Welcome to Wide Area Workflow e-Business Suite.
This demonstration contains audio narrative. Please adjust your volume accordingly.

Step 1

This is an overview of Administration changes.
Step 2

Logon to WAWF e-Business Suite.

Step 3

Open the WAWF e-Business Suite Administration Console from the Administration menu drop-down.
**Step 4**

Click the User / Role Management link from the menu option.

**Step 5**

If the administrator needs to manage a particular user, the “Search by User” option may be utilized. This option allows the administrator to search for a user based on User ID, First Name, Last Name, E-mail, DoD ID, and/or X509 Subject Name. Partial searches are permitted.

Note: For Government Administrators, only users in the Government Administrators span of control will be returned.
Step 6

The Search Results page will display a list of users that were returned from the search. This page will also allow an administrator to quickly see which application the user has roles for. To manage a specific user, click the User Id link for that user.

Step 7

The User Details page will be displayed with information specific to the user. The following menu options will be available:

- Overview
- Profile
- Justification / Attachments
- Supervisor or Sponsor
- Agency or Company
- Reset Certificate or Password
- GAM/CAM Letter (for GAM/CAM users only)
- User Roles
- Role History
- Profile History

PIEE Super Administrators will have an additional option to Delete users that have never gained access to the suite.
Step 8

The Overview page will display the user's active, pending admin approval, and pending supervisor/sponsor approval roles. The user can view the roles' comments and attachments and any other additional role information, as well.

Step 9

When the Profile link is clicked, the User Profile data will be displayed. The Administrator will have the option to edit the profile, unless the profile was populated from DMDC. The PEE Administrator and PEE Super Administrator may also Block or Unblock the user at the profile level.
Step 10

When the Supervisor or Sponsor link is clicked, the Supervisor/Sponsor Information for the user will be displayed. The Administrator will have the option to edit this data.

Step 11

When the Agency or Company link is clicked, the Agency/Company Information for the user will be displayed.
**Step 12**

When the Justification/Attachments link is clicked, the Justification/Attachments for the user profile will be displayed. The Administrator will have the capability to attach or add additional comments to the user’s profile.

**Step 13**

When the Reset Password or Reset Certificate link is clicked, the information for the user's profile will be displayed. The Administrator will be required to enter comments for any non-vendor users to reset their password/certificate and the security questions will be displayed for password users.
Step 14

When the User Roles link is clicked, all roles for this user will be displayed.

A series of radio buttons will allow the administrator to filter the rows based on status.

An indicator will show if a role is part of a job series. Clicking Edit Contract will present a screen to edit contract instrument details.

Step 15

Enter new contract expiration date and click the Save button.
Step 16

A Success message is displayed letting the User know the Contract information has been updated successfully.

Step 17

1. The Administrator may change a role status by selecting a value from the Actions dropdown for that role. Values in the dropdown are as follows:
   - Activate
   - Deactivate
   - Archive
   - Reject
   - Block
   - Unblock

   Business logic will determine the action that can be taken on each role.
Step 18

2. Roles that are part of a job series must all be set to the same activation status. 3. A “Change All” dropdown will allow the administrator to set all of the dropdowns to the same value if all the roles are in the same status. 4. Click the Update button to submit the activation changes.

Step 19

After the administrator clicks the Update button, a Confirmation page will be displayed. Only the roles being changed will be displayed.
Justifications will be required when changing a role status. For the following roles, when it is the first time the role is being activated, a Government Administrator is required to confirm the user is a Government Employee: Acceptor, Cost Voucher Approver, Grant Approver, and LPO.
Step 20

When the Role History link is clicked, the role history for all the user’s roles will be displayed.

Step 21

When the Profile History link is clicked, the profile history for the user will be displayed.
When the GAM/CAM Letter link is clicked, the appointment letter for the GAM/CAM is displayed and the role history for the user’s GAM/CAM roles are displayed.

The Search by Role functionality will allow an administrator to take non-user specific actions against roles. This option allows the administrator to search for a user based on User ID, First Name, Last Name, E-mail, DoD ID, Job Series, Location Code, Role, Group Name, Application, Contract Expiration Date, Status, Access Approval Status, and DD577 Status. Partial searches are permitted.

Note: For Government Administrators, only users in the Government Administrators span of control will be returned.
Step 24

The Search by Role Results will contain the roles returned from the search.

Step 25

A "Change All" dropdown will allow the administrator to set all of the dropdowns to the same value depending upon the role status.
The User ID link will take the administrator to the User Details page. From there the administrator can view, add comments, add attachments, and review forms for the user.

If the role is for a Support Contractor and the administrator has authorization to edit contract instrument details such as the expiration date, the Edit Contract link will appear. Clicking Edit Contract will present a screen to edit contract instrument details.
Step 28

Enter new contract expiration date and click the Save button.

Step 29

A Success message is displayed letting the User know the Contract information has been updated successfully.
Step 30

The Administrator may change a role status by selecting a value from the Actions dropdown for that role. Values in the dropdown are as follows: Activate, Deactivate, Archive, Reject, Block, Unblock.

Step 31

Roles that are part of a job series can be activated individually.
Step 32

Click the Update button to submit the activation changes.

Step 33

Open the WAWF e-Business Suite Administration Console from the Administration menu drop-down.
Step 34

Click the Group Management link from the menu option.

Step 35

Group Structures will no longer be application specific.

There are two separate hierarchies:

- Procurement/Finance/Logistics
- Security
Step 36

The Procurement/Finance/Logistics Group Information page is displayed with a list of Level 1 groups.

Enter a group name in the Subgroup Filter text box and click the Filter button.

The majority of administrators will not see the Level 1 groups. The administrator will only see the groups within administrator’s span of control.

Step 37

1 record is returned from the search.

The Level 1 "PROGRAM OVERSIGHT" group will hold the Help Desk administrators and PMO users.
Step 38

Actions on the Group Information page are grouped into categories.

Step 39

While viewing Subgroups, the admin may select 'View Location Codes for Current Group' to see all Location Codes assigned to the current group.
Step 40

While viewing Location Codes, the admin may select 'View Subgroups for Current Group' to switch back to the Subgroups display.

---

Step 41

Group Lookup - Search will be limited by hierarchy - Procurement / Finance / Logistics or Security - instead of application.
Step 42

Awaiting Location Codes functionality will no longer be application specific.

Each hierarchy - 'Procurement / Finance / Logistics' and 'Security' - will have their own awaiting location codes management.

Step 43

Administrators will have the option of searching by Location Code or Group Name. Application is optional.
Level 2 PFL GAMs, will see the following question on the search page - “Are you deactivating Pay Location Codes?” The answer will default to 'No'. When changed to 'Yes', Location Code and Group Name will become optional fields and application will default to 'iRAPT'. If both Location Code and Group Name are left blank, all Pay Location Codes within the agency will be included in the search results.

When no application is selected on the search page, admins will be directed to an intermediate search results screen showing the Activity Name, PFL Group Name (if available), and Security Group Name (if available).

PFL GAMs will not be able to see the ‘Security Group’ column and Security GAMs will not be able to see the ‘PFL Group’ column. Same goes for CAMs.

The ‘View Org. Emails’ link may be selected to view all Org. Email(s) for an individual Location Code across applications.
Step 46

Admins may update individual org. email addresses by selecting the ‘Edit’ link in the Action column or add a new extension with org. emails for a location code via the ‘Add Extension’ button. There will also be an option to update org. emails for multiple records at one time.

(2.) When an application is selected in the dropdown on the search page, the intermediate page with Activity Name and Group Name will be bypassed. This allows an admin to view Org. Emails for a specific location code across applications OR view Org. Emails for location codes restricted to a single application.

Step 47

Application is required and will be defaulted to ‘NCCS’ for Security GAMs that do not have access as a PFL GAM. Same condition applies to CAMs.

The Email Settings default to ‘All Emails’ and may only be updated by a GAM / CAM. Other options include ‘No Emails’ and ‘Negative Emails’.

Use the Cancel button to cancel changes and return to the previous page. Use the Save Changes button to save the new extension with org. emails.
Step 48

Level 2 Service / Agency PFL GAMs will have the option to deactivate Location Codes with Current Status set to ‘Active’.

Use the Back button to return to the search page. Use the Save Changes button to deactivate the selected Pay Location Codes.

Step 49

Select the ‘PKI Exemption’ link under Table Management to add/update exemptions.

Note: Management of the PKI Exemptions is restricted to the WAWF PMO and NCCS PMO.
Step 50

Select NCCS Exemption, if the user is registered for any NCCS roles, they are only exempt if they have an NCCS Exemption.

Step 51

Expiration Date, Justification, and Additional Justification have been added to the PKI Exemption table. Expiration Date cannot be a date in the past. Justification is a dropdown field. Additional Justification is optional and is limited to 2000 characters. Justification dropdown choices:

- Dual Persona
- Foreign Nationals when the CAC certificates issued are not compatible with the WAWF Suite
- Production System Validation accounts assigned to a user with specific application roles assigned to each account
- Federal Agency employees not supported by the ECA/Federal bridge policy
- Temporary technical specific CAC related account issues not to exceed three work days. Approval by GAM is required. Approval from PMO is required.
Select NCCS Exemption, if the user is registered for any NCCS roles, they are only exempt if they have an NCCS Exemption.

End

This concludes our demonstration.