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.

1. **User Access Section** – Fields that are grayed out are unavailable.

    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.

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.

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

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
External System User (**GSA user**)	1. User is a GSA employee. 2. User is NOT directly associated with the System/Application office (employee is in a different organization location than the System/Application approving office)	1. Manager approves access to System and Subsystem ONLY. 2. Leave the Role as ***TBD ***, this will flow the access request to the Liaison for approval	Liaison
External Client User (**non-GSA user**)	1. User is NOT a GSA employee.	1. Manager approves access to System and Subsystem ONLY. 2. Leave the Role as **TBD***, this will flow the access request to the Liaison for approval	Liaison

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

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.

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

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.

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

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.

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.

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.

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.

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.

2. **User Profile Section** – Fields that are grayed out are unavailable

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

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

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

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

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

   2.6. Phone Number* – Enter 10 digit phone number

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

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.

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

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.

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. **

2.12. User Security Verification

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.

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.

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.

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.

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)

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

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

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. 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).

3.1.1. 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.
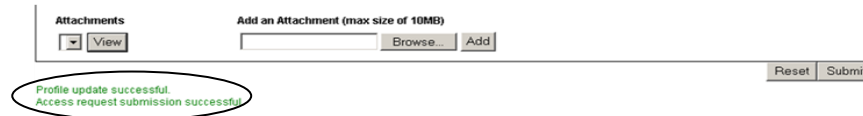
3.1.2. The newly submitted request will appear or disappear in the Request Queue based on the Access Request state.

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

3.1.4. 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.

3.1.5. 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.