Office of the Chief Information Officer

Enterprise Access Request System (EARS)

User Guide

Document Information:

Author:	Terry Smith
Office:	Financial Administrative Systems Division (ICDFS)
Date Created:	10/6/2009
Date Last Modified:	3/26/13
Version	1.2

Record of Changes Log

Date of Change	Ver/ OCP #	Person Requesting Change	Page No.	Change Comments
10/6/2009				Initial Document Created
11/15/2010	18649	Wanda Rickard	Various	EARS Phase2 Enhancements
11/19/2010		Wanda Rickard	31	Clarification provided on GSA Rules of Behavior for Recertification's
3/26/13	V1.2	Terry Smith		- Strike Out References to External or Non-GSA Users Marked Out - Replaced sections in this document with those that had been updated individually as user guides in the FAQ separately

Table of Contents

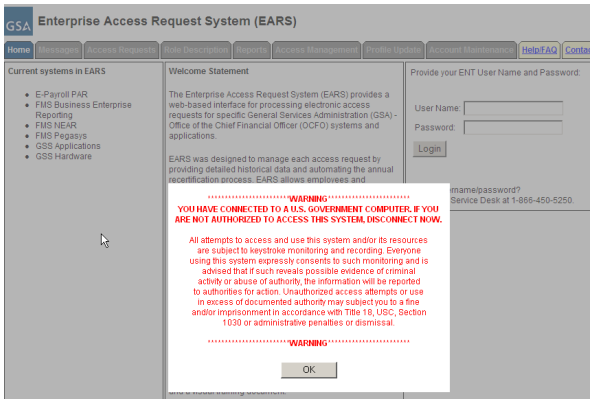
1. Overview of EARS

The Enterprise Access Request System (EARS) provides a web-enabled front-end environment for processing electronic access requests for specific General Services Administration (GSA) - Office of the Chief Financial Officer (OCFO) systems and applications. EARS allows employees, *both Internal and External*, and managers to submit access requests for new accounts, cancel existing accounts, and process the annual recertification within those systems and applications. Actions submitted through EARS are captured and processed into a backend database referred to as Enterprise System Change (ESC). ESC provides for an integrated workflow process supporting all required levels of access request approvals. Managers, Liaisons, System Owners and the Information System Security Officer (ISSO) will perform all access management functions (approval, denial, recertification, role assignment, etc.) via EARS.

2. EARS Web Page Login

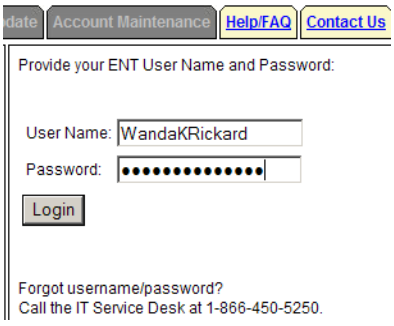
2.1. EARS Web Page is hosted on the public internet, but requires user login to provide an additional layer of security.

2.2. The EARS application is by accessed by opening up a web browser and pointing it to the website address: **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**. Upon visiting this website address a Warning Banner is presented to the user. Click OK to proceed. This allows user access to the Home, Help/FAQ, and Contact Us pages only. To submit an access request and/or perform the approval processes, the user must Login.

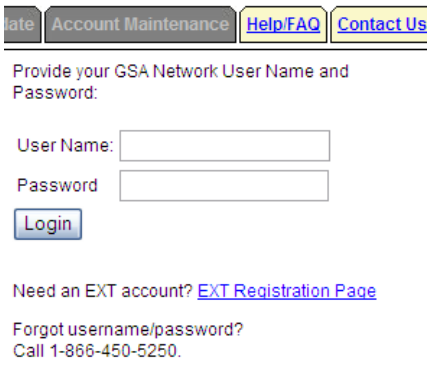


2.3. The User's IP address will determine if the web page requires ENT ~~or GSA Network (EXT)~~ account credentials to Login.

2.3.1. GSA Users will use their ENT login credentials



~~**2.3.2. External Users (Non-GSA Users) will use their GSA Network (EXT) account login credentials**~~



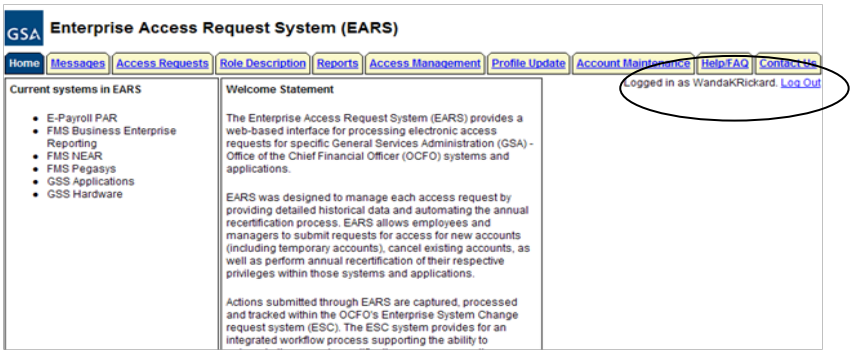
~~**2.3.3. If the External User does not not have an EXT account, see the interim Special Processing for External (Non-GSA) Users workaround in section 16.**~~

2.4. Upon successful login, the account logged in will display in the upper right corner.

2.5. The menu tabs are available based upon user login credentials as specified below, some menu tabs are currently under construction (identified in section 14).

2.5.1. User – Home, Messages, Access Requests, Profile Update, Help/FAQ, and Contact Us

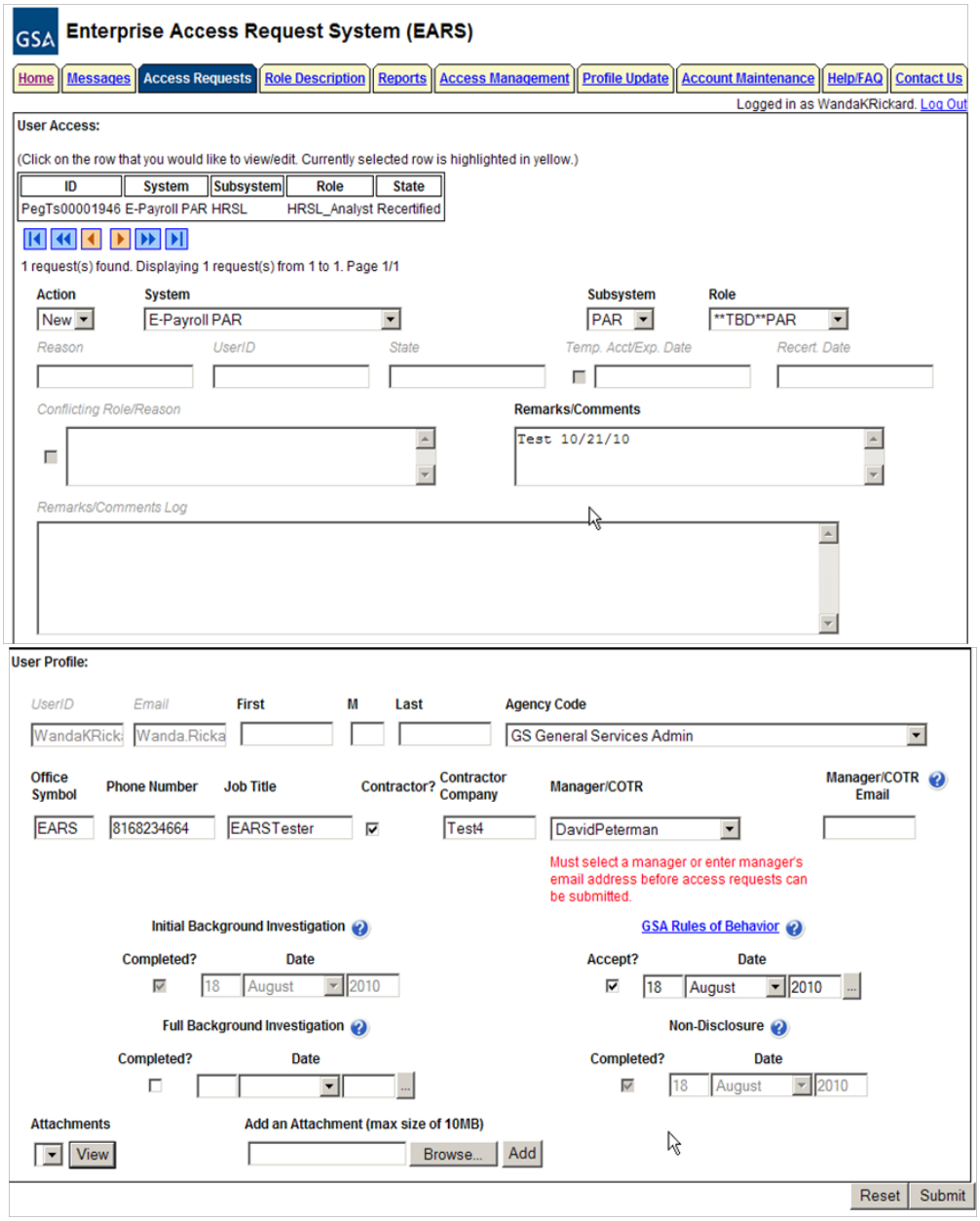
2.5.2. Manager/Liaison/System Owner/ISSO – Home, Messages, Access Requests, Role Description, Access Management, Profile Update, Help FAQ, and Contact Us



3. Access Request Details

Below is a picture of the EARS Access Request page. Each field will be listed with an explanation of the data to be populated in each field.

The User and Managerial Approval groups have specific instructions to complete their duties; within each separate process, the fields to be updated are identified.



3.1. User Access Section – Fields that are grayed out are unavailable.

3.1.1. Action - This is the basis for all access requests and approvals. It is a required field throughout each step of the access request process. Starting with a New Access Request, through all Manager Approvals, User Access Verification, Annual Recertification, and the Cancellation of access requests. Each individual section within this document gives the available actions based on the state of the access request and required action.

3.1.2. System – By clicking the down arrow button, it will display all Systems maintained by EARS/ESC for which an access request is required to gain access to the System.

3.1.3. Subsystem – By clicking the down arrow button, it will display all of the available Subsystems for the corresponding System selected.

3.1.4. Role/Additional Role *(not visible to the User)* **–** The User will NOT select the Role. Either the Manager or the Liaison will perform the Role(s) assignment; System Owner also has the ability to add an additional role. Refer to the table below for explanation of Internal/~~**External**~~ GSA users ~~**and External Client users**~~ and the person responsible for role assignment. Managerial groups (Manager, Liaison, System Owner, and ISSO) have access to role description document, which can be found under the Role Description Menu tab. To select Additional Roles, hold down the Ctrl key while clicking on the additional roles.

User Type	User Type Definition	Approval of System/Application	User to perform Role Assignment
Internal System User **(GSA user)**	1. User is a GSA employee. 2. Manager selected in Access Request is listed in the ESC Manager's table for corresponding System/Application approval path.	1. Manager approves access to System and Subsystem. 2. Manager performs Role Assignment	Manager

3.1.4.1. Internal System User - the Manager is expected to perform the role(s) assignment.

~~**3.1.4.2. External System and External Client User - The Manager is expected to leave the role as ***TBD***, this operation will be performed by the Liaison.**~~

3.1.5. Reason – Authorized User. This field is populated behind the scenes once the User submits the initial access request.

3.1.6. UserID – This field will remain blank on new access requests throughout the entire approval process. The Implementation group will populate once the access has been granted. It will be verified by the user during the Verify Active process. Once populated, it will display each time that specific access request is selected.

3.1.7. State – Displays the current state of the access request, blank upon the initial creation of an access request.

3.1.8. Temporary Account Indicator and Expiration Date – This field is used to identify an access request (all roles selected) as a temporary account. If the box is checked, an expiration date will be required. The Manager, Liaison, and System Owner are allowed to populate this field. If populated, the system will automatically deactivate the record on the requested date; no notification will be sent to the user or manager.

3.1.9. Recert Date – The system will populate this date which is one year from the date the access was granted. This date is used to initiate the annual recertification process.

3.1.10. Conflicting Role Indicator and Reason – The conflicting role check box will populate automatically once the role(s) assignment has been submitted/verified, based on the conflicting roles identified within the role description document which are set up in ESC upon the initial data load of the System/Application. This field is not displayed to User, Manager, or Liaison approval levels. The System Owner will be required to enter a reason if this field is checked.

3.1.11. Remarks/Comments – This field is available to ALL users and managerial approval groups. Any comments recorded in this field will remain in the historical data associated with this access request and displayed in the Remarks/Comments Log upon success access submission.

3.1.12. Remarks/Comments Log – The entire data flow of the request with detailed information, including text from Remarks/Comments text box, associated with this access request as well as the historical approval details.

3.2. User Profile Section – Fields that are grayed out are unavailable

3.2.1. UserID – Unavailable for update by the User, field is populated from Active Directory.

3.2.2. Email – Unavailable for update by the User, field is populated from Active Directory.

3.2.3. Employee Name – First Name, Middle Initial (if applicable), and Last Name if changed.

3.2.4. Agency Code – Click the down arrow button to select your employing Agency

3.2.5. Office Symbol – Optional text field to allow entry of your Office Symbol

3.2.6. Phone Number* – Enter 10 digit phone number

3.2.7. Job Title – Optional text field to allow entry of your Job Title

3.2.8. Contractor - Checkmark the Contractor box if applicable - This will require the user to acknowledge that a signed Non-Disclosure Agreement (NDA) is on file with the GSA contractor.

3.2.9. Contractor Company – Optional text field to enter the Contractor Company with which you are employed.

3.2.10. Manager/COTR - Select Manager from drop down menu. If your manager is not displayed, then enter your Manager/COTR email address in the next field.

3.2.11. Manager/COTR email - If the manager's name is not displayed in the Manager/COTR drop down menu, then enter your manager's email address. ** This access request

will be sent to the email address provided (for approval), so please double-check the email address before submitting. **

3.2.12. User Security Verification

3.2.12.1. Initial Background Investigation – Required to submit an access request. If received, check the Completed box and enter the Date completed. This is required only once per UserID.

3.2.12.2. Full Background Investigation – Optional field. If user has received a full background investigation, check the Completed box and enter the Date completed.

3.2.12.3. GSA Rules of Behavior – Required to submit an access request (also required to be reviewed on an annual basis). The link will direct you to the current GSA Rules of Behavior; once reviewed, check the Accept button as acknowledgement that you agree to adhere to the rules of behavior. Enter the Date completed.

3.2.12.4. Non-Disclosure – If you checked the Contractor box, this becomes a required field. Check the Completed box and enter the Date completed which signifies that you have reviewed/signed the NDA and given it to your COTR.

3.2.12.5. Attachments – The first attachment box allows the user to 'view' existing attachments. The second box allows the user to 'add' an attachment (i.e. email of background investigation for audit support)

3.2.13. Reset Button – Clears the screen and allows for reentry

3.2.14. Submit Button – Click the Submit button to begin the access request process.

3.2.14.1. Upon clicking the Submit button, the User will receive a Confidentiality Statement which must be acknowledged by clicking OK before the access request will be submitted. The Managerial groups will receive a Confirmation Statement which must be acknowledged by clicking OK before the approval request will be submitted.

3.3. Submitting the access request does not grant immediate access, it simply verifies the request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the approval workflow process (see section 15 for workflow process).

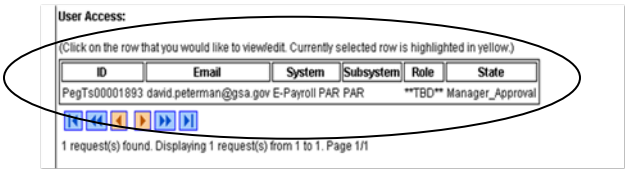
3.3.1. The bottom left of the page will display if the User Profile was updated successfully and/or the Access Request was submitted successfully. It will also display errors with the requested submission.

3.3.2. The newly submitted request will appear or disappear in the Request Queue based on the Access Request state.

3.3.2.1. The employee will be able to see ALL access requests associated with their UserID and the corresponding state.

3.3.2.2. The newly submitted request will appear in the Request Queue, for Users, showing a state of Manager_Approval, meaning it has been forwarded to the specified manager for approval.

3.3.2.3. Upon each level of Managerial approval, the Request will be removed from their Request Queue as confirmation that the request has been forwarded to the next level of approval.



4. Access Request – New

Requests for access to applications administered by EARS must be made for each "Role" that the requestor and his/her supervisor has agreed is needed to perform their assigned duties. The granting of access by role is a multi-step approval process dictated by security rules in effect in the agency.

Overview – New Access Request Process Steps for Applications

1) **Sign into EARS**
2) **Check and update your User Profile for your current supervisor (if necessary)**
3) **Select the System and Sub-System (Application) you need access to**
4) **Choose the Role required to do your assigned duties (the specific role needed generally comes from your supervisor)**
5) **Submit the Access Request**

That's all you need to do !!

See below for Detailed Steps for Requesting Access

4.1 Detail – New Access Requests

The User will sign into EARS using their ENT login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**. Refer to the EARS User Guide (EARS Web Page Login), located in the Help/FAQ menu tab, for assistance with the login screen.

Click on the **Profile Update tab** –**** Please verify the Manager listed is your current manager, this is the person used to verify your access to the system/application ****

1 - If the Supervisor/COTR is correct - Skip to Step 3

2 - If the Supervisor/COTR is NOT Correct - Use Pull-Down to see if your manager is on the existing list of managers and choose him/her and go to Step 2.5

3 - If the manager is NOT on the list, then click on the "not listed" link. You need to provide the ENT Name AND email of the manager you wish to add. Please note that the manager MUST be listed in

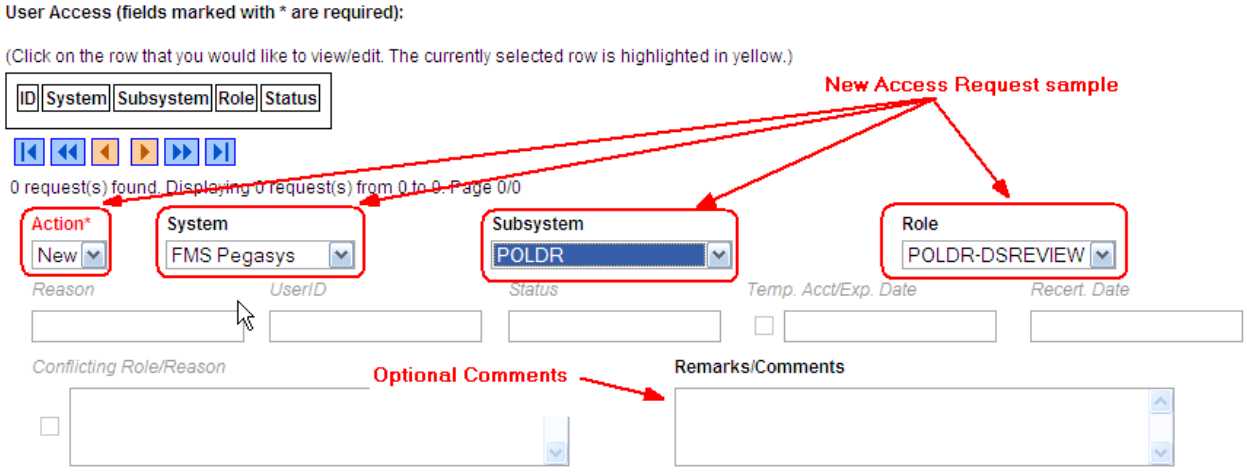
CHRIS as a manager or other evidence provided or audit rules will not permit the addition.

4 - Once you provide the new manager ENT and email, a request will be made to add the manager. You will be notified when the request is complete.

5 - Go to the bottom of the form and click "Submit" button

Wait for a message of "Submission Successful" OR take a screen shot of any error message and send to ears.support@gsa.gov and then log out, as your manager change was not successful

6 - Once the User Profile has been checked/updated, the User will click the **Access Request** menu tab to perform the New Access request. The first part of a sample new access request is shown below. The step following goes into greater detail on the individual fields requirements..



User Access Section (“ * ” denotes Required field) – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the ‘User’.**

1. **- Action*** – Click the down arrow button and select ‘NEW’
2. **System***– Click the down arrow button to select the System to which you are requesting access.
3. **Subsystem*** – Click the down arrow button to select the Subsystem to which you are requesting access.
4. **Role –** The Role is mandatory, DO NOT use the ** TBD ** role. You should obtain the specific role you need from your supervisor or co-worker with similar duties. Select the specific role needed from the list if it does not default to a Role.
5. **Remarks/Comments** – You may enter remarks/comments in this field, it will remain in your access record and be displayed to all managers throughout the approval process.

User Profile Section

1 **Employee Name** – First Name, Middle Initial (if applicable), and Last Name

2 **Agency Code** – Click the down arrow button to select your employing Agency

3 **Office Symbol** – Optional text field to allow entry of your Office Symbol

4 **Phone Number** – Enter 10 digit phone number

5 **Job Title** – Optional text field to allow entry of your Job Title

6 **Contractor** - Checkmark the Contractor box if applicable - This will require the user to acknowledge that a signed Non-Disclosure Agreement (NDA) is on file with the GSA contractor.

7 **Contractor Company** – Optional text field to enter the Contractor Company with which you are employed.

8 **Manager/COTR *** If the manager is NOT on the list, then click on the "not listed" link. You need to provide the ENT Name AND email of the manager you wish to add. Please note that the manager MUST be listed in CHRIS as a manager or other evidence provided or audit rules will not permit the addition.

9 Once you provide the new manager ENT and email, a request will be made to add the manager. You will be notified when the request is complete

10 **User Security Verification**

Initial Background Investigation * – Required to submit an access request. If received, check the Completed box and enter the Date completed. **This is required only once per UserID**.

Full Background Investigation – Optional field. If user has received a full background investigation, check the Completed box and enter the Date completed.

GSA Rules of Behavior * – Required to submit an access request (also required to be reviewed on an annual basis). The link will direct you to the current GSA Rules of Behavior; once reviewed, check the Accept button as acknowledgement that you agree to adhere to the rules of behavior. Enter the Date reviewed or completed.

Non-Disclosure – **If you checked the Contractor box, this becomes a required field**. Check the Completed box and enter the Date completed which signifies that you have reviewed/signed the NDA and given to your COTR.

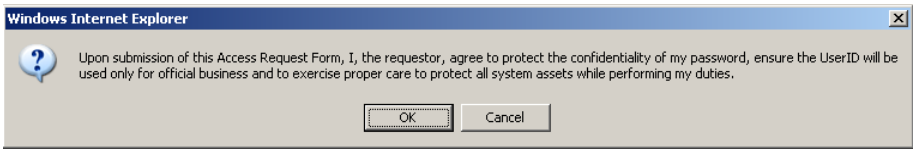
Attachments – The first attachment box allows the user to 'view' existing attachments. The second box allows the user to 'add' an attachment (i.e. email of background investigation for audit support)

Reset Button – Clears the screen and allows for reentry

Submit Button – Click the Submit button to begin the access request process.

Upon clicking the Submit button, a Confidentiality Statement will appear.

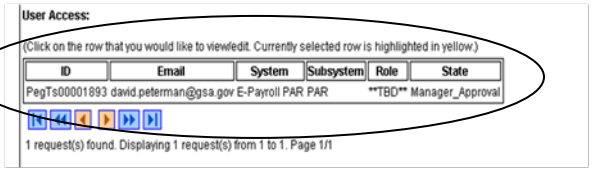
The User must "…agree to protect the confidentiality of their password, ensure the UserID will be used only for official business and to exercise proper care to protect all system assets while performing their duties." by clicking OK before the access will be submitted



Submitting the access request does not grant immediate access, it simply verifies the request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the approval workflow process.

The bottom left or upper left of the page will display if the User Profile was updated successfully and/or the Access Request was submitted successfully.

The newly submitted request will appear in the Request Queue, showing a state of Manager_Approval, meaning it has been forwarded to the specified manager for approval.



If no further action is required, select Logout, located in the upper right hand corner of the screen.

User Access Section (* denotes Required field) – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'User'.**

Action* – Click the down arrow button and select 'NEW'

System*– Click the down arrow button to select the System to which you are requesting access.

Subsystem* – Click the down arrow button to select the Subsystem to which you are requesting access.

Remarks/Comments – You may enter remarks/comments in this field, it will remain in your access record and be displayed to all managers throughout the approval process.

User Profile Section

Employee Name – First Name, Middle Initial (if applicable), and Last Name

Agency Code – Click the down arrow button to select your employing Agency

Office Symbol – Optional text field to allow entry of your Office Symbol

Phone Number – Enter 10 digit phone number

Job Title – Optional text field to allow entry of your Job Title

Contractor - Checkmark the Contractor box if applicable - This will require the user to acknowledge that a signed Non-Disclosure Agreement (NDA) is on file with the GSA contractor.

Contractor Company – Optional text field to enter the Contractor Company with which you are employed.

Manager/COTR - Select Manager from drop down menu. If your manager is not displayed, then enter your Manager/COTR email address in the next field.

Manager/COTR email - If your manager's name is not displayed in the Manager/COTR drop down menu, then enter your manager's email address. ** This access request will be sent to the email address provided (for approval), so please double-check the email address before submitting. **

User Security Verification

Initial Background Investigation – Required to submit an access request. If received, check the Completed box and enter the Date completed. This is required only once per UserID.

Full Background Investigation – Optional field. If user has received a full background investigation, check the Completed box and enter the Date completed.

GSA Rules of Behavior – Required to submit an access request (also required to be reviewed on an annual basis). The link will direct you to the current GSA Rules of Behavior; once reviewed, check the Accept button as acknowledgement that you agree to adhere to the rules of behavior. Enter the Date completed.

Non-Disclosure – If you checked the Contractor box, this becomes a required field. Check the Completed box and enter the Date completed which signifies that you have reviewed/signed the NDA and given to your COTR.

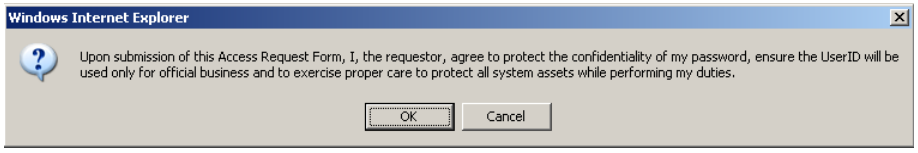
Attachments – The first attachment box allows the user to 'view' existing attachments. The second box allows the user to 'add' an attachment (i.e. email of background investigation for audit support)

Reset Button – Clears the screen and allows for reentry

Submit Button – Click the Submit button to begin the access request process.

Upon clicking the Submit button, a Confidentiality Statement will appear.

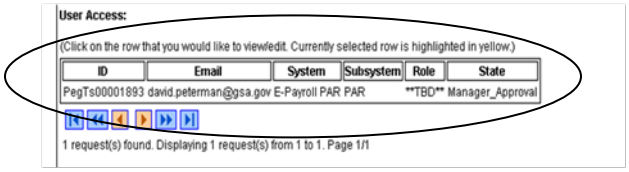
The User must "…agree to protect the confidentiality of their password, ensure the UserID will be used only for official business and to exercise proper care to protect all system assets while performing their duties." by clicking OK before the access will be submitted



Submitting the access request does not grant immediate access, it simply verifies the request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the approval workflow process (see section 15 for workflow process).

The bottom left of the page will display if the User Profile was updated successfully and/or the Access Request was submitted successfully.

The newly submitted request will appear in the Request Queue, showing a state of Manager_Approval, meaning it has been forwarded to the specified manager for approval.



If no further action is required by the Manager, select Logout, located in the upper right hand corner of the screen.

5- Manager Approval

Manager approval is a simple process that is required by security regulations for each role a user has in an application. Any new access cannot be implemented without your

approval. Additionally, if you fail to approve recertification requests, in a timely manner, for a role that a member of your staff is using, their access will be cancelled and they will have to re-apply for access.

Normally, managers are notified by email when they have a new access request or re-certifications for their staff, but this is not always the case. A manager can check at any time to see if there are pending requests that need to be processed.

An example of no notification is when a staff member submits a request under an incorrect manager and then changes their User Profile to reflect the correct manager. The correct manager will not get an email notification of the requests and must log in and go into the "Access Management" tab to process the new requests.

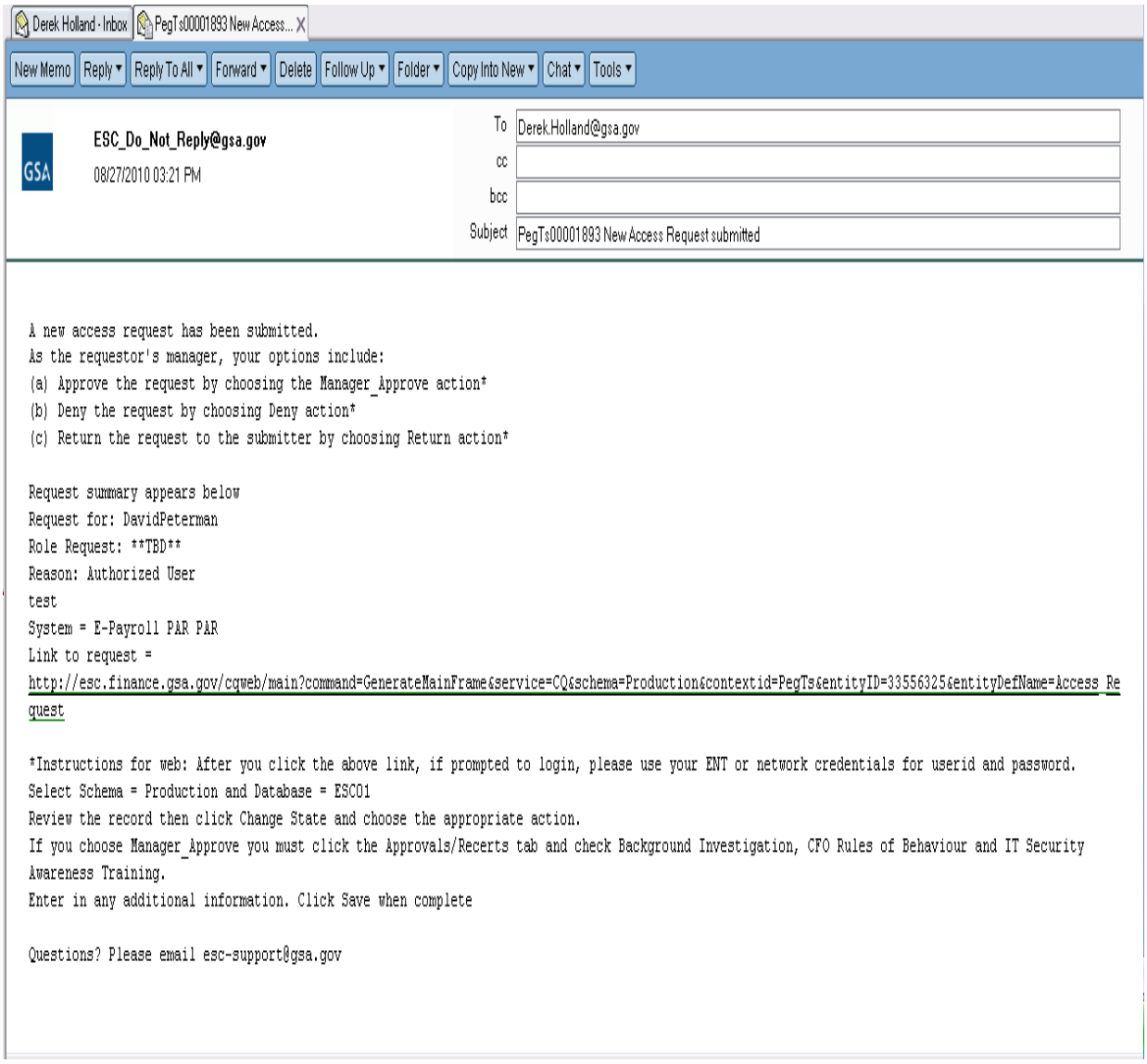
Overview - Manager Approval for New Access or Recertification

1) **Sign into EARS**
2) **Proceed to "Access Management" tab for list of any approvals that you need to do (there may be none if you have received no emails to do so)**
3) **Highlight the request you want to process.**
4) **Choose the appropriate "Action" from the pulldown list (See details below)**
5) **Click "Submit" button to process the request.**
6) **Repeat for each requests in your list.**

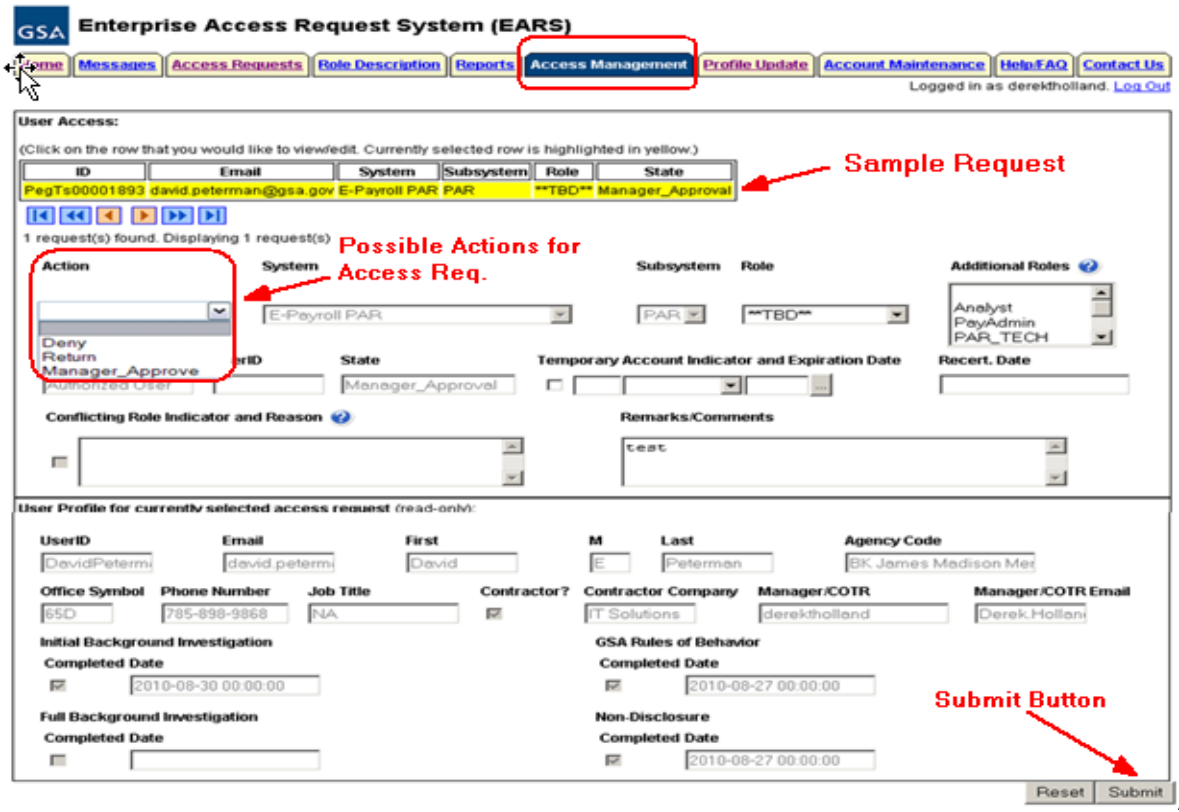
That's All you need to do !!

Detail – Manager Approval

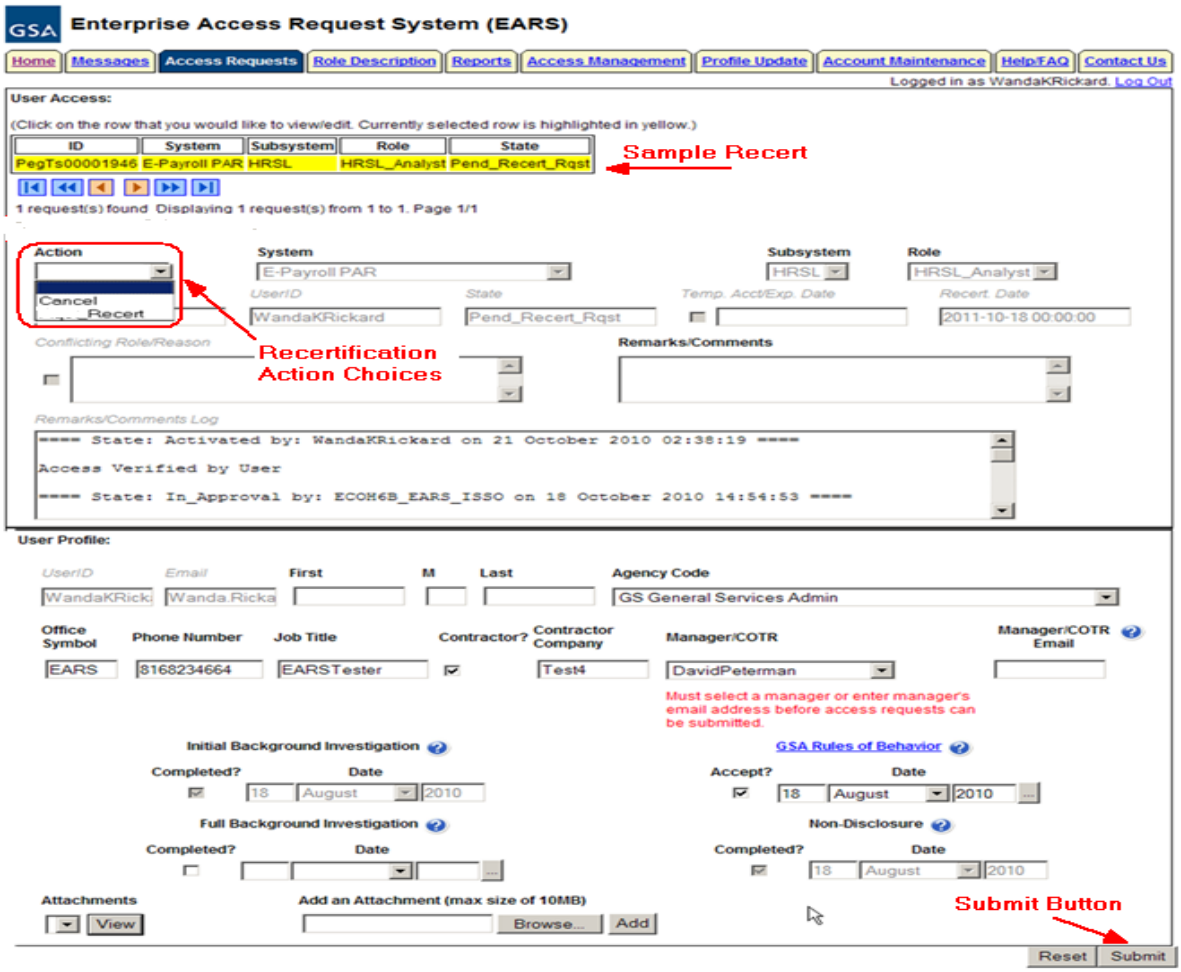
1. The Manager identified within the Access or Recertification Request will receive an email from the sender "ESC-Do Not Reply@gsa.gov" (see example below) to approve the request. A link will direct the selected Manager to the corresponding Access Request, once logged into EARS. As mentioned earlier, it is NOT necessary to have an email to initiate request approvals in EARS.



2. The manager will sign into EARS using their ENT or GSA network (EXT) login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**. Refer to the EARS User Guide (EARS Web Page Login), located in the Help/FAQ menu tab, for assistance with the login screen.
3. Once logged in, the Manager will click the **Access Management** menu tab to perform the manager approval duties. (See Below) The access request queue will display all requests that require your action. If more than 10 records exist, the arrow keys will maneuver between pages. Click on the access request you wish to approve, this will display the access request and highlight the populated request in the request queue.



Access Request Screen-Shot



Recertification Request Screen-shot

User Access Section (* denotes Required field) – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'Manager'**

Actions* - There are different actions depending on whether they are for Access Requests or Recertification Requests. See the details Below.

Access Actions The Manager can Approve (Manager_Approve), Return, or Deny by clicking the down arrow Action button and choosing the appropriate action.

Manager_Approve action will forward the access request to the System Owner (for Internal System GSA users) as long as a Role is assigned. If a role is not assigned (ex Role **TBD**) , it will forward that access request to the Liaison or System Owner.

Manager_Approve action will forward the access request to the Liaison (for External System GSA users and External Client users) as long as the role has not been assigned (ex Role **TBD**).

Return action will return the access request to the User (requestor); **comments are required.**

Deny action will cancel the access request; **comments are required.**

Recertification Actions –

Recertify – Approve the request from the user to continue in this role in this application

Cancel – Do not approve the request from the user to continue in this role in this application

Check-Recert – DO NOT USE

Role / Additional Roles Assignment* (if applicable-not normally used) – The role description document can be found under the Role Description Menu tab. To select Additional Roles, hold down the Ctrl key while clicking on the additional roles. ~~**Refer to the table below for explanation of Internal/External GSA users and External Client users and the person responsible for role assignment**~~

User Type	User Type Definition	Approval of System/Application	User to perform Role Assignment
Internal System User **(GSA user)**	1. User is a GSA employee. 2. Manager selected in Access Request is listed in the ESC Manager's table for corresponding System/Application approval path.	1. Manager approves access to System and Subsystem. 2. Manager performs Role Assignment	Manager

Internal System User - The Manager is expected to perform the role(s) assignment.

Temporary Account Indicator and Expiration Date – Used to identify an access request (all roles selected) as a temporary account. If checked, an Expiration Date is required. If populated, the system will automatically deactivate the record on the requested date; no notification will be sent to the user or manager.

Remarks/Comments – This allows the Manager to record any comments to be associated with the access request.

Remarks/Comments Log – Displays all data recorded in the Remarks/Comments text box associated with this access request as well as historical approval details.

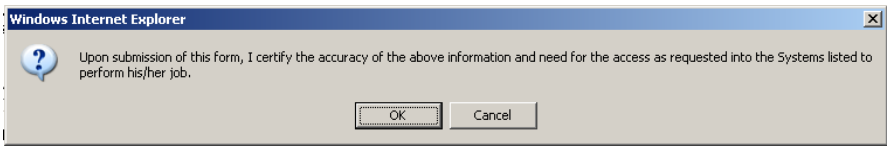
User Profile Section – The Manager is NOT allowed to make any updates to this section.

Reset Button – Clears the screen and allows for reentry

Submit Button – Click the Submit button to forward the access request to the next approver.

Upon clicking the Submit button a Confirmation Statement will appear.

The Manager must "… certify the accuracy of the above information and need for the access as requested into the Systems listed to perform his/her job." by clicking OK before the access will be submitted. This will submit and apply the Manager approval to ALL roles selected.



The Manager approving/submitting the access request **does not grant immediate access;** it simply verifies the approval request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the approval workflow process.

The access request screen will clear and display the results of the access request submission, in the upper or lower left corner of the access request screen.

Access request submission successful.

The access request screen will remove this request from the access request queue.

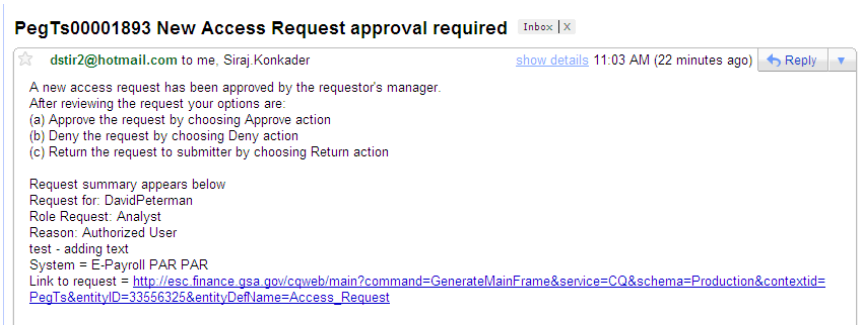
If multiple access requests require your approval, repeat steps 3 thru 7 as appropriate for the request involved..

If no further action is required by the Manager, select Logout, located in the upper right hand corner of the screen.

.

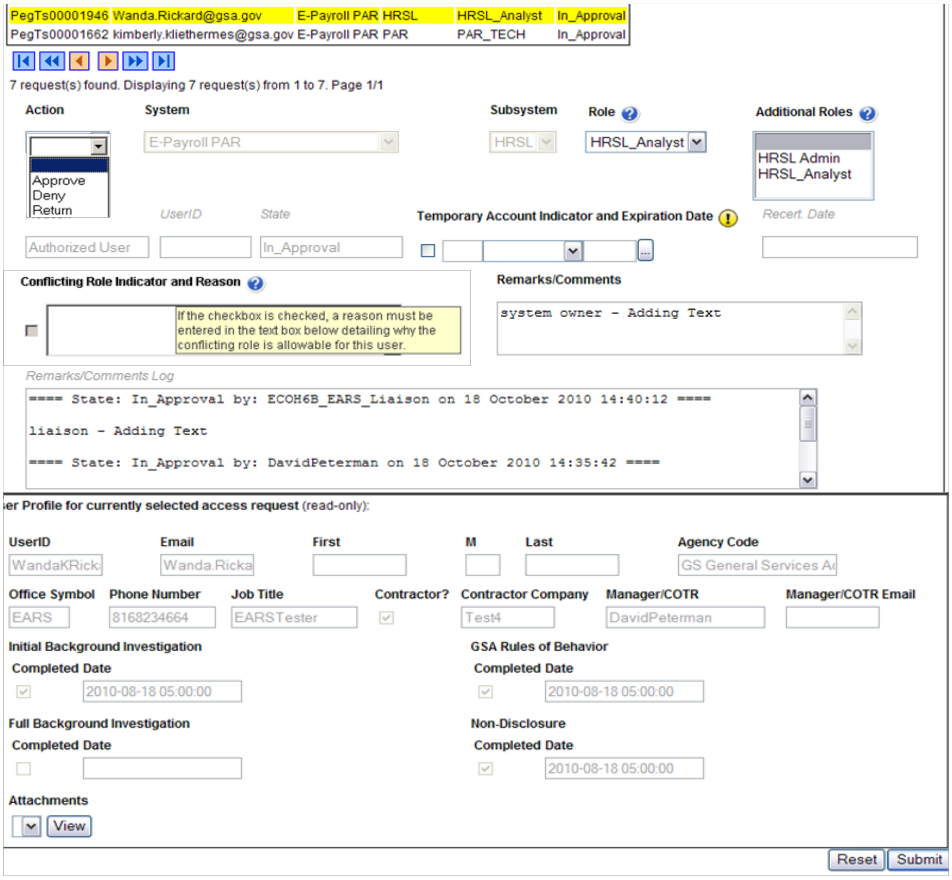
6- System Owner Approval

The System Owner will receive an email from the Manager to approve request A link in the body of the email will direct the System Owner to the corresponding Access Request.



b. The System Owner will sign into EARS using their ENT login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**.Once logged in, the System Owner will click the Access Management menu tab to perform the System Owner approval

duties. The access request queue will display all requests that require your action. If more than 10 records exists, you can use the arrow keys to maneuver between pages. Click on the access request you wish to approve; doing this will display the access request and highlight the populated request in the request queue.



e. **User Access Section (* denotes Required field)** – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'System Owner'.**

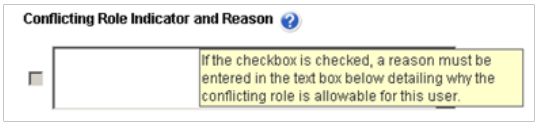
   i. **Action*** - The System Owner can Approve, Return, or Deny by clicking the down arrow Action button and choosing the appropriate action.

      1. **Approve** action will forward the access request to the Information System Security Office (ISSO).
      2. **Return** action will return the access request to the User (requestor); comments are required.
      3. **Deny** action will cancel the access request; comments are required.

   ii. **Role / Additional Roles Assignment** – This field will be populated with the role assigned by the Manager or Liaison. If unsure of the role assigned, you can review the roles under the Role Description Menu tab. The System Owner can assign Additional Roles if desired.

iii. **Temporary Account Indicator and Expiration Date –** Used to identify an access request (all roles selected) as a temporary account. If checked, an Expiration Date is required. If populated, the system will automatically deactivate the record on the requested date; no notification will be sent to the user or manager.

iv. **Conflicting Role Indicator and Reason -** If this field is checked, a reason must be entered in the text box field detailing why the conflicting roles is allowable for the identified user. *The conflicting roles identified within the role description document are set up in ESC upon the initial data load of the System/Application.*



v. **Remarks/Comments –** This allows the System Owner to record any comments to be associated with the access request.

vi. **Remarks/Comments Log –** Displays the entire data flow of the request with detailed information, including text from Remarks/Comments text box, associated with this access request as well as the historical approval details.

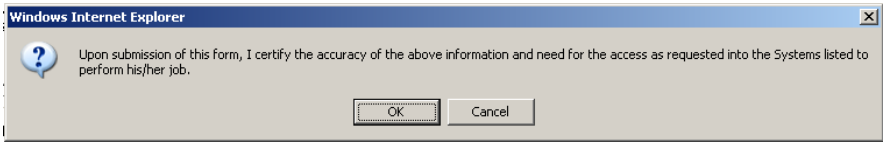
f. **User Profile Section** – The System Owner is NOT allowed to make updates to this section.

g. **Reset Button** – Clears the screen and allows for reentry

h. **Submit Button** – Click the Submit button to forward the access request to the next approver.

i. Upon clicking the Submit button a Confirmation Statement will appear.

ii. The System Owner must "… certify the accuracy of the above information and need for the access as requested into the Systems listed to perform his/her job." By clicking OK before the access will be submitted.



i. The System Owner approving/submitting the access request does not grant immediate access; it simply verifies the approval request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the approval workflow process (see section 15 for workflow process)

i. The access request screen will clear and display the results of the access request submission, in the lower left corner of the access request.

Access request submission successful.

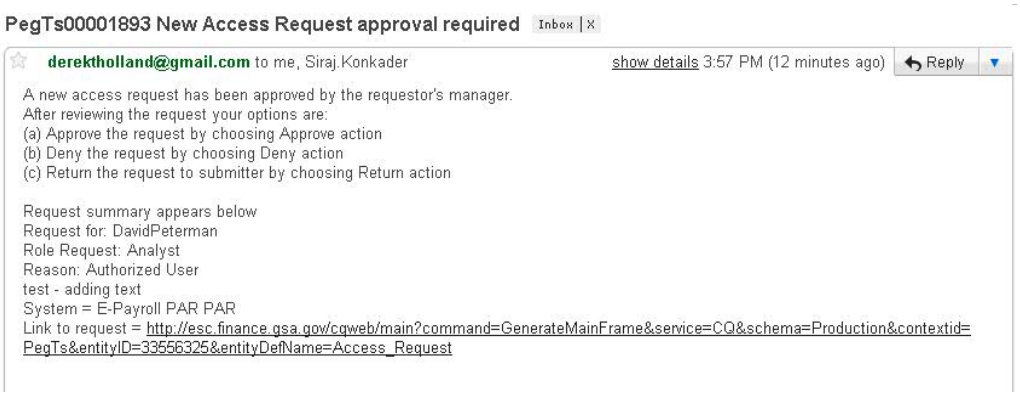
ii. Also verify the access is removed from the access request queue.

j. If multiple access requests require your approval, repeat steps 7.4 thru 7.9.

k. If no further action is required by the System Owner, select Logout, located in the upper right hand corner of the screen.

7- Information System Security Officer (ISSO) Approval

a. The ISSO will receive an email from the System Owner to approve the request. A link in the body of the email will direct the ISSO to the corresponding Access Request.


PegTs00001893 New Access Request approval required Inbox | x

derektholland@gmail.com to me, Siraj.Konkader show details 3:57 PM (12 minutes ago) Reply

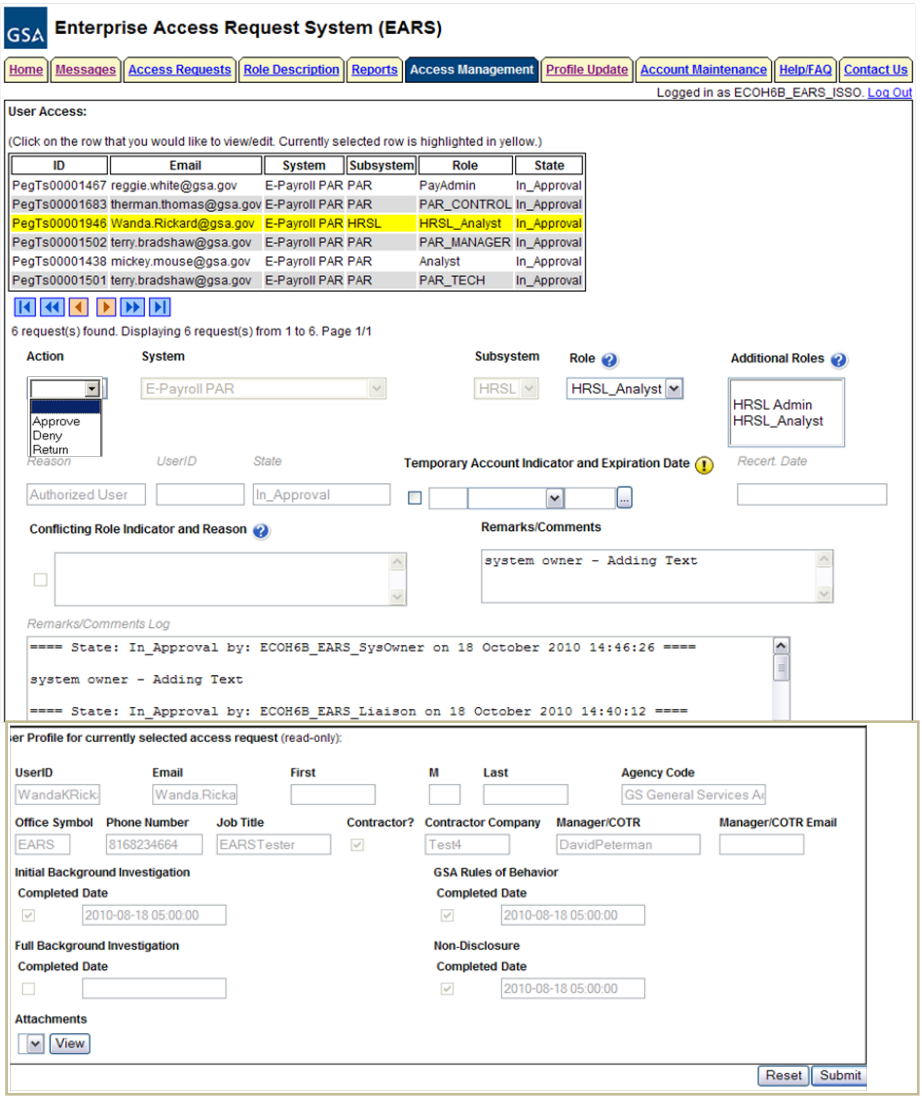
A new access request has been approved by the requestor's manager.
After reviewing the request your options are:
(a) Approve the request by choosing Approve action
(b) Deny the request by choosing Deny action
(c) Return the request to submitter by choosing Return action

Request summary appears below
Request for: DavidPeterman
Role Request: Analyst
Reason: Authorized User
test - adding text
System = E-Payroll PAR PAR
Link to request = http://esc.finance.gsa.gov/cqweb/main?command=GenerateMainFrame&service=CQ&schema=Production&contextid=PegTs&entityID=33556325&entityDefName=Access_Request

b. The ISSO will sign into EARS using their ENT login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**

c. Once logged in, the ISSO will click the Access Management menu tab to perform the ISSO approval duties. The access request queue will display all requests that require your action. If more than 10 records exists, you can use the arrow keys to maneuver between pages

d. Click on the access request (will highlight the request displayed) to populate the access request to allow approval duties.



e. User Access Section (* denotes Required field) – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'ISSO'.**

i. **Action*** - The ISSO can Approve, Return, or Deny by clicking the down arrow Action button and choosing the appropriate action.

1. **Approve** action will forward the access request to the Implementation Group.
2. **Return** action will return the access request to the User (requestor); comments are required.
3. **Deny** action will cancel the access request; comments are required.

ii. **Remarks/Comments –** This allows the ISSO to record any comments to be associated with the access request.

iii. **Remarks/Comments Log –** Displays the entire data flow of the request with detailed information, including text from Remarks/Comments text box, associated with this access request as well as the historical approval details.

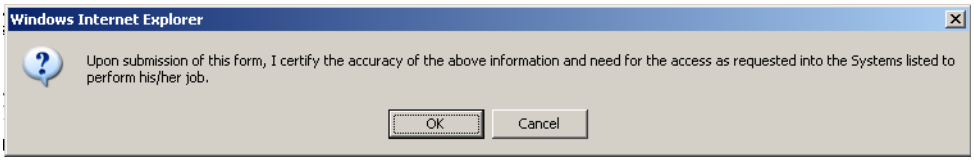
f. **User Profile Section** – The ISSO is NOT allowed to make updates to this section.

g. **Reset Button** – Clears the screen and allows for reentry

h. **Submit Button** – Click the Submit button to forward the access request to the implementation group to set up the account/database access.

i. Upon clicking the Submit button a Confirmation Statement will appear.

ii. The ISSO must "… certify the accuracy of the above information and need for the access as requested into the Systems listed to perform his/her job." By clicking OK before the access will be submitted.



i. The ISSO approving/submitting the access request does not grant immediate access; it simply verifies the approval request has been transmitted from EARS into the ESC system and will be forwarded to the next level in the workflow process (see section 15 for workflow process)

i. The access request screen will clear and display the results of the access request submission, in the lower left corner of the access request.

Access request submission successful.

ii. Also verify the access is removed from the access request queue.

j. If multiple access requests require your approval, repeat steps 8.4 thru 8.9.

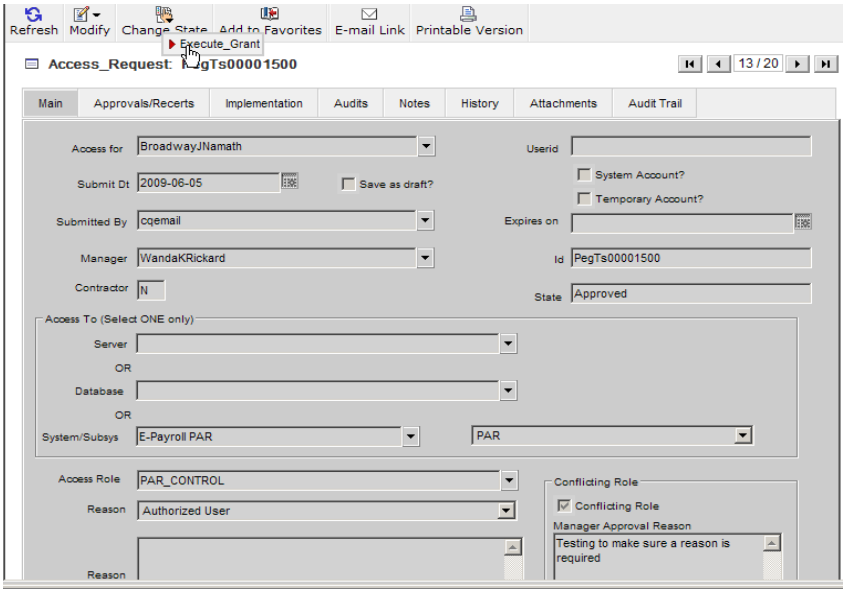
k. If no further action is required by the ISSO, select Logout, located in the upper right hand corner of the screen.

8- Implementation Group/Database Administrators (DBA) Grants Access

a. The Implementation group assigns the specified UserID to the corresponding database/role based upon the approved access request form.

b. An email notification is sent to the employee with their UserID and temporary password.

c. The DBA then loads the UserID information into the Access Request in ESC and performs "Execute Grant".

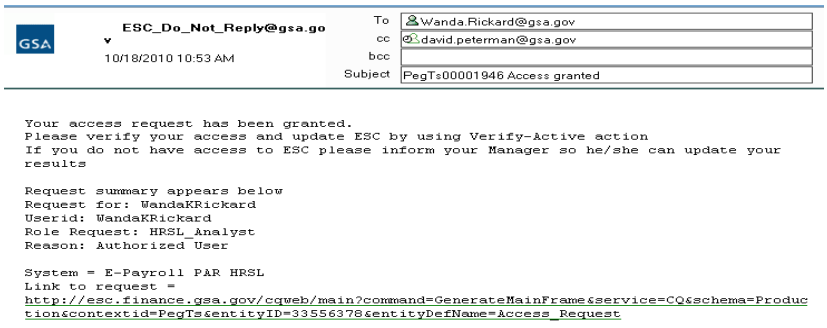


9- Account Access Verification

a. Once the employee receives their UserID and temporary password *(separate emails)*, they need to access the assigned system for which they requested access.

b. The employee will be required to change their password immediately.

c. If the employee is able to access the assigned system, he/she is required to 'Verify' their access in EARS. Use the link in the email provided by the Implementation Group.



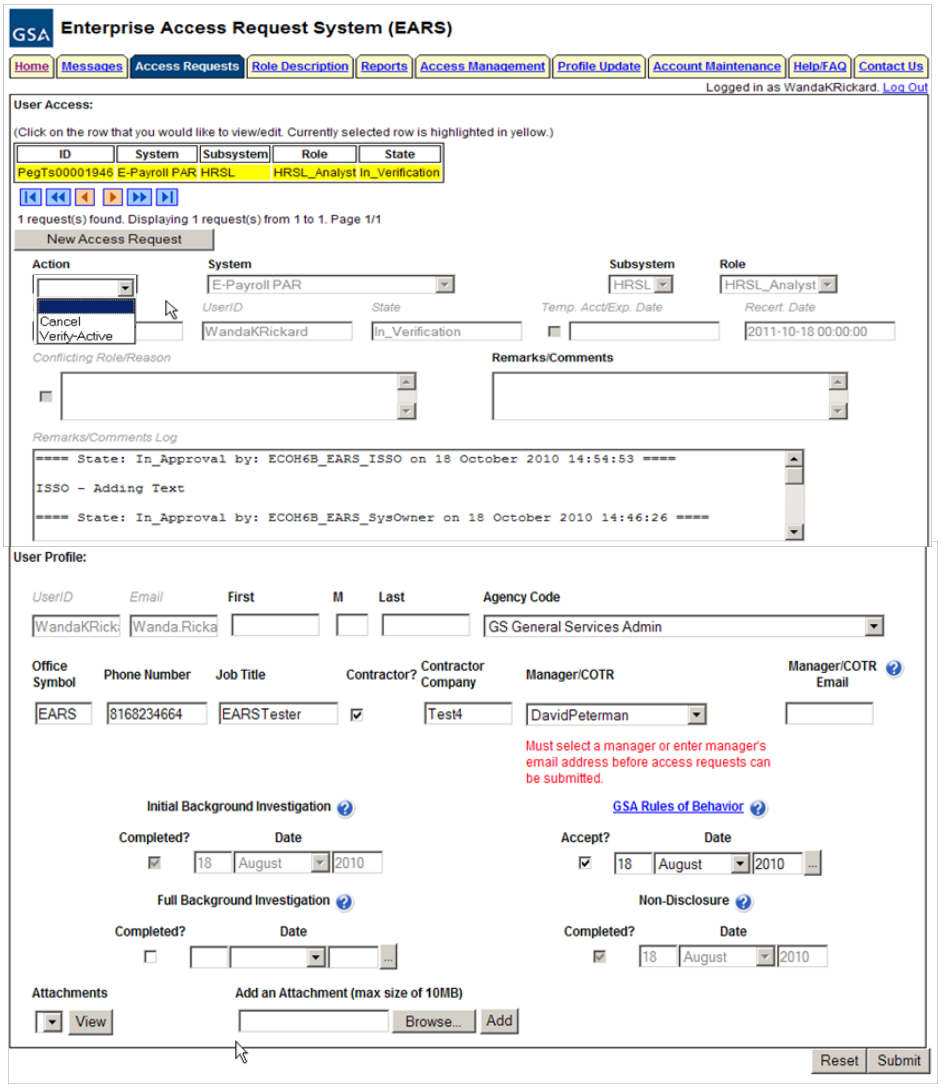
d. If the employee is unable to access the application with the specified Username/password combination, the employee should notify their manager immediately.

e. The User will sign into EARS using their ENT or GSA network (EXT) login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp.**

f. Once logged in, the User will click the Access Request menu tab to perform the Access Verification duties. The access request queue will display all requests that require your action. If more than 10 records exists, you can use the arrow keys to maneuver between pages

g. Click on the access request you wish to verify; this will display the access request and highlight the populated request in the request queue. ** Notice the UserID and

Recert Date fields are now populated. The UserID field corresponds with the UserID in the email from the Implementation Group. The Recert Date is 1 year from the date that the Implementation Group granted access to the System/Application. **



h. User Access Section (* denotes Required field) – Fields that are grayed out are unavailable. **The fields listed below are the ONLY field that are to be processed by the 'User'**

i. **Action *** - The employee can Verify_Active or Cancel by clicking the down arrow Action button and choosing the appropriate action.

1. **Verify_Active** action will Activate the specified access request.
2. **Cancel** action will generate a cancellation access request for the specified role and upon Submit will forward to the identified manager.

ii. **Remarks/Comments –** This allows the ISSO to record any comments to be associated with the access request.

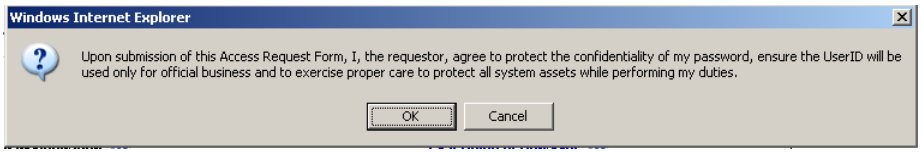
i. **User Profile Section** – All fields can be modified (with the exception of the UserID, Email, Initial Background Investigation, and Non-Disclosure)

j. **Reset Button** – Clears the screen and allows for reentry

k. **Submit Button** – Click the Submit button to finalize the access request process.

i. Upon clicking the Submit button a Confirmation Statement will appear.

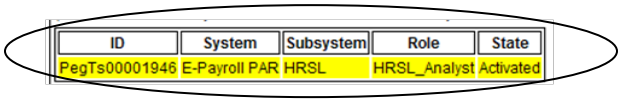
ii. The User must "… agree to protect the confidentiality of their password, ensure the UserID will be used only for official business and to exercise proper care to protect all system assets while performing their duties" by clicking OK, will complete the access request process and Activate the account.



iii. Bottom of the page will display if the Profile was updated successfully and/or the access request was submitted successfully.

Profile update successful.
Access request submission successful.

iv. The newly submitted request will appear in the Request Queue, showing a state of Activated



l. If no further action is required by the User, select Logout, located in the upper right hand corner of the screen.

10- Access Request - Modification

a. There is no longer a 'change' option on the access request form. In the event a role needs to be changed for an employee a 'new' access request will be processed for the new requested role and a 'cancellation' will be processed for the role you wish to be cancelled.

b. The access requests are not based solely on UserID's but a combination of UserID and Role per system. There is a specific access granted date and recertification date associated with that UserID and Role, therefore, for auditing purposes, a separate access request is required per requested action.

11- Access Request - Cancellation

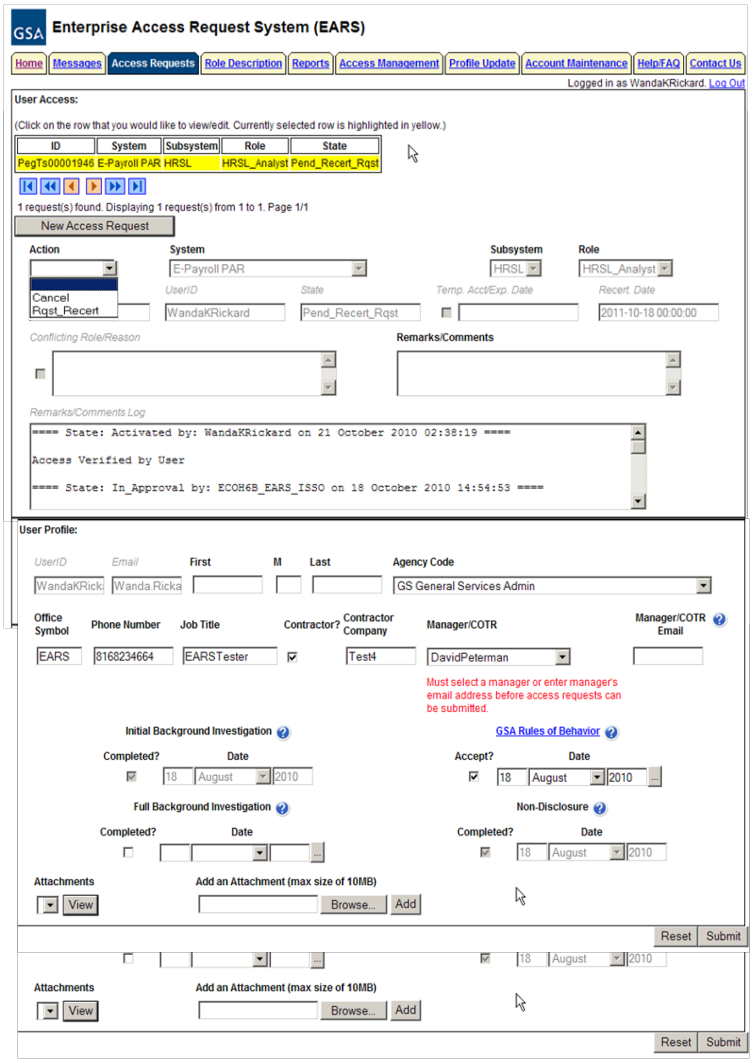
User Request to "CANCEL" an access request

a. The User can request to "CANCEL" an access request via the EARS application.

b. The User will sign into EARS using their ENT or GSA network (EXT) login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**.

c. Once logged in, the User will click the Access Request menu tab to perform the Recertification request. The access request queue will display all requests that require your action. If more than 10 records exist, you can use the arrow keys to maneuver between pages.

d. Click on the access request you wish to verify; this will display the access request and highlight the populated request in the request queue.



e. **User Access Section (* denotes Required field)** – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'User'**

i. **Action*** – The User can Cancel by clicking the down arrow Action button and choosing the appropriate action.

1. **Cancel –** This action will forward the cancellation request directly to the Implementation group.

ii. **Remarks/Comments** – You may enter remarks/comments in this field, it will remain in your access record and be displayed to all managers throughout the approval process. If Cancel action is selected, this field becomes a required field.

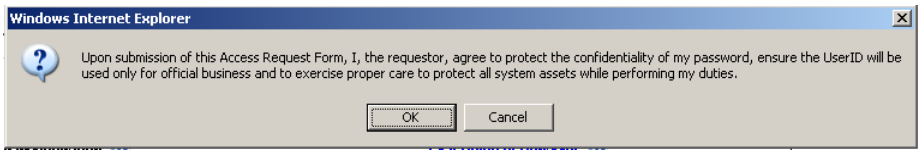
f. **User Profile Section** – All fields can be modified (with the exception of the UserID, Email, Initial Background Investigation, and Non-Disclosure)

g. **Reset Button** – Clears the screen and allows for reentry

h. **Submit Button** – Click the Submit button to start the Cancellation process.

i. Upon clicking the Submit button a Confirmation Statement will appear.

ii. The User must "… agree to protect the confidentiality of their password, ensure the UserID will be used only for official business and to exercise proper care to protect all system assets while performing their duties" by clicking OK, will complete the access request process and Activate the account.



iii. Bottom of the page will display if the Profile was updated successfully and/or the access request was submitted successfully.

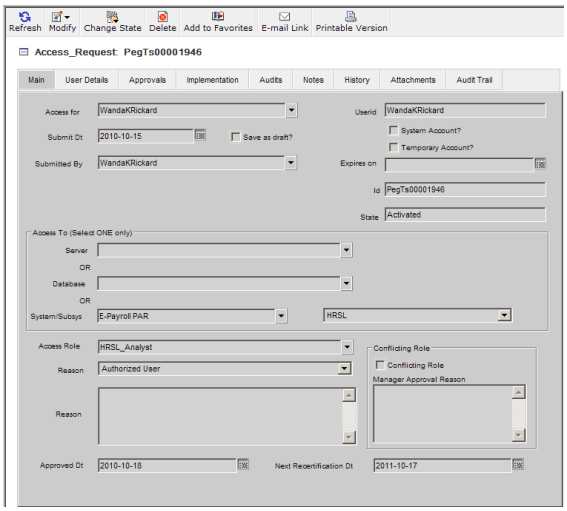
Profile update successful.
Access request submission successful.

i. If no further action is required by the User, select Logout, located in the upper right hand corner of the screen.

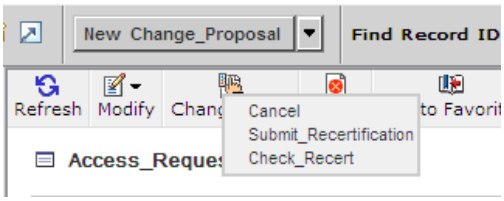
Manager, Liaison, System Owner, or ISSO Request to "CANCEL" an access request

4.1. The Manager, System Owner, or ISSO will sign into ESC using their ENT windows network username/password combination … http://esc.finance.gsa.gov/cqweb/login

4.2. Perform a search for the appropriate employee and access record within the selected Database.



4.2.1. Once the employee record is displayed, the manager, system owner, or ISSO will click on Change State, and then select 'Cancel'. Notes are required to be added as to why the account is being cancelled.



4.2.2. The Manager, Liaison, System Owner, or ISSO must 'Save' the record to start the cancellation process.

4.2.3. Once the cancellation record has been saved the action request is forwarded directly to the Implementation Group for access removal. Once the access is removed, an email is generated to the manager to verify the cancellation. The employee will never receive direct communication that the account was cancelled.

12- Access Request - Annual Recertification

a. One of the benefits of the implementation of EARS/ESC is the automation of the recertification process. Once the Implementation group grants access, the Recertification Date (1 year from the Approved Date) is populated.

b. The workflow for the Recertification Process is as follows:

   i. The User will initiate the Rqst_Recert.

   ii. The Manager identified within the User Profile section of the Access Request will Approve the request for recertification. At this time, this level of approval satisfies the access request recertification requirements; therefore, no further approval levels are required

c. Thirty days out from the recertification date, the user will receive an email from "ESC_Do_Not_Reply@gsa.gov" stating it is time to recertify the specified role(s). Additional email notifications will be sent at two weeks prior and one week prior if the access request has not been recertified.

Subject: PegTs00001893 Access Request requires recertification.

Access request for the user listed below requires recertification.
Please recertify by signing in to ESC and selecting the Recertify action*
If you do not recertify within 7 days of this notice, the account will be automatically cancelled
If you are no longer have the authority to certify access, please forward this email to the user's new manager or to the user
User: DavidPeterman
Userid: PeterWomackMan
Role: Analyst
System = E-Payroll PAR PAR
Link to request =
http://esc.finance.gsa.gov/cqweb/main?command=GenerateMainFrame&service=CQ&schema=Production&contextid=PegTs&entityID=33556325&entityDefName=Access_Request

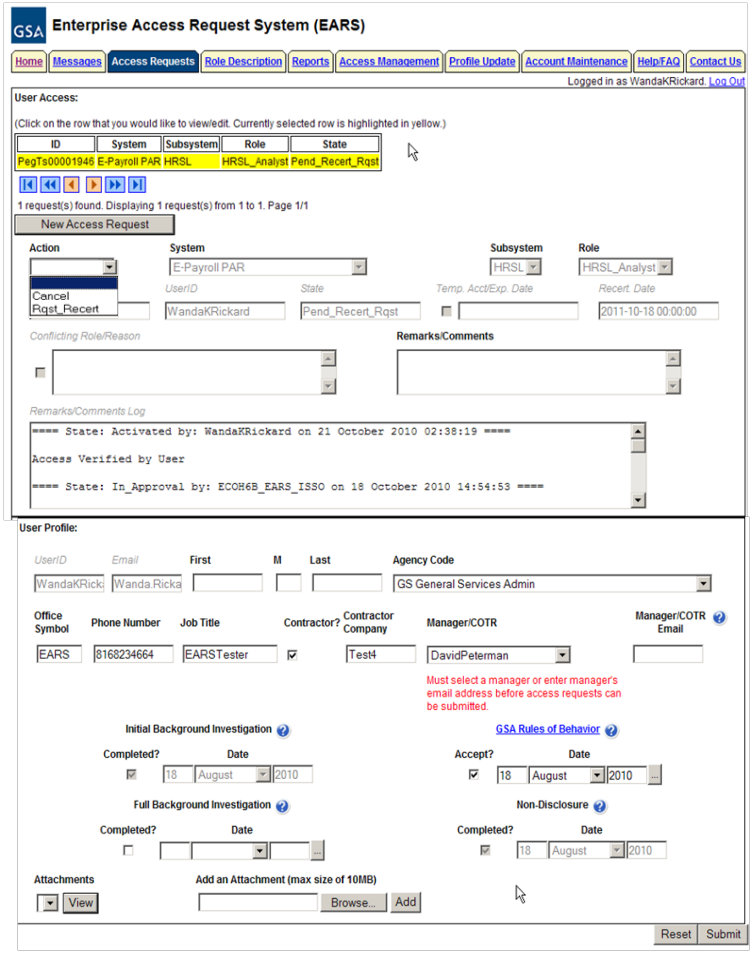
*Instructions for web: After you click the above link, if prompted to login, please use your ENT or network credentials for userid and password.
Select Schema = Production and Database = ESC01
Review the record then click Change State and choose the appropriate action.
Enter in any additional information. Click Save when complete

Questions? Please email esc-support@gsa.gov

d. The User will sign into EARS using their ENT or GSA network (EXT) login credentials via **https://ears.ocfo.gsa.gov/ears/faces/home.jsp**. Refer to the EARS User Guide (EARS Web Page Login), located in the Help/FAQ menu tab, for assistance with the login screen.

e. Once logged in, the User will click the Access Request menu tab to perform the Recertification request. The access request queue will display all requests that require your action. If more than 10 records exist, you can use the arrow keys to maneuver between pages.

f. Click on the access request you wish to verify; this will display the access request and highlight the populated request in the request queue.



g. **User Access Section (* denotes Required field)** – Fields that are grayed out are unavailable. **The fields listed below are the ONLY fields that are to be processed by the 'User'**

   i. **Action*** – The User can Request Recertification (Rqst_Recert) or Cancel by clicking the down arrow Action button and choosing the appropriate action.

      1. **Rqst_Recert –** This action will forward the recertification request to the specified manager, identified in the User Profile section of the access request.
      2. **Cancel –** This action will forward the cancellation request directly to the Implementation Group.

   ii. **Remarks/Comments** – You may enter remarks/comments in this field, it will remain in your access record and be displayed to all managers throughout the approval process. If Cancel action is selected, this field becomes a required field.

h. **User Profile Section** – All fields can be modified (with the exception of the UserID, Email, Initial Background Investigation, and Non-Disclosure) **** Please verify the Manager listed is your current manager, this is the person used to verify your access to the system/application is still required/authorized ****

   i. The user will be required to acknowledge that they reviewed and agree to adhere to the GSA Rules of Behavior (link provided) by placing a checkmark in the Accept? box and entering the date they reviewed the document. This is associated with the access requests maintained in the EARS/ESC system.

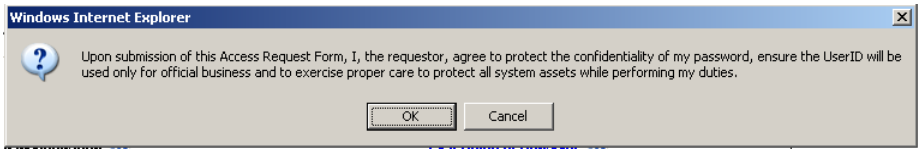
      1. This is required if the current system date is greater than 365 days from the last date reviewed.
      2. This section is independent from the GSA Rules of Behavior email that the OCIO requires GSA employees to review on an annual basis.

i. **Reset Button** – Clears the screen and allows for reentry

j. **Submit Button** – Click the Submit button to start the Recertification process.

   i. Upon clicking the Submit button a Confirmation Statement will appear.

   ii. The User must "… agree to protect the confidentiality of their password, ensure the UserID will be used only for official business and to exercise proper care to protect all system assets while performing their duties" by clicking OK, will complete the access request process and Activate the account.



   iii. Bottom of the page will display if the Profile was updated successfully and/or the access request was submitted successfully.

Profile update successful.
Access request submission successful.

4.3. If no further action is required by the User, select Logout, located in the upper right hand corner of the screen.

13- Menu Tab/Pages under construction

a. **Messages** - This page will display access request records that require action based on account logged in (i.e. employee access verification, manager access request approvals, annual recertifications,etc.)

b. **Reports** – This page will contain an Individual User Report, User Access Request Management Report, and an ESC Access Activity Report (available to ISSO only). Each report will contain various searchable criteria to produce a customized report.

c. **Account Maintenance** – This page will allow management groups to assign temporary alternate manager(s) for a specified period of time. Also allows System Owners to assign managers to a management group.

14-Access Request Workflow Process

a. "NEW" Access Requests – Established ENT~~/EXT Account~~

New User

- EARS Login (ENT ~~or EXT login credentials)~~
- Select Access Requests Menu Tab
- Complete 'NEW' Blank Access Request *(only allowed to select System, Subsystem, and Remarks)* including the User Profile section.
- Submit
  - ↳ Update to ESC
  - ↳ ESC sends email notification to identified Manager

Existing User

- EARS Login (ENT ~~or EXT login credentials)~~
- Select Access Requests Menu Tab
- Complete 'NEW' Blank Access Request *(only allowed to select System, Subsystem, and Remarks)*
- Update User Profile section if applicable
- Enter text in Remarks (i.e. reason for access)
- Submit
  - ↳ Update to ESC
  - ↳ ESC sends notification to Manager

Manager (Internal System User (GSA User))

- EARS Login (ENT login credentials)
- Select Access Management Menu Tab
- Select Approve, Return or Deny as Action
- If Approve action, then assign/select Role(s)

- Submit - Approve
  - ↳ Update to ESC
  - ↳ ESC sends notification to System Owner
- Submit - Return
  - ↳ Update to ESC
  - ↳ ESC sends notification to User
- Submit - Deny
  - ↳ Update to ESC
  - ↳ ESC sends notification to User

Manager (External System User (GSA User) and External Client User (Non-GSA User))

- **EARS Login (ENT or EXT login credentials)**
- **Select Access Management Menu Tab**
- **Select Approve , Return, or Deny as Action**
- **Leave the Role as ***TBD***, if you are sure of the role to be assigned, then enter it in the Remarks section of the access request .The Liaison will assign the role(s)**
- **Submit – Approve**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to Liaison**
- **Submit - Return**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to User**
- **Submit - Deny**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to User**

Liaison for (External System User (GSA User) and External Client User (Non-GSA User))

- **EARS Login (ENT login credentials)**
- **Select Access Management Menu Tab**
- **Any Access Request submitted without an Assigned Role; the role will need to be assigned to the Liaison**
- **Select Approve, Return, or Deny as Action**
- **If Approve, then select Role(s)**
- **Submit - Approve**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to System Owner**
- **Submit - Return**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to User**
- **Submit - Deny**
  - **↳ Update to ESC**
  - **↳ ESC sends notification to Manager and User**

System Owner

- EARS Login (ENT login credentials)

- Select Access Management Menu Tab
- Select Approve, Return or Deny as Action
- If role(s) is a conflicting role, then System Owner will be required to provide comments as to why the conflicting role(s) are being required.
- Submit - Approve
  ↳ Update to ESC
  ↳ ESC sends notification to ISSO
- Submit - Return
  ↳ Update to ESC
  ↳ ESC sends notification to User
- Submit - Deny
  ↳ Update to ESC
  ↳ ESC sends notification to Liaison (if applicable), Manager and User

ISSO

- EARS Login (ENT login credentials)
- Select Access Management Menu Tab
- Select Approve, Return, or Deny as Action
- Submit - Approve
  ↳ Update to ESC
  ↳ ESC sends notification to DBA Group
- Submit - Return
  ↳ Update to ESC
  ↳ ESC sends notification to User
- Submit - Deny
  ↳ Update to ESC
  ↳ ESC sends notification to System Owner, Liaison (if applicable), Manager and User

Implementation Group (update of UserID and Execute Grant performed in ESC)

- ESC Login
- Execute Grant or Deny
- Establish account in System Database
- Update ESC database with UserID
- Generate email notification to User and Manager that account has been established.
- A separate email is sent to the User with a temporary password

User

- EARS Login (ENT or EXT login credentials)
- Select Access Request Menu Tab
- Use UserID/Password provided to access each System/Application with assigned role.
- Select Verify Active, Cancel as Action
- Submit - Approve
  ↳Update to ESC
  ↳Account is Activated

- Submit - Cancel
  - ↳ Update to ESC
  - ↳ ESC sends notification to Implementation Group

b. "CANCEL" Existing Access

Existing User

- EARS Login (ENT or EXT login credentials)
- Select Access Requests Menu Tab
- Update User Profile section if applicable
- Select "CANCEL" action for corresponding System/Role/UserID
- Enter text in Remarks (reason for cancellation)
- Submit
  - ↳ Update to ESC
  - ↳ ESC sends notification directly to the Implementation Group

Manager (Internal System User), Liaison (External System/Client User), System Owner, or ISSO

- ESC Login
- Perform employee/access record search within selected database
- Once record is displayed – Select Change State
- Select ' Cancel'
- Select Notes menu tab and enter Reason
- Click on Save
  - ↳ Update to ESC
  - ↳ ESC sends notification directly to the Implementation Group

Implementation Group

- Verify Cancel
- Remove account/accesses in selected System Database
- Update ESC database of removal
- Generate email notification to User and Manager that account has been deactivated.

c. Annual "RECERTIFICATION" of Existing Access

Existing User

- ESC sends email notification 1 month from recertification expiration date.
- ESC will send a second notification to the user 2 weeks prior to the recertification/expiration date if the access not been recertified.
- ESC will send a third notification to the user 2 weeks prior to the recertification/expiration date if the access not been recertified.
- EARS Login (ENT or EXT login credentials)

- Select Access Requests Menu Tab
- Update User Profile section if applicable
- Select Rqst_Recert or Cancel as Action
- Select Recertify action for corresponding System/Role/UserID
- Submit – Rqst_Recert
  - ↳ Update to ESC
  - ↳ ESC sends notification to Manager
- Submit - Cancel
  - ↳ Update to ESC
  - ↳ ESC sends notification directly to Implementation Group

Manager

- EARS Login (ENT or EXT login credentials)
- Select Access Management Menu
- Select Approve, Return, or Deny as Action
- Submit - Approve
  - ↳ Update to ESC
  - ↳ Account is Recertified
- Submit - Return
  - ↳ Update to ESC
  - ↳ ESC sends notification to User
- Submit - Deny
  - ↳ Update to ESC
  - ↳ ESC sends notification to User