SUM for Special Users
This page intentionally left blank.
Table of Contents

1. Introduction .............................................................................................................. 1

2. WAWF Administrators ............................................................................................... 2
   2.1 PIEE Super Administrator / PIEE Administrator .................................................. 3
   2.2 Government and Contractor Administrators ....................................................... 4
       2.2.1 Procurement Finance Logistics and Security Government Administrator .......... 4
       2.2.2 Procurement Finance Logistics and Security Contractor Administrator .......... 5
   2.3 Functional Auditor .............................................................................................. 6

3. PIEE Administration Categories ........................................................................... 6
   3.1 Group Management ............................................................................................. 6
       3.1.1 Procurement / Finance / Logistics Group Information .................................. 7
       3.1.2 Group Lookup ........................................................................................... 9
       3.1.3 Awaiting Location Codes ......................................................................... 10
       3.1.4 Group History .......................................................................................... 11
   3.2 Location Management ......................................................................................... 12
       3.2.1 Location Information ............................................................................... 12
   3.3 History Management ........................................................................................... 13
   3.4 Table Management ............................................................................................. 13
   3.5 Subject Matter Expert (SME) Management ....................................................... 14
   3.6 User/Role Management ..................................................................................... 14
   3.7 Web Service Administration ............................................................................. 17
   3.8 Additional Administration .................................................................................. 20
   3.9 Additional Administration Console Overview ................................................... 21

4. WAWF Administrator Roles ..................................................................................... 26
   4.1 WAWF System Administrator ........................................................................... 26
   4.2 WAWF PMO ....................................................................................................... 28
   4.3 Group View All .................................................................................................... 29
   4.4 DLA Energy Table Administrator ....................................................................... 30

5. MIPR Administrator Roles ....................................................................................... 31
   5.1 MIPR Administrator ........................................................................................... 31
6. **IUID Administrator Roles** ................................................................. 32
   6.1 IUID Help Administrator ................................................................. 32

7. **CORT Administrator Roles** ........................................................... 33
   7.1 Administrator (DPAP) ................................................................. 33
   7.2 Administrator (Department) ....................................................... 34

8. **NCCS Administrator Roles** ........................................................... 35
   8.1 NCCS Administrator ................................................................. 36
   8.2 NCCS PMO ................................................................................. 37
   8.3 Auditor ....................................................................................... 38
   8.4 Other NCCS Reviewer and View Only Roles ................................ 38

9. **GFP Administrator Role** ............................................................... 44
   9.1 GFP System Administrator .......................................................... 44

10. **CLS Administrator Roles** ............................................................ 46
   10.1 Program Management Office (PMO) ........................................... 46

11. **Solicitation Administrator Roles** .................................................. 47
   11.1 Solicitation Administrator .......................................................... 47

12. **PPML Administrator Roles** ........................................................ 48
   12.1 PPML PMO .............................................................................. 48

13. **PC Administrator Roles** .............................................................. 49
   13.1 GPC DoD PMO ....................................................................... 49
   13.2 GPC HAM ............................................................................. 49
   13.3 GPC Auditor ......................................................................... 50
   13.4 GPC Support View Only .......................................................... 50

14. **SPRS Administrator Roles** .......................................................... 51
   14.1 SPRS HAM ............................................................................ 51

15. **Contract Deficiency Report Administrator Roles** ......................... 52
   15.1 Administration ....................................................................... 52
   15.2 C/S/A Administration .............................................................. 52
   15.3 Location Administration .......................................................... 52

16. **Purpose Code Management (PCM)** ............................................ 53
16.1 DCMA Contract Admin Office (CAO) Manager ..................................................... 53
16.2 Contractor DoDAAC Manager ........................................................................... 54
16.3 Purpose Code Flag Administrator ..................................................................... 55
1. Introduction

The Procurement Integrated Enterprise Environment application requires a varied level of involvement in the administration of the various daily activities; from simply viewing records, providing user assistance in document creation and troubleshooting production problems.

It is beyond the scope of this document to highlight the various business rules that would provide oversight to the various administrative functions and to make Standard Operating Procedures for that administration. However, this document will highlight the various functional capabilities provided for the administration of the system.

Through a series of ECPs a consolidation of Administrator Roles at the PIEE level has occurred. The functions of user and group management and system administration duties have been delegated to PIEE level administrators across PIEE.

<table>
<thead>
<tr>
<th>PIEE Administrative Role</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIEE Super Administrator</td>
<td>Highest level of access</td>
</tr>
<tr>
<td>PIEE Administrator</td>
<td>Subset of the PIEE Super Administrator</td>
</tr>
<tr>
<td>Procurement, Finance and Logistics (PFL) Government Administrator</td>
<td>• Administer the Group Structure (Level 2 restriction)</td>
</tr>
<tr>
<td>Security Government Administrator</td>
<td>• Administer the Location Codes in the Group (Level 2 restriction)</td>
</tr>
<tr>
<td>PFL Contractor Administrator</td>
<td>• Manage Org. Emails and Location Notifications</td>
</tr>
<tr>
<td>Security Contractor Administrator</td>
<td>• User / Role Management in the Group</td>
</tr>
</tbody>
</table>

Most applications added in the PIEE Environment will have Application Level Administrators. They will manage the administrative duties within each specific application. They will not administer the PIEE Users, Roles, or Groups.
2. **WAWF Administrators**

This section reviews the functionalities of each of the administrators in PIEE. The table below is an overview of the level of privileges for each type of administrator.

<table>
<thead>
<tr>
<th>Group Management</th>
<th>Super Administrator</th>
<th>Administrator</th>
<th>Government Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement/Finance/Logistics Group Information</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Security Group Information (NCCS)</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Group Lookup</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Awaiting Location Codes</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Group History</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Location Management</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Location Information</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Notification Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIER</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>eMIPR</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Contract Closeout</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>WAWF</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCCS</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table Management</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>PIER</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eMIPR</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract Closeout</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAWF</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCCS</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage SME</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User/Role Management</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Web Service Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Service Registration</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activation and Information</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Addition Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>History</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SYSUID</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Misc</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Explorer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portal</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
2.1 PIEE Super Administrator / PIEE Administrator

This is the highest-level administrator in PIEE, this administrator has access to all the available function as a PIEE Super Administrator. This is reserved for a select group of personnel due to the accessibility of data and ability to make data changes. Each of the areas of functionality this administrator oversees will be reviewed in more detail in Section 4.0 PIEE Administration Categories. The other PIEE Administrators have a subset of the full set of administrative functions available for the Super Administrator.

<table>
<thead>
<tr>
<th>Function</th>
<th>Function Description</th>
<th>PIEE Super Admin</th>
<th>PIEE Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Management</td>
<td>Administer groups and subgroups by adding, renaming, moving / deleting groups in the group structure, and adding / moving locations in the group structure.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Location Management</td>
<td>Administer locations by editing locations, adding extensions, editing extensions and viewing location and extension data.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>History Management</td>
<td>Review historical data for database tables.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Table Management</td>
<td>Administer database tables by adding, editing, deleting and viewing table data.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Subject Matter Expert (SME) Management</td>
<td>Manage Subject Matter Experts (SME) by Application and/or Location Code</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>User/Role Management</td>
<td>Administer database tables by adding, editing, deleting and viewing table data.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Web Service Administration</td>
<td>Administer database tables by adding, editing, deleting and viewing table data.</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Additional Administration</td>
<td>Administer database tables by adding, editing, deleting and viewing table data.</td>
<td>x</td>
<td>Subset of the Super Admin</td>
</tr>
</tbody>
</table>
2.2 Government and Contractor Administrators

The Government and Contractor Administrators will have similar functions, one set of administrators will manage the Government component and the other will manage the contractors. The following four roles will manage the functions of this area:

- Procurement, Finance and Logistics (PFL) Government Administrator
- Security Government Administrator
- PFL Contractor Administrator
- Security Contractor Administrator

Diagram 1: Group Management

2.2.1 Procurement Finance Logistics and Security Government Administrator

As shown in Diagram 1, the PFL Government Administrator will manage all the modules except for the NCCS module. The Security Government Administrator will oversee the function of this
module. These two administrators are responsible for the Government users and have the following functions available in their role:

- Level 2 Only – Move, Rename, and Delete Groups as well as Manage Location Codes within Agency.
- Level 2 Only – Deactivate Pay Location Codes within their Agency. (Only applicable to PFL Structure)
- Lookup Government Administrators for their structures.
- View Groups they are assigned to as well as any subgroups.
- View Location codes within their group and any subgroups.
- Manage org. emails and extensions within their group and any subgroups.
- Manage Users within their group and any subgroups including reset password / certificate.
- Manage user’s roles within their group and any subgroups.
- Send Notification emails to users within their span of control.

2.2.2  Procurement Finance Logistics and Security Contractor Administrator

As shown in Diagram 1, the PFL Contractor Administrator will manage all the modules except for the NCCS module. The Security Contractor Administrator will oversee the function of this module. These two administrators are responsible for the contractor or non-Government users and have the following functions available in their role:

- Lookup Contractor Administrators for their structure.
- View Groups they are assigned to as well as any subgroups.
- View Location codes within their group and any subgroups.
- Manage org. emails, extensions, location notifications (only applicable to WAWF) within their group and any subgroups.
- Manage Users within their group and any subgroups including reset password / certificate.
- Manage user’s roles within their group and any subgroups.
- Send Notification emails to users within their span of control.
2.3  Functional Auditor

The Auditor role has access to information in the system for auditing purposes. Auditor Role activation is handled through the PMO Office. The Auditor has access to the following links under Reports. Only the Auditor has access to Self-Registration Events, Logon Events and Document Events. These links are described in further detail under the Reports section of the Special User’s Manual.

3.  PIEE Administration Categories

3.1  Group Management

The users of Wide Area Workflow e-Business Suite are broken down into groups of seven levels. Each group is administered by one or more Group Administrators (GAMs).

There will only be two groups under TOP:
- OSD will be the root of the government group structure.
- OGDEN VENDORS will be the root of the vendor group structure. There will not be an option to add additional groups at this level.

**Service/Agency Level 2 GAM**
- Add a New Subgroup
- Rename a Level 2 Group
- Add Location Codes to a Level 2 group (although location codes are not required at this level). Navigate the entire group structure under the Service/Agency
- At Levels 3-6, the Service/Agency (Level 2) GAM will have options to Add Location Codes, Add Groups, Rename Groups and Move Groups. If a group does not have any subgroups, the Service/Agency GAM will have the option to delete the group.
- At Level 7, the Service/Agency GAM will have options to Add Location Codes, Rename Groups, Move Groups and Delete Groups.

**Service/Agency Level 3-7 GAM**
- Ability to navigate the entire structure under their group
- These GAMs will not be able to add new groups, delete groups or add/move location codes.
3.1.1 Procurement / Finance / Logistics Group Information

Group Structures will no longer be application specific.

There will be two separate hierarchies:

- Procurement / Finance / Logistics
- Security
This Group Management functionality gives the Administrator the ability to manage subgroups in the PFL or Security hierarchy, depending on the role they are assigned. They have access to adding, renaming, moving or deleting groups as well as adding or moving location codes in a group structure.
3.1.2 Group Lookup

The Group Lookup window allows the user to search by the Group Type. If Location Code is selected, the label will read "Location Code" and if Group Name is selected, the label will read "Group Name." When the user clicks Submit, the database conducts a search for a Group that matches the Group Name or Location Code.

There are times when the Group may have a Location Code that is not known, but is required to perform some action such as registering a user or determining the GAM associated with a specific Location Code. The GAM has a "review only" ability to view accounts that are more than two levels below his/her groups in the hierarchy.
3.1.3 Awaiting Location Codes

Administer Awaiting Location Codes from DAASC by assigning them to a Service/Agency within the PFL and/or Security group structures. This function is now available only to the PIEE level Administrators.
3.1.4 Group History

This is a dashboard for the Administrator to quickly review by any of the search criteria available when records were last updated. The available criteria are:

- Group Name
- Group Type
- Action Code
- Group Level
- Location Code
- Location Type Code
- User ID
- Parent Group ID
- Update from and to Dates

3.2 Location Management

This option is available to the Administrators under the Location tab on the Administration Console. Using these actions, the administrator may modify/update the organizational e-mail assigned to a group. This is also the location where they would add an extension to the selected location code. This option is more direct than navigating from Group to Group as with the User Administration (which is primarily focused on the users within a Group). To access these actions, the administrator enters the Location Code they want to administer. This section also allows the administrator to deactivate a location code.

3.2.1 Location Information
3.3 History Management

This is a view only access to the records that have had a change in each of the data tables. Each of the views of the tables will all contain a Date/Time Stamp of the last time the record was modified.

3.4 Table Management

This functionality gives the administrator view only access to all the records on the data table.
3.5 Subject Matter Expert (SME) Management

The administrators have access to this table to record the SME for each module. PIEE users have access to a lookup that utilizes this data table.

3.6 User/Role Management

User administration is the joint responsibility of the GAM/CAM and the PIEE Administrators. However, the GAM/CAM does not have access to the User Deletion link. Administrators have the option to View, Edit and Delete User profiles as well as reset passwords and certificates.

User Information
This option permits the Administrator to select a user or series of users. Once a user (or group of users) is identified, the Administrator may:

- View/Edit the profile
- View/Add to the user's roles
- Add attachments to a user's profile
- Add/Edit EDI attachment location paths (PIEE Administrator only)
- Archive any inactive accounts (This function is accessed through the Role link under the PIEE Administration Console and explained under Role Activation).

The Administrators may view the user's profile and/or the roles associated with the user, as well as view the time/date for activation/deactivation. In addition, the GAM / CAM / PIEE Administrators may edit the profile to update any portion of the information associated with that user such as telephone numbers etc.

User Deletion

This function permits the PIEE Administrators to search for and delete inactive users. Users are searched by entering a Registration Date Range.

Reset Password

Recognizing that the functional users can have occasions where the they forget passwords, the Administrators all can reset the user's password. By entering in the user's user ID, the Administrator can cause the system to generate that a one-time password has been given via secure fax or by phone. This permits the user to log on to PIEE with the one-time password. The user will then be prompted to answer the three security questions, enter their new password and confirm their new password.

Reset Certificate

The Administrators as well as the CAM/GAM are provided with the capability to reset passwords for one-time use and substitute a User ID credential for a certificate when required. The most significant reason for a certificate user to have an inability to use their certificate is that they have locked their smartcard because they have forgotten or mistyped their Personal Identification Number (PIN). The PIN is the password equivalent for the CAC card. Given the potential gap in time while a CAC user waits for replacement CAC after losing it or a PIN reset after locking it, we have provided a capability for the end user to request activation of the temporary credential of a User ID with strong password.

After receiving the request, the administrator can generate a one-time password for the user and an e-mail is sent to the user letting them know that a one-time password has been given via secure fax or by phone. This permits the user to log on to PIEE with the one-time password and the user's user ID (from the expired certificate). The user will then be prompted to answer the three security questions, enter their new password and confirm their new password. After
the user has replaced an expired software certificate, lost CAC, or received a PIN reset, that user can revert to the preferred credential through revised profile maintenance features.

The determination of the individual's User ID, which is system-generated for certificate users, can be made by searching the User Information using the affected user's First, Last Name, and optionally adding additional criteria such as an affiliated location code, role, or other available criteria. Resetting a certificate user changes their credential to User ID and password and all references to the previous credential are lost.

If the User being reset is a Government or Government Support Contractor, they will be allowed access to PIEE using a User Id/Password for the number of days specified in the System Properties table.

Role Administration

Role Information: View user role data, add a role, comments and attachments.

Role Activation: Activate, deactivate and archive user roles.

Role Activation Report: View role activation reports including disabled accounts.

Role Information

This option permits the administrators to select a user or series of users. Once a user (or group of users) is identified, the Administrator may:

• View and Add roles
• Add comments and attachments
• A Government Administrator can add the "Business Intelligence Access" role to existing Government users.

A Government GAM can add the new "Business Intelligence Access" role to existing Government users. The AKO E-Mail is mandatory and will be populated from the User Profile if it is there, otherwise it will have to be entered manually.

Government GAMs will also be permitted to manage the new "Business Intelligence Access" role.

Role Activation

The activation of government users is primarily the responsibility of the Government Administrator. That is the person who has the direct contact and control of their Group. However, since the Vendor community is not required to have a Contractor Administrator, the PIEE Administrator (Help Desk) also has the ability to activate users. In addition, an Administrator must activate the initial GAM/CAM in a Group.
By entering a variety of search criteria, a single user may be selected or a series of users may be selected from within a Group. At this point, his/her status may be changed from Inactive to Active, or Active to Inactive, and comments can be logged or files attached, as to the reason for the change. The Administrators may also archive inactive accounts. NOTE: The Functional Auditor Role can only be activated by the PMO.

Role Activation Report
This option permits the GAM to view role activation reports as well as information on disabled accounts. Filtered results provide the GAM with access to User ID history, roles and comments.

3.7 Web Service Administration
The functionalities of the Web Service Administration are available only to the PIEE Super Administrator.
### Web Service Registration

<table>
<thead>
<tr>
<th>Row</th>
<th>System ID</th>
<th>System Name</th>
<th>Logon Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SYS0_5F1260065484C13BA9FE193</td>
<td></td>
<td>System Name / Password</td>
</tr>
<tr>
<td></td>
<td>First Name</td>
<td>Last Name</td>
<td>Commercial Telephone</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>Confirm Email</td>
<td>DSN Telephone</td>
</tr>
<tr>
<td></td>
<td>Organization</td>
<td>Grade/Rank</td>
<td>Title</td>
</tr>
<tr>
<td></td>
<td>DITPR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The PIEE Super Administrator will log on to the WAWF application via the PIEE Home Page.
Activation

The activation of government users is primarily the responsibility of the Group Administrator. That is the person who has the direct contact and control of their Group. However, since the government users who intend on viewing WAWF attachments using Web Services, are not required to have a WAWF user account, the PIEE Super Administrator must activate the Web Service user. The PIEE Super Administrator will enter the appropriate data to search for the Web Service User to be activated and click the Submit link.

Information

When PIEE Super Administrator clicks on the System Name link for a particular user, a Web Service – Manage System Profile page will be displayed with 3 tabs:

- Profile
- Justification/Attachments
- Reset Password / Certificate

On the Profile tab, PIEE Super Administrator can view the Web Service user profile information, such as System ID, System Name, and Logon Type. The Admin user can also edit the profile information such as user’s name, phone number, organization and add/deleted a DoDAAC.

On the Justification/Attachments tab, the Admin user can view/add/delete system attachments and view/add justification.
Reset Web Service Password tab

Recognizing that the Web Service users can have occasions where he/she forgets his/her password, the PIEE Super Administrator has the ability to reset the user's password. By entering a value in the System Name field, the Admin can cause the system to generate a one-time password for the user and have that password sent to the email address that is contained in the user’s system profile.

Reset Web Service Certificate tab

The PIEE Super Administrator is provided with the capability to reset passwords and substitute a System ID credential for a certificate when required. The most significant reason for a certificate user to have an inability to use their certificate is that they have locked their smartcard because they have forgotten or mistyped their Personal Identification Number (PIN). The PIN is the password equivalent for the CAC card. Given the potential gap in time while a CAC user waits for replacement CAC after losing it or a PIN reset after locking it, we have provided a capability for the end user to request activation of the temporary credential of a User ID with strong password.

After receiving the request, the PIEE Super Administrator is able to generate and transmit a password to be paired with the new Web Service ID for viewing documents. After the user has replaced an expired software certificate, lost CAC, or received a PIN reset, that user can revert to the preferred credential through revised profile maintenance features.

Recognizing that the Web Service users can have occasions where their certificates expire and need to transfer their user ID to a new certificate, the Admin has the ability to reset the user's certificate. By entering in the user's Web Service ID (from the expired certificate), the Admin can cause the system to reset the user’s certification.

3.8 Additional Administration

**Administration Console**

<table>
<thead>
<tr>
<th>Tables</th>
<th>History</th>
<th>Reports</th>
<th>Standard</th>
<th>Web</th>
<th>SYSUID</th>
<th>Misc.</th>
<th>Explorer</th>
<th>Portal</th>
<th>Exit</th>
</tr>
</thead>
</table>

**Administration Console for System Administrators**

- **Tables**: Administrator database tables by adding, editing, deleting and viewing table data
- **History**: View changes to database tables
- **Reports**: View reports on Activation History
- **Standard**: Administrator standard extracts by registering extracts, activating extracts, registering pay office and viewing pay office data
- **Web**: Administrator web services by registering web services, activating web services, resetting web service passwords, resetting web service certificates and viewing web service data
- **SYSUID**: Administrator systems by registering systems, activating systems, resetting system passwords, resetting system certificates and viewing system data
- **Misc.**: Add SSO5 certificates, regenerate FTP/ESX notifications, edit system properties and add/edit system messages
- **Explorer**: Administrator explorer email list and send explorer email notifications
- **Portal**: Administrator ERP Systems
- **Exit**: Close the administration console window

Select an option from the console administration menu at the top of the page to begin.
3.9 Additional Administration Console Overview

System Tables are accessible by the WAWF PMO, Administrators and Auditor roles through the PIEE Administration Console menu. Tables are located under the ‘Tables’ and ‘History’ menu links. User privileges for these tables are based upon the assigned role of the logged in user.

There are four actions that may be taken on the system tables depending on the user role logged in:

- Search
- Add
- Edit
- Delete

Each system table has a matching history table where every action taken on the system table is recorded. The history tables have the same name as the system tables with a suffix of ‘_HST’.

**Table Administration Menu**

- Agency Help Desk
- Certificate Authorities
- Contract Closeout
- Contract Information
- Contract Number Type
- Contractor DoDAACs
- Currency Codes
- DCAA Direct Bill Authorization Codes
- DCMA Direct Bill Authorization Codes
- DCMA Administration Location Codes
- DCMA Cost Voucher Processing Location Codes
- DFAS Pay Codes
- DoDAAC Prefix Suffix
- DSS Acceptor
- EDI Location Codes
- EDI Extracts
- EEBP Locations Codes
- Energy Tests - Master List
- Energy Commodities
- Energy Sub Commodities
- Energy Tests - Add/Edit/Delete
• Order Energy Tests
• Energy Test Categories
• Group Energy Tests
• Energy Test Types
• Energy Issue By DoDAACs
• Energy Signature NSNs
• Entitlement Status Update
• Extract Suppression
• File Extensions
• Foreign Military Sales Codes
• Group Role Id
• IUID Data Correction Locations
• IUID DoDAAC Prefix Suffix
• Legacy AAI Codes
• Matching DUNS/CAGE
• Misc. Fee Type Codes
• Misc. Pay DBS
• Misc. Pay Type Codes
• Navy ERP Ship To Codes
• One-Pay AAlCs
• One-Pay TFS AAIs
• ONR Cost Voucher Processing Location Codes
• Org Location Codes
• Org Location Notifications
• PKI Constrained Policy Sets
• PKI Exemption
• PKI Policy Configurations
• Pay System Misc. Tax and Fee Codes
• QCTS DoDAACs
• Payment and Accounting Systems
• System Extracts
• System Misc. Pay Types
• Receiving Activities
• Reference Taxes
• Restricted Currency Codes
• Special Package Markings
• Standard Extracts
• Standard Systems
• SUPSHIP DoDAACs
• Tax Type Codes
• Unit Of Measure
• WAWF Extra Data

The History Administration option is available to the Administrators, WAWF PMO and Auditor roles. This allows the administrator to view changes to database tables.

Each system table has a matching history table where every action taken on the system table is recorded. The history tables have the same name as the system tables with a suffix of ‘_HST’.

**History Table Administration Menu**

• Agency Help Desk
• Certificate Authorities
• Contract Closeout
• Contract Number Type
• Currency Codes
• DCAA Direct Bill Authorization Codes
• DCMA Direct Bill Authorization Codes
• DCMA Administration Location Codes
• DCMA Cost Voucher Processing Location Codes
• DFAS Pay Codes
• DoDAAC Prefix Suffix
• DSS Acceptor
• EDI Location Codes
• EDI Extracts
• EEBP Locations Codes
• Energy Test Master
• Energy Results Dropdown Master
• Energy Test Categories
• Energy Results Dropdown
• Energy Issue By DoDAACs
• Energy Signature NSNs
• Energy Test
• Energy Test Codes
• Energy Test Types
• Entitlement Status Update
• Extract Suppression
• File Extensions
• Foreign Military Sales Codes
• Group Role Id
• IUID Data Correction Locations
• IUID DoDAAC Prefix Suffix
• Legacy AAI Codes
• Misc. Fee Type Codes
• Misc. Pay DBS
• Misc. Pay Type Codes
• Navy ERP Ship To Codes
• One-Pay AAs
• One-Pay TFS AAs
• ONR Cost Voucher Processing Location Codes
• Org Location Codes
• Org Location Notifications
• QCTS DoDAACs
• Payment and Accounting Systems
• System Extracts
• System Misc. Pay Types
• Pay System Misc. Tax and Fee Codes
• Receiving Activities
• Reference Taxes
• Restricted Currency Codes
• Standard Extracts
• Standard Systems
• SUPSHIP DoDAACs
• Tax Type Codes
• Unit Of Measure
• WAWF Extra Data

Reports

• User Activation History
• Administrator Activation History

Standard

This allows administrators to administer standard extracts by registering extracts, activating extracts, registering pay offices and viewing pay office data.

Standard Extract Registration - Provides the administrator the ability to sign up External Entities to receive Standard Extracts.

Standard Extract Activation - Provides the administrator the ability to activate and deactivate Standard Extracts.
Pay Office Registration - Prior to the administrator signing up External Entities to receive Standard Extracts they must ensure that the External Entity has a Standard Pay DoDAAC within the WAWF program.

Pay Office Information - Allows administrators to Editing Standard Pay Office Information.

Misc Administration

The Miscellaneous Administration option is available to the PIEE Super Administrator and PIEE Administrator. This allows the administrator to add X509 certificates and regenerate FTP/EDI notifications.

In addition, the PIEE Super Administrator, PIEE Administrator and WAWF PMO are responsible for the System Properties and System Messages sections.

Add Certificate

The System Administrators are provided with the capability to save the Root and the Root Issuer certificate authority details into the database by using the application.

FTP/EDI Notification Regeneration

This option is available to the PIEE Super Administrator and PIEE Administrator only. This allows the administrator to regenerate FTP/EDI notifications.

System Properties

The SYSTEM_PROPERTIES entity stores all the FTP/EDI and some of the property file parameters. It has all the sensitive data stored and is an editable PMO table.

System Messages

The SYSTEM_MESSAGES entity stores all the system messages and can be added to and edited by the WAWF PMO.

Exploder

The administrator exploder email lists and send exploder email notifications using the Exploder Information link. The information can be edited and deleted as well.

Portal Administration

The Portal Administration menu is available to select administrators. ERP Systems Administration manages ERP systems that are registered with PIEE. ERP CAGE Administration manages CAGEs that are assigned to ERP Systems.
4. **WAWF Administrator Roles**

4.1 **WAWF System Administrator**

The WAWF System Administrator (formerly the WAWF SAM/HAM) will have the following functions available:

- View Documents in WAWF

![WAWF](image)

**Document Administration**

- View DOCUMENTS
- View IGT Receiving Report DOCUMENTS
- View 2.0 DOCUMENTS
- Send Key To PMO
- Delete Documents
**View DOCUMENTS**

**FOUO - Privacy Sensitive:** This information is protected under the Privacy Act of 1974 and shall be handled as "FOR OFFICIAL USE ONLY."

<table>
<thead>
<tr>
<th>Search For</th>
<th>Active Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems</td>
<td>WAFF</td>
</tr>
<tr>
<td>Contract Number</td>
<td>equal to</td>
</tr>
<tr>
<td>Delivery Order</td>
<td>equal to</td>
</tr>
<tr>
<td>Reference Procurement Id</td>
<td>equal to</td>
</tr>
<tr>
<td>Gaining Contract Number</td>
<td>equal to</td>
</tr>
<tr>
<td>Gaining Delivery Order</td>
<td>equal to</td>
</tr>
<tr>
<td>Shipment Number</td>
<td>equal to</td>
</tr>
<tr>
<td>Invoice Number</td>
<td>equal to</td>
</tr>
<tr>
<td>Batch Number</td>
<td>equal to</td>
</tr>
<tr>
<td>Location Code</td>
<td>Extension</td>
</tr>
<tr>
<td>Location Code</td>
<td>Extension</td>
</tr>
<tr>
<td>Location Code</td>
<td>Extension</td>
</tr>
<tr>
<td>Type Document</td>
<td></td>
</tr>
<tr>
<td>Inspection Point</td>
<td></td>
</tr>
<tr>
<td>Acceptance Point</td>
<td></td>
</tr>
<tr>
<td>Is Part of a COMBO?</td>
<td></td>
</tr>
<tr>
<td>SSN</td>
<td></td>
</tr>
<tr>
<td>EIN/Tax Id</td>
<td></td>
</tr>
<tr>
<td>Create Date</td>
<td>YYYY/MM/DD - thro - YYYY/MM/DD</td>
</tr>
</tbody>
</table>

- Send Key To PMO to request document deletion
Delete WAWF documents that have been approved by PMO

**4.2 WAWF PMO**

The WAWF PMO administrator has accessibility to the following functions:
• View Documents in WAWF

![WAWF Interface]

**Document Administration**

- View DOCUMENTS
- View IGT Receiving Report DOCUMENTS
- View 2.0 DOCUMENTS
- Approve / Deny Deletion

• Approve or Deny Documents that have been requested for deletion

![WAWF Interface with Approved / Denied Document Table]

- Role Management: Administer roles by activating, deactivating, and archiving user roles.

- History Management: Review historical data for database tables.

- Table Management: Administer database tables by adding, editing, deleting and viewing table data.

Additional Administration

4.3 Group View All

The Group View All Administrator will have view only capabilities to a set of documents in WAWF. It will be based on the location codes in the Group as well as any subgroups.
4.4 DLA Energy Table Administrator

The DLA Energy Table Administrator will have access to edit or delete data on the DLA Energy tables. This administrator also has the ability to view the history of changes to the DLA Energy tables.

Tables:
- Table Administration
- Energy Tests - Master List
- Energy Commodities
- Energy Sub Commodities
- Energy Tests - Add/Edit/Delete
- Order Energy Tests
- Energy Test Categories
- Group Energy Tests
- Energy Test Types
- Reference Taxes

History:
- History Table Administration
- Energy Test Master
- Energy Results Dropdown Master
5. MIPR Administrator Roles

5.1 MIPR Administrator

The eMIPR Administrator will have access to view Purchase Request documents. The screenshot below are the available search criteria available.
6. IUID Administrator Roles

6.1 IUID Help Administrator

Many of the administrative role privileges for the IUID module have been elevated to the PIEE level administrators. The remaining Help Administrator has access to the following duties for the module:

- Add new IUID records
- Update all existing IUID records
- Correct all existing IUID records
- Query all IUID records
- Run all Reports for IUID records.

Additionally, the administrator has access to a metrics view and the IUID documentation.
7. **CORT Administrator Roles**

CORT Tool Administration is accomplished through two CORT Tool specific administrative roles: Administrator (DPAP) and Administrator (Department). Many of the administrative functions have been transferred to an administrator at the PIEE level.

### 7.1 Administrator (DPAP)

The DPAP Administrator manages all groups, users, nominations, emails and documentation that affects the CORT Tool.
CORT Tool Administrative functions in CORT Tool Menu:

- **Admin Email (ADMIN):** Edit and view CORT generated email messages.
- **All COR Submitted Documents:** Review Contract Management Reports associated for all contracts in the CORT Tool.
- **Local Forms and POCs:** Add and delete Points of Contact and forms for download for each Contracting Center Department.
- **COR Misc Codes (ADMIN):** Administers codes that control the CORT Tool application options and text.
- **Course List (ADMIN):** Manage course list options used on the COR Profile page.
- **Document Templates:** Add and delete templates for download on the document templates page.
- **Document Upload (ADMIN):** Add and delete documents for download on the CORT Home page.
- **Link to Reports (ADMIN):** Add and delete Misc Reports for download on the Link to Reports page.
- **View All CORs (ADMIN):** To manage all the nominations throughout the system. DPAP Administrators can reject, cancel and recall nominations, update QAPOC, ACO, supervisor, contracting officers and contract specialist on the nomination, revise the contracting information.
- **View All Users (ADMIN):** View all CORT users and their supervisor’s information.
- **Merge Profiles (ADMIN):** To merge role and contract nomination data for a Source User ID into the user profile of a Destination User ID. The Source User ID roles and profile data are deleted during the merge.
- **POPs Country / POP Unit / POP Sub Unit / POP NIA / POP Zip Code**

7.2 Administrator (Department)
The Department Administrator manages nominations within their designated department in the CORT Tool.

**CORT Tool Administrative functions in CORT Tool Menu:**

- **Document Upload (ADMIN):** Review documents for download on the CORT Home page.
- **Link to Reports (ADMIN):** Review Misc Reports for download on the Link to Reports page.
- **View All CORs (ADMIN):** To manage the nominations within their Contracting Center. Department Administrators can cancel and recall nominations, update QAPOC, contracting officers and contract specialist on the nomination, revise the contracting information.
- **All COR Submitted Documents:** Review Contract Management Reports for contracts associated within their Department.
- **Local Forms and POCs:** Add and delete Points of Contact and forms for download for their Contracting Center Department. View Points of Contact and local forms for outside of their Department.
- **Document Templates:** Review document templates.

### 8. NCCS Administrator Roles

NCCS includes the following Administrator Roles:

- **NCCS Administrator – View Documents in NCCS /Edit Help pages and Title text**
- **NCCS PMO**
  - View Documents in NCCS
  - Edit Help pages and Title text
  - Edit Security and Contracting Policy Text
  - Edit Blocks 10 and 11 labels
  - Update system properties
  - Add or delete NCCS Help Documents.

- **NCCS Group View All – View Limited Documents in NCCS (based on location codes in the Group as well as any subgroups)**

- **NCCS Auditor – Has the ability to View changes to NCCS database tables and View Document Events.**
The following roles are activated by the NCCS PMO administrator. These roles give the user access to various levels of update or view capabilities within NCCS.

- Facility Branch Officer Reviewer / Facility Branch Officer Reviewer View Only
- Oversight View All
- NID Reviewer / NID Reviewer Only
- NID Control Agency Reviewer / NID Control Agency Reviewer Only

8.1 **NCCS Administrator**

NCCS Administrator – View Documents in NCCS / Edit Help pages and Title text

NCCS Management: Edit Help pages and Title text. Edit Security and Contracting Policy Text.
8.2 NCCS PMO

The NCCS PMO Administrator has access to the following PIEE Administrative privileges.

Additionally, the NCCS PMO administrator has access to the following functions within the NCCS module. The NCCS PMO administrator has the same capabilities as the NCCS Administrator to search and view documents.

- View Documents in NCCS
- Edit Help pages and Title text
- Edit Security and Contracting Policy Text
- Edit Blocks 10 and 11 labels
- Update system properties
- Add or delete NCCS Help Documents
8.3 Auditor

The NCCS Auditor has the privileges to search and view documents in NCCS.

8.4 Other NCCS Reviewer and View Only Roles
Facility Branch Officer Reviewer and View Only

*No admin console*
### Group View All

**View Only Search**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Folder</td>
<td>Current</td>
</tr>
<tr>
<td>Document ID</td>
<td></td>
</tr>
<tr>
<td>Prime Contract Number</td>
<td></td>
</tr>
<tr>
<td>Subcontract Number</td>
<td></td>
</tr>
<tr>
<td>Solicitation Number</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Please Select</td>
</tr>
<tr>
<td>Type</td>
<td>Please Select</td>
</tr>
<tr>
<td>Level</td>
<td>Please Select</td>
</tr>
</tbody>
</table>

**Advanced Search Criteria**

**Agency Lookup**

| Agency Name | **|
### Oversight View All

#### View Only Search

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Folder</td>
<td>CURRENT</td>
</tr>
<tr>
<td>Location Type</td>
<td>--- Please Select ---</td>
</tr>
<tr>
<td>Location Code</td>
<td></td>
</tr>
<tr>
<td>Document ID</td>
<td></td>
</tr>
<tr>
<td>Prime Contract Number</td>
<td></td>
</tr>
<tr>
<td>Subcontract Number</td>
<td></td>
</tr>
<tr>
<td>Solicitation Number</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>--- Please Select ---</td>
</tr>
<tr>
<td>Type</td>
<td>--- Please Select ---</td>
</tr>
<tr>
<td>Level</td>
<td>--- Please Select ---</td>
</tr>
</tbody>
</table>

#### Agency Lookup

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Name</td>
<td></td>
</tr>
</tbody>
</table>
### NID Reviewer and View Only

**National Interest Determinations Search**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Folder</td>
<td>INBOX</td>
</tr>
<tr>
<td>Document ID</td>
<td></td>
</tr>
<tr>
<td>Prime Contract Number</td>
<td></td>
</tr>
<tr>
<td>Subcontract Number</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>--- Please Select ---</td>
</tr>
<tr>
<td>Type</td>
<td>--- Please Select ---</td>
</tr>
</tbody>
</table>

**View Only Search**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Folder</td>
<td>INBOX</td>
</tr>
<tr>
<td>Document ID</td>
<td></td>
</tr>
<tr>
<td>Prime Contract Number</td>
<td></td>
</tr>
<tr>
<td>Subcontract Number</td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>--- Please Select ---</td>
</tr>
<tr>
<td>Type</td>
<td>--- Please Select ---</td>
</tr>
</tbody>
</table>
9. **GFP Administrator Role**

The GFP System Administrator has the following administrative functionalities available.

- Search GFP Attachment
- GFP Scheduler
- View Property Documents
- Send Key to PMO
- Delete Documents

9.1 **GFP System Administrator**

The GFP System Administrator has access to search and view the GFP Attachments.
This administrator can also view statuses of different scheduled tasks. It allows starting/Stopping of specific tasks. Special care MUST be taken when starting or stopping a specific task as it will affect how the application is behaving.

The GFP System Administrator has access to search and view the GFP Documents.

The GFP System Administrator will have privileges to Send Key to PMO.

The GFP System Administrator will also have the rights to delete GFP Documents.
10. CLS Administrator Roles

The other administrative roles within the CLS module have automatic access to EDA Contracts role. They can access the CLS application but have no access to the PIEE Administration Console.

10.1 Program Management Office (PMO)

The Program Management Office Administrator for the CLS module has access to the PIEE Administration Console to manage the users of the CLS Module only.
11. Solicitation Administrator Roles

11.1 Solicitation Administrator

The Solicitation Administrator has access to search and view the solicitations. There is also the capability to search for the available Product/Service Codes and NAICS.

![Solicitation Search Criteria](image)

**Lookup Functionality**

![Product or Service Code Lookup](image)

![NAICS Lookup](image)
12. PPML Administrator Roles

12.1 PPML PMO

The Program Management Office Administrator for the PPML application has access to the PIEE Administration Console to manage the users of the PPML module only.
13. PC Administrator Roles

13.1 GPC DoD PMO

The GPC DoD Program Management Officer for the PC application has access to the PIEE Administration Console to manage the users of the PC module only.

13.2 GPC HAM

The GPC HAM user for the PC application has the capability to search appointments in JAM.
13.3 GPC Auditor

The GPC Auditor user for the PC application has access to the Solicitation and PCM modules.

13.4 GPC Support View Only

The GPC Support View Only user for the PC application has access to the following modules: Solicitation, PBIS, PCM, JAM, and U.S. Bank.
14. SPRS Administrator Roles

14.1 SPRS HAM

The SPRS HAM user for the SPRS application has access to the PIEE Administration Console to manage the users of the SPRS module only.
15. **Contract Deficiency Report Administrator Roles**

Please refer to the PIEE Admin section for more detailed descriptions of the functions listed below.

15.1 **Administration**

- Account Information/Activation
- Government Support Contractor Request
- Reset Password
- Reset Certificate
- EDA POC Assignments
- Account Activation History

15.2 **C/S/A Administration**

15.3 **Location Administration**
16. Purpose Code Management (PCM)

The Purpose Code Management (PCM) Module will provide three main functionalities:

- Contract Administration Office (CAO) DoDAAC and Pay Office (PO) DoDAAC Tool
  - DCMA Contract Administration Office Manager – manage the relationships between the CAO and PO DoDAACs with zip codes and CAGE codes.
  - Users – will have the ability to select zip codes or CAGE codes and retrieve the corresponding CAO and PO DoDAACs
- Contract Administration DoDAAC Requests – Registered and non-Registered PIEE users
- Purpose Code Flag Administration

16.1 DCMA Contract Admin Office (CAO) Manager

The DCMA CAO Manager is the administrator of the Contract Admin Office and Pay Office DoDAACs. This manager will manage the relationship of the CAO and Pay Office DoDAACs with zip codes and countries. They will also manage any CAGE codes with exceptions to the DCMA assignments.
Additionally, the DCMA CAO Manager also has access to a list of data tables. These data tables are a convenient way for this administrator to view all the data elements on one spreadsheet. These spreadsheets can be downloaded for further analysis by the DCMA CAO Manager.

16.2 Contractor DoDAAC Manager

The Contractor DoDAAC Manager role serves as the approver for the Contractor DoDAAC Requests.

- The current PIEE Users that belong in the Job Series 1102 (includes ACO, Contract Specialist ACO, PCO, and Contract Specialist PCO) will automatically be granted this role.
- Job Series 1102 Users with this role may submit a Contractor DoDAAC request and can self-approve the request, they will also have the ability to approve other requests within their DoDAAC.

Non-1102 Series PIEE users may register for this role, however they will not have the ability to approve their own requests. They can only approve the requests within their DoDAAC.
16.3 Purpose Code Flag Administrator

The following roles have been added for the Purpose Code Management application:

- Payment Office Purpose Code Manager
- Procurement & Grant Purpose Code Manager
- Contract Admin Purpose Code Manager
- Contractor Admin Purpose Code Manager

As PIEE users submit requests for purpose code flag updates these managers will have the ability to approve or reject the requests.