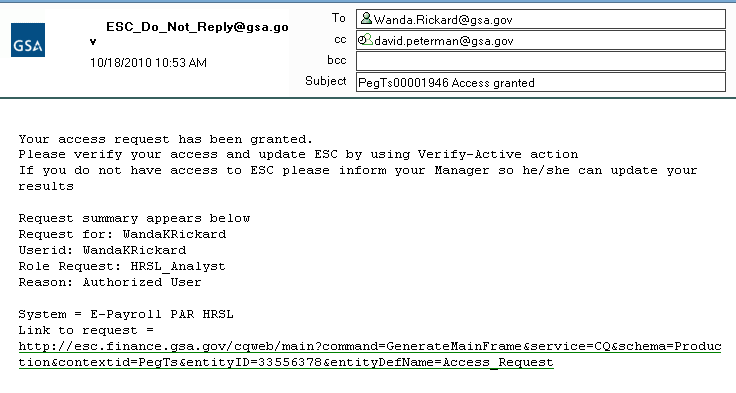
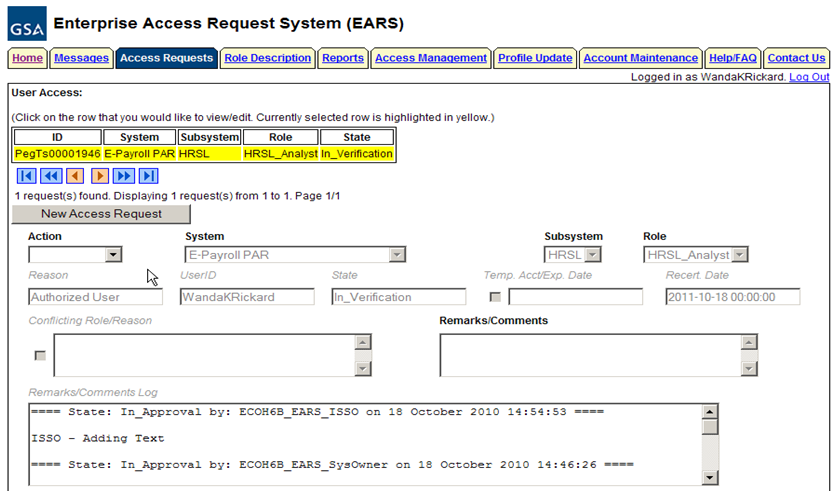
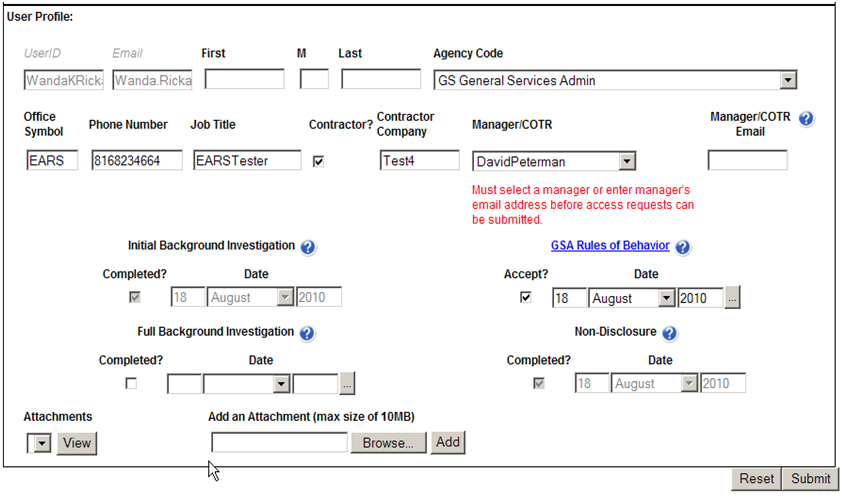
# Account Access Verification

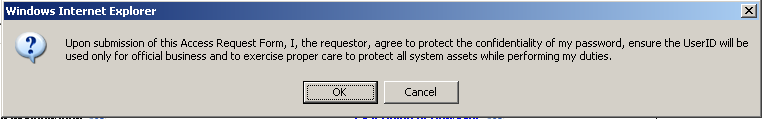
1. Once the employee receives their UserID and temporary password *(separate emails)*, they need to access the assigned system for which they requested access.
2. The employee will be required to change their password immediately.
3. If the employee is able to access the assigned system, he/she is required to ‘Verify’ their access in EARS. Use the link in the email provided by the Implementation Group.



1. If the employee is unable to access the application with the specified Username/password combination, the employee should notify their manager immediately.
2. 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>.**
3. 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
4. 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. \*\*



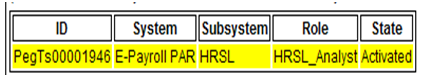
1. **User Access Section (\* denotes Required field)** – Fields that are grayed out are unavailable. **The fields listed below are the ONLY field that are to be processed by the ‘User’**
   1. **Action \*** - The employee can Verify\_Active or Cancel by clicking the down arrow Action button and choosing 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.
   2. **Remarks/Comments –** This allows the ISSO to record any comments to be associated with the access request.
2. **User Profile Section** – All fields can be modified (with the exception of the UserID, Email, Initial Background Investigation, and Non-Disclosure)
3. **Reset Button** – Clears the screen and allows for reentry
4. **Submit Button** – Click the Submit button to finalize the access request process.
   1. Upon clicking the Submit button a Confirmation Statement will appear.
   2. 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.



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



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



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