00 PM
Location/ Conference #	6 Story St. Conference Rm	Meeting Host	Magnus Bjorkman

Invitees

Magnus Bjorkman	X	Carolyn Brzenzinski	X
Steve Duncan	X	Sara Sclaroff	X
David Orlandella	X	Rich Ohlsten	X
Sherif Hashem	X	Colin Murtaugh	X
Indir Avdagic		Dan Fitzpatrick	
Raj Singh	X	Eileen Flood	X
Jake Yerdon	X	Grainne Reilly	X
David Faux		Micah Nelson	X
Jonah Pollard		Greg Covelle	X
Tim Gleason			

Agenda and Notes

Topics:

- ✓ ‘Get Started’ on the IAM website (iam.harvard.edu).
  - Something for the committee to bring back to their group.
- ✓ The Find Person service.
- ✓ Create/Reuse ID service.

1. Executive Committee synced up with the Technical Committee
   - ✓ Discussed the membership of the Executive Committee to see if anyone saw a gap in the membership.
   - ✓ Reviewed what was discussed in the most recent Executive Committee (on May 12th)
2. Chairs Report – Status Update
   a. Discussed InCommon and what it is
      - ✓ Magnus explained that InCommon is federation across many (over 700) universities in the US. It is a trust relationship to share and authenticate across many academic systems. We are very close meeting the requirements for the InCommon Bronze level.

   b. Cloud Migration
      - ✓ IAM has two applications in the cloud (Harvard Connections and App Portal).
      - ✓ The Cloud Reference Model is under the resources page on the IAM website.

   c. Reviewed the IAM Dashboard
      - ✓ It was a very brief review of the dashboard because there were not a lot of changes to report and there was plenty to discuss. Everything is ‘green’.

   d. O365 Single Tenant Review
      - ✓ People had questions about whether everyone’s email would be under the same domain as well.
      - ✓ Magnus explained that single tenant and single domain are different. Everyone

Chair's Report: Change in Focus to the Collaboration Program

In order to meet revised requirements, the three IAM teams will prioritize development efforts for the Provisioning and Directory Services projects until December 2015. Overall schedule impact slides can be found in Appendix B.

Benefits

- SailPoint IIQ to allow for automated provisioning/deprovisioning across the University for ~35,000 users
- Future IAM releases will be less complex due to centralized user population, and will allow for improved user experience for IAM services and HUIT shared services
- New onboarding and account management features will be delivered earlier in the schedule
- The ability for users to find contact and calendar (free/busy) information across participating Harvard schools will be advanced by six months

Impact

- Cloud Migration project work will continue in order to realize projected infrastructure savings
- Decommissioning of PIN3 will be advanced in order to realize projected infrastructure savings
- SSN Truncation project work will continue in order to mitigate unnecessary security exposure
- Project work to support SIS and Alumni releases will continue
- Delays to most release work in all other projects due to resource constraints and new priorities

Chair's Report: July Executive Meeting Notes

The SailPoint IIQ foundation release has been postponed to August 16.

The Cause

- A race condition is created by IdDB changes processed into IIQ while changes are being made in FAS and University AD
- This condition was found late in integration testing

The Solution

- Communicate the need to migrate direct access to a SailPoint IIQ-managed approach to impacted AD system administrators
- Design and develop additional interfaces for direct and batch updates into University AD
- Work in collaboration with Unified Communications to update O365 processes and scripts
- Define and execute coordinated test cases
- Prepare support documentation and train the University AD community and HUIT Help Desk staff
- Reschedule production go-live through change management process

Chair's Report: July Executive Meeting Notes

Although minor delays will take place as a result of delaying the provisioning release, larger overall timelines will not be affected.

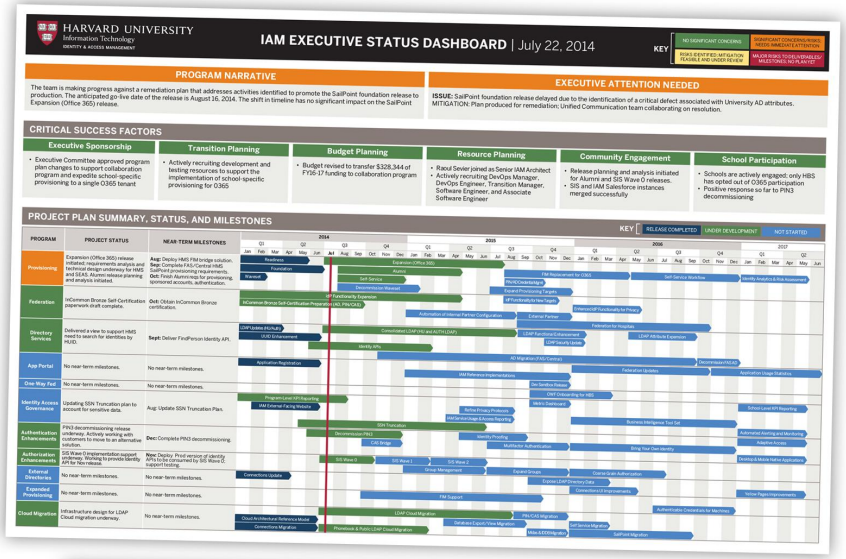
Project	Release	Description	Impact	Plan Date	New Date
Directory Services	Identity APIs	QA Resource contention	Delay to Find Person service deployment	August 2014	September 2014

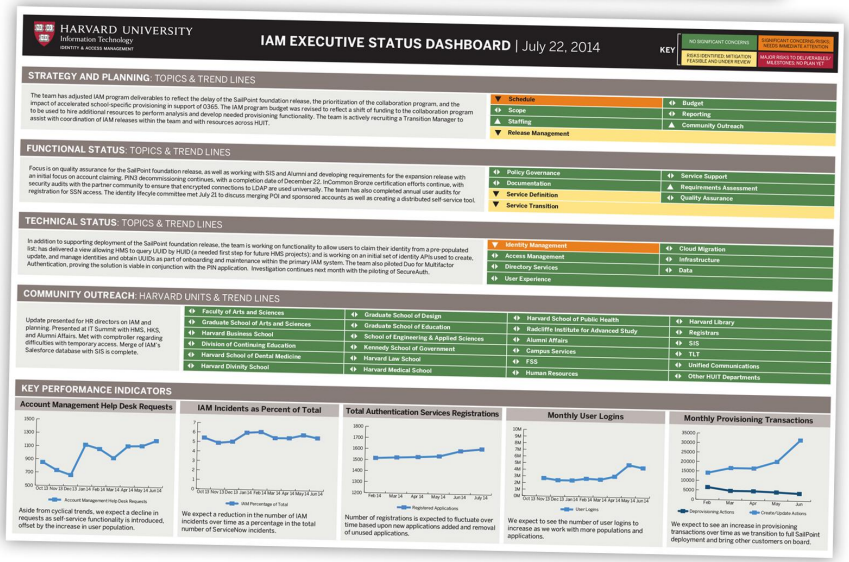
Chair's Report: Program Status

Download the latest executive status dashboard at iam.harvard.edu/resources

Current Program Status:

- The team is making progress against a remediation plan that includes additional functionality intended to replace the need to edit user accounts via AD
- Anticipated go-live date of the foundation release is August 16
- Timeline shift has no significant impact on the SailPoint expansion (Office 365) release





Shared Topics of Interest: SailPoint IIQ Technical Overview

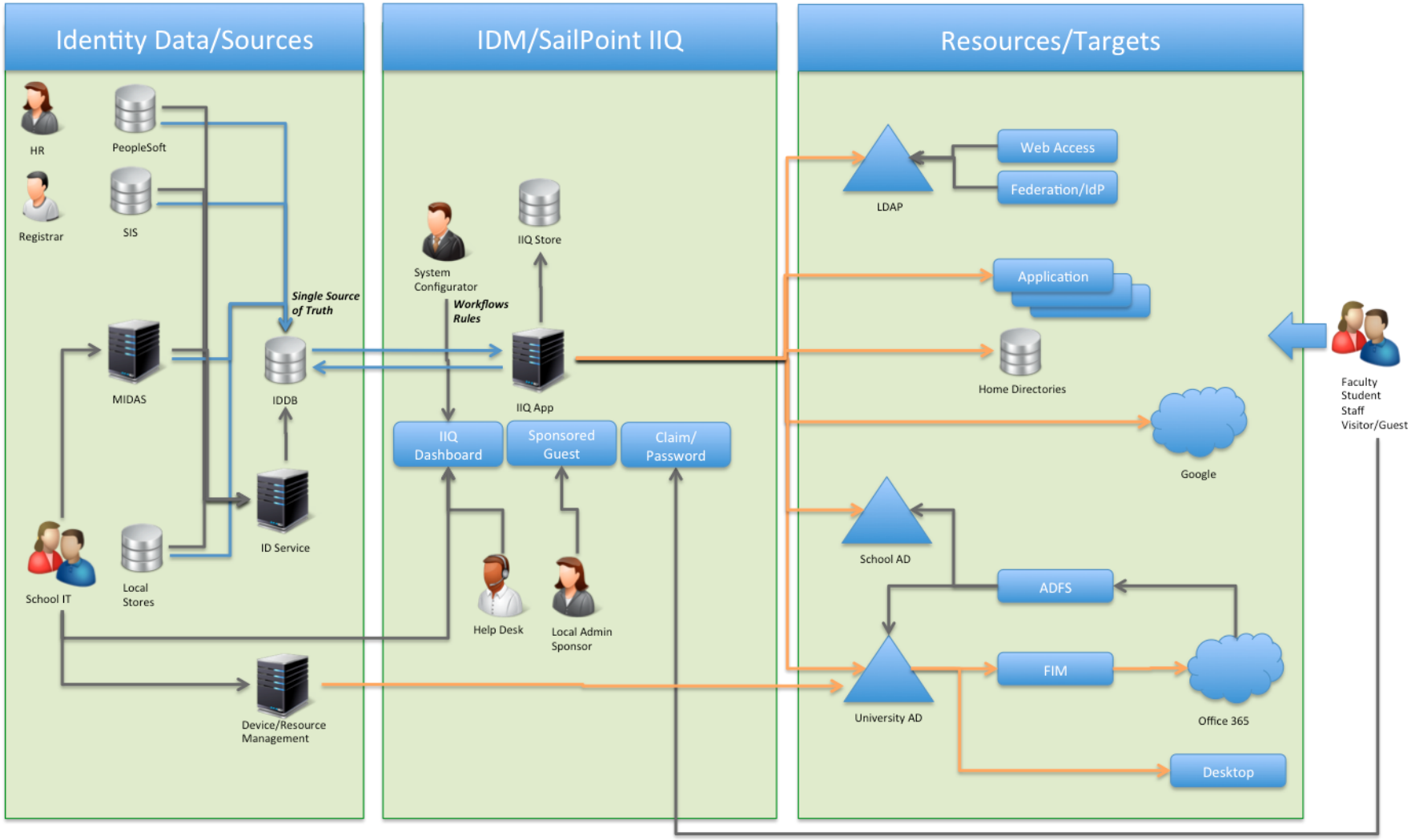
- What is SailPoint IIQ?
- Workflow
- SailPoint IIQ Overview and Demo
- Upcoming Releases
- Future Functionality

SailPoint IIQ Technical Overview: What is SailPoint?

- SailPoint IdentityIQ (IIQ) is a fully functional Identity Management System
- Information is gathered across all connected applications to create an Identity Cube, which includes all attributes related to all the connected applications
- Business logic can be defined programmatically via BeanShell
- SailPoint IIQ itself is a .war file that can be deployed into a Tomcat server
- Development of rules or custom connectors can be done in IntelliJ/netbeans/Eclipse IDEs
- RESTful APIs exist to integrate custom applications with IIQ — one example is our new Claim Account application
- Online resources for learning more:
  - IIQ Support community portal with good training materials and programmer resources
  - IdentityIQ product overview and brochure

SailPoint IIQ Technical Overview: What is SailPoint?

SailPoint IIQ Technical Overview: Workflow



SailPoint IIQ Technical Overview: Overview and Demo

Let’s see firsthand how it works.

SailPoint IIQ Technical Overview: Upcoming Releases

Foundation

- Identity Cubes created from data in IDDB
- Configured applications (endpoints) aggregated and correlated to Identity Cubes
- Assignation of role based on certain attributes triggers provisioning to University AD
- Changes to selected attributes in University AD via batch or web interface within IIQ

Near-Term

- Claiming application written in Java/Spring environment communicates to IIQ via RESTful interface
- Provisioning to additional connectors through IIQ:
  - Google Apps (University/College)
  - School-specific Active Directories/LDAP
  - FAS:
    - HomeDIR (Home Directories)
    - Kerberos (Unix password management)
    - FAS LDAP
    - FAS AD
    - FASMAIL
- Provisioning/updates to these applications governed by birthright roles

SailPoint IIQ Technical Overview: Future Functionality

- Replacement of FIM with IIQ for provisioning of Office 365
- Configuration of identities and management of access to additional shared applications such as Jira or Salesforce
- General availability of IIQ GUI (end-user access)
  - Example: Manage Access windows, where people can request access to applications and app managers can review and accept/deny requests
- Access governance available via reports and analysis based on others in a particular group
  - Example: When a staff member changes roles, locations, or departments, access rights can be adjusted based on comparisons with others and/or general group rights

Shared Topics of Interest: Revised IAM Password Policy

Harvard IT Security Policy includes provisions on acceptable default password policies. The policy remains under review and has not yet been ratified. The unpublished draft includes three possible approaches:

- 8 characters with annual expiration
- 10 characters with no expiration
- Multi-factor

There are additional points that need to be considered with each approach.

As we plan deployment and updates to HUIT services, selecting the most appropriate password policy is an important consideration. Pending the outcome and final publication, IAM will be utilizing a 10-character password without expiration.

Revised IAM Password Policy: AD Example

Setting	Value
Password Length	10
Password Complexity Requirements	Windows complexity
Force Password Change Frequency	None
Minimum Password Age	0 days
Lockout on Failed Login Attempts	Yes
Lockout on Number of Attempts During Period	20 attempts in 10 minutes
Lockout Duration	30 minutes
Number of Previous Passwords Remembered	5
Store Passwords Using Reversible Encryption	Disabled

Survey Results: Technical Oversight Committee Meeting Topics

"My stuff is so dependent upon IAM, I want to know all about it. And the technology you are using is stuff I want to know about too."

Key topic areas:

- Migration to the cloud; cloud topics in general
- SailPoint/Provisioning (Discussed in this session)
- Find Person API/identity creation and related authentication
- Overall IAM service offerings

Please continue to send us your requests for meeting topics!

General Discussion

Appendix A

Technical Oversight Committee Members

Technical Oversight Committee Members

Chair: Magnus Bjorkman, Director of IAM Engineering

Name	School/Group
Steve Duncan	Harvard Kennedy School
Tyson Kamikawa	Harvard Medical School
Sherif Hashem	Harvard Law School
Indir Avdagic	SEAS
Ken Ho	GSE
Jake Yerdon	HSPH
David Faux	HUIT Admin Tech/FAS & College
Jonah Pollard	Unified Communication/Cloud
Tim Gleason	HUIT IAM/AD

Name	School/Group
Carolyn Brzezinski	SIS
Sara Sclaroff	HUIT Admin Tech/HR
Rich Ohlsten	HUIT Admin Tech/Alumni
Colin Murtaugh	HUIT Academic
Dan Fitzpatrick	Partners
Eileen Flood	Campus Services
Randy Stern	Library IT
Micah Nelson	HUIT Security

Appendix B

Program Plan Schedule Impact

Program Plan Schedule Impact: Provisioning

Adjustments to the Provisioning project enable the IAM program to implement accelerated user management and provisioning across Schools.

Project	Release	Description	Plan Date	New Date	Impact
Provisioning	Decommission Waveset	Decommission product and supporting infrastructure.	November 2014	January 2015	No end user impact. Support end-of –life product for additional time.
Provisioning	HUIT Expansion Role Transition Expanded Provisioning	Combine and rename release “Expansion (Office 365)” and track 0365 milestones within this updated release.	December 2016	August 2015	Delivery date for functionality significantly improved. Scope of prior releases still achievable, including updates for POI.
Provisioning	PIN/AD Credentials Management	Give end users the ability to use Active Directory credentials for any PIN-protected system or application they are permitted to access.	August 2015	November 2015	Delay new functionality.

Program Plan Schedule Impact: Federation

Adjustments to the Federation project reflect a reduced need for federation resulting from the move to a single Office 365 tenant.

Project	Release	Description	Plan Date	New Date	Impact
Federation	idP Functionality Expansion	Incorporate additional attributes and profiles into Identity Provider in order for partners to gain access to expanded services and resources.	November 2014	May 2015	Low volume of demand. Partners continue customization of their applications to use legacy protocols.
Federation	Automation of Internal Partner Configuration	Enable self-service for school application teams to onboard with new service providers.	July 2015	September 2015	Low volume of demand. Continue time-consuming manual setup process for new service providers.
Federation	Federation for Hospitals	Allow hospital credentials to be used to access University resources.	June 2016	November 2016	Use cases and ongoing discussions with HMS will continue. Pilot with Partners targeted as an interim step.

Program Plan Schedule Impact: Directory Services/External Directories

Adjustments to the Directory Services and External Directories projects reflect delays to LDAP consolidation and enhancement, with no impact to end users resulting from the prioritization of accelerated provisioning.

Project	Release	Description	Plan Date	New Date	Impact
Directory Services	Consolidated LDAP	Collapse HU and Auth LDAP attributes in the cloud	February 2015	May 2015	No impact to new or existing users. Delay improvements for new application set-up and integration.
Directory Services	LDAP Functional Enhancement	Expand attributes to provide clearer role and affiliation information, and incorporate standard attributes to support federation	July 2015	October 2015	Delay new functionality.
Directory Services	LDAP Security Update	Apply security best practices in line with InCommon and industry.	July 2015	October 2015	Continue with current security risk profile.
Directory Services	Identity APIs	Create utility and additional APIs to enable identity administration for UUIDs to support expanded school provisioning.	**New**	November 2015	New release required to support accelerated provisioning.
External Directories	Expose LDAP Directory Data	Expose enhanced LDAP directory data through alternative protocols to fit application needs (e.g., SAML, CAS, AD)	September 2015	April 2016	Delay new functionality.

Program Plan Schedule Impact: App Portal

The App Portal project is a discrete track providing new functionality to University application owners who wish to more efficiently integrate with IAM. Delivering the new functionality needed to support accelerated provisioning will incur a delay.

Project	Release	Description	Plan Date	New Date	Impact
App Portal	Application Registration	Enable application owners to register their applications with IAM	July 2014	**Complete**	Internal release delivered. Application teams to continue consultation with the IAM team for registration.
App Portal	IAM Reference Implementation	Expand the App Portal to include examples of reference implementations of pre-developed code	February 2015	January 2016	Delay new functionality. Continue consulting with the IAM team for set-up and integration needs.
App Portal	Developer Sandbox Release	Provide a 'turnkey' environment for partners to perform testing their applications with IAM services.	July 2015	January 2016	Delay new functionality Continue with existing testing approaches.
App Portal	Federation Updates	Provide self-service tools for applications to participate in federations and roll out of new features.	June 2016	June 2016	Delay new functionality. Implement manual workarounds, where possible.

Program Plan Schedule Impact: One-Way Federation

The need for One-Way Federation is greatly reduced due to the decision to move to a single Office 365 tenant.

Project	Release	Description	Plan Date	New Date	Impact
One-Way Federation	OWF Onboarding	Expand school targets for OWF	February 2015	**Remove**	Bridging strategy of OWF is no longer required due to accelerated provisioning. If need exists for HBS, new release will be created under Federation Project.
One-Way Federation	Credential Mapping	Incorporate additional users from schools and departments into the identity store with local user credentials.	November 2014	**Remove**	Identity API release within the Directory Service project will deliver this capability.
One Way Federation	OWF Onboarding for HBS	Proposed release for HBS OWF integration with IAM.	**New**	April 2016	HBS-specific OWF work tentatively planned.