# EARS Access Request Workflow Process

1. **“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

1. **“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.

1. **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