Pre-Function Lobby

Drop in to demo OneUSG Connect during breaks Wednesday & Thursday
Introduction of Panel
Auto-Provision Process/Dynamic Security Roles
Single Sign On
Row level Security/Time and Labor Security
Terminated/Retiree Access
Workflow Administration
Delegation
Object Security/Types of Query Access
PII Data
Pain Points for Cohort 1 and Lessons Learned
What's Coming Next
Q&A
Auto-Provisioning/Dynamic Security Roles

- User Ids Auto Generated Upon New Hire
- Base Security Roles are Automatically Assigned by the System
- Dynamic Roles are Also Removed Once they no longer meet the criteria
- Only Practitioner Access has to Be Manually Added and Removed upon Termination
Single Sign-On

- Required for current employee access to OneUSG Connect
- Traditional Credential Management not in HCM.
- Uses Institution’s Local Directory to pass the following attributes: Last Name, Emplid, Company
OneUSG Connect uses row level security to control data access by Institution.

After an employee is hired into a Job or has a Job change, Time and Labor Security needs to be set up.

Time Approvers have to be assigned to allow for time/absence request approvals.

T&L Security is primarily concerned with ensuring the correct access of reportees to managers as well as controlling the dates which are open to any employee to report time.
• Security roles automatically updated upon Termination or Retirement
• Allows base access to Pay checks, W2s, etc.
• Practitioner Access is removed by a batch process (Cohort 2)
• Monitors Workflow Transactions for issues such as: Escalations, No approvers found, reassignments...
• Work with security administrators and managers to ensure issues are corrected and transactions are rerouted correctly
• General understanding of approval process at the respective institution
Delegation

- Delegation – Authorizing approval of pending transactions by another person
- Authorized for a specific or indefinite period of time
- Request will be entered in FLUID by the Approver, using Delegation Tile
- Delegation requests will be routed via Workflow to the “delegate” for acceptance
- Delegation will take effect when accepted by the delegate
• OneUSG Connect has delivered hundreds of public queries for institutional use.
• Queries are protected via Object Security to ensure they are not overwritten.
• Query Access at the institution level should be restricted to Query Viewer unless end user has been through training.
• Query Private access allows an end user to create private queries that they can share with other users by copying them to their individual user ids.
• Query Public will be limited to one or two super users at each institution for audit purposes. These individuals will have completed query training.
– Sensitive (PII) Access is controlled by a Security Role and should be limited to a few select Practitioners

• Access

<table>
<thead>
<tr>
<th>Bank</th>
<th>1234561234</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN</td>
<td>123-45-5617</td>
</tr>
</tbody>
</table>

• No Access

<table>
<thead>
<tr>
<th>Bank</th>
<th>******1234</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSN</td>
<td>*****5617</td>
</tr>
</tbody>
</table>
Cohort 1 Pain Points and Lessons Learned

- Single Sign On Issues – Last Name not matching / Name changes
- Time and Labor Security Questions
• Over 16 new MSS transactions with workflow options
• Email Approval for Workflow
• Self Service Delegation
Questions/Answers
All presentations will be placed on:
- OneUSG Project website: usg.edu/oneusg
- Georgia Summit website: usg.edu/georgia_summit
- Smartsheet

Our subscribers will receive an email with presentation links and follow-up information.
- Subscribe to OneUSG Connect emails at usg.edu/contact_us