



Security Workshop

by

Brian Davis, Jordan Morgan, &
Mike Taliaferro

October 11, 2006

9am – 12noon

Agenda

- Introduction
- User Types: Self-Service vs. Functional
- Restrict Access using Portal Technology
- Self-Registration
- BOR Security Model
- Support Level & User Maintenance
- Manual Cutover Tasks
- Important Notes
- Departmental Security
- Q&A
- Self-Registration Demo

User Types

■ Functional

- Current users (HR, Benefits, Payroll, Budget, etc.)
- Created by local campus security administrator
- Access PS application via PeachNet only
- Access to the EMPLOYEE portal

■ Self-Service

- New users plus the current users
- Created via self-registration process by employees themselves
- Access PS application via Internet and PeachNet
- Access to the HREAPPS portal

■ Employee Type

- All user profiles must have an ID type of Employee and be assigned an employee ID

Restrict Access using Portals

■ What is portal?

- HRMS Portal Pack technology provides a method by which USG can specify the type and nature of HRMS content available to the Functional and Self-Service users, and the visual and process flow attributes and characteristics common to the collection of content.
- In short, portal is like a folder with a distinct set of content
- Distinguished by different URLs

Restrict Access using Portals

- *continued*

■ Portals for HRMS

□ EMPLOYEE (Default)

- Contain pages and programs currently used by functional users like HR, Benefits, Payroll, and Budget to perform business tasks
- Does not contain self-service functionalities used by employees
- MUST be accessed via PeachNet
- URL provided to functional users directly

□ HREAPPS

- Contain only the self-service functionalities used by general employees
- Existing functional users already have access to the self-service
- Can be access via both the Internet and PeachNet
- URL is not provided to employees. Users need to access the HREAPPS portal via campus PeachNet website

Self-Registration

■ Benefits

- User profiles (userids) only exist for active users. This eliminates unused user profiles as a security exposure.
- User profiles (userids) are granted access to one, and only one, employee account. No user profile is granted access to multiple employee accounts.
- User profiles (userids) are created and maintained by the user. This relieves the institutional security administrator from having to create user profiles or maintain user profiles on an ongoing basis. Local security administrators still retain administrative authority for all user profiles created through the Self Registration process and those created manually.

BOR Security Model

■ New Permission Lists

□ BORDP99 (Data Permission List)

- Data permission list assigned to the new user profiles created via self-registration

□ BORPP99 (Primary Permission List)

- Primary permission list assigned to the new profiles created via self-registration

□ BORPRC99 (Process Monitor Permission List)

- Process monitor permission list assigned to the new profiles created via self-registration

BOR Security Model - *continued*

- New Permission Lists

- BORHSS20 (Self-Service)

- Assigned to the existing BOR PeopleSoft User role
 - This is the permission list that contains self-service functionalities

- BORWFPE20 (Personnel Worklist)

- Assigned to the new Personnel Administrator role

- BORWFPY20 (Payroll Worklist)

- Assigned to the new Payroll Administrator role

BOR Security Model - *continued*

■ New User Roles

- Personnel Administrator (PS delivered with BOR modifications)
 - Assigned to any user responsible for administering the personnel worklist items (Name Change & Marital Status Change)
- Payroll Administrator (PS delivered with BOR modifications)
 - Assigned to any user responsible for monitoring the W-2 Reissue requests

BOR Security Model - *continued*

- Existing User Role

- BOR PeopleSoft User

- Addition of the new permission list BORHSS20
 - **MUST** be assigned to every user (functional and self-service)

BOR Security Model - *continued*

- Stronger Password Control
 - 8 characters minimum
 - Must contain at least 2 digits
 - Expire every 180 days
 - 5 maximum logon attempts

Support Level & User Maintenance

■ Local Security Administrator

- Functional users and Self-Service users
- Areas/Issues supported:
 - Unlock user profile
 - Unable to create account via self-registration
 - Administer campus security assignment
 - Implement Departmental Security

■ OIIT Production Support

- Local Security Administrator and functional users
- Areas/Issues supported:
 - Unlock user profile
 - Assist with security assignments
 - Troubleshoot worklist problems
 - Maintain the BOR Security Model

Manual Cutover Tasks

for both UAT and Production

- For each existing user profiles (Production)
 - Required to change user type from None to Employee
 - Required to populate the user's EmplID for each existing user profile
 - Preferably populate the Email address with user's email address
- Identify users who will be monitoring worklist items (HR and Payroll users)
 - Assign Personnel Administrator and Payroll Administrator to appropriate users
 - Identify the user who will monitor the worklist items that are undeliverable and assign that user to the System Default User
 - Path: PeopleTools > Workflow > Defaults & Messages > Set Workflow Defaults
- Make sure all existing users set up secret questions and answers; otherwise, they will not be able to reset their passwords via self-registration. However, they can still request new password be emailed to them.

Important Notes

- In order to access full worklist functionalities, a user MUST have access to either the Personnel Administrator or Payroll Administrator roles.
- In order to access all functionalities available from the worklist, a user MUST also have either BOR HR Manager or BOR HR Administrator role.
- Either Personnel Administrator or Payroll Administrator role will give user access to the Worklist Reports

Departmental Security

- **NOT** required for Self-Service Phase I
- Methods of Implementation:
 - Department Table
 - Department Security Tree

Departmental Security - *continued*

■ Department Table

- Manager ID in the DEPT_TBL table must be populated

■ Pros

- Standard data-entry to set up
- Tree management is minimal (departmental changes only)

■ Cons

- Provide single-level access only
- Requires additional data entry for permission list

Departmental Security - *continued*

- Department Security Tree
 - Manager ID in the DEPT_TBL table must be populated
 - Currently department security tree is “flat”
- Pros
 - Provides hierarchical reporting
 - Requires less entry on setting up permission lists
- Cons
 - Takes more effort and planning to implement

Departmental Security - *continued*

■ Position Management

- Reports-To field in POSITION_DATA table must be populated

■ Pros

- It is already set up for some campuses
- Can work in conjunction with department security tree if the Reports-To field is not populated

■ Cons

- Provide single-level access only.

Q&A

- Any questions?
- Hands-on demo
 - Self-Registration
 - Upgrade access: Employee who has a user profile created via self-registration now became a functional user
 - Downgrade access: Functional user became an employee only user