



US Army Corps  
of Engineers

---

USERS MANUAL

# **ACCESS REQUEST MANAGEMENT SYSTEM (ARMS)**

07 NOV 2003

CEEMS  
CEEMS  
CEEMS

Corps of Engineers Financial Management System

# **ACCESS REQUEST MANAGEMENT SYSTEM (ARMS)**

Corps of Engineers Financial Management System  
(CEFMS)

Users Manual  
(UM)

# ACCESS REQUEST MANAGEMENT SYSTEM (ARMS)

## TABLE OF CONTENTS

|                                                                                     | <u>PAGE</u>    |
|-------------------------------------------------------------------------------------|----------------|
| <b>SECTION 1 ADD AND CHANGE CEFMS ACCESS TO<br/>A REMOTE SITE .....</b>             | <b>1-1</b>     |
| <b>1.1 CEFMS Access Request And Approval<br/>        Screen .....</b>               | <b>1-3</b>     |
| <b>1.1.1 Entering A CEFMS Access Request.....</b>                                   | <b>1-3</b>     |
| <b>1.1.2 Approving A Completed CEFMS Access<br/>                Request .....</b>   | <b>1-4</b>     |
| <b>1.1.3 Applying An Approved CEFMS Access<br/>                Request .....</b>    | <b>1-5</b>     |
| <b>1.1.4 Access Request Summary .....</b>                                           | <b>1-7</b>     |
| <b>1.2 Request Status Code .....</b>                                                | <b>1-8</b>     |
| <b>1.3 Access Request Organization Correlation</b>                                  | <b>1-10</b>    |
| <br><b>SECTION 2 ACCESS CONTROL REQUEST MANAGEMENT<br/>SYSTEM (ARMS) .....</b>      | <br><b>2-1</b> |
| <br><b>SECTION 3 ACCESS DEACTIVATION IN ARMS .....</b>                              | <br><b>3-1</b> |
| <b>3.1 Local Access Deactivation .....</b>                                          | <b>3-2</b>     |
| <b>3.2 Request To Deactivate A Limited Number<br/>        Of Remote Sites .....</b> | <b>3-5</b>     |

**ACCESS REQUEST MANAGEMENT SYSTEM (ARMS)**

**TABLE OF CONTENTS (Cont.)**

**APPENDICES**

|                                                                                        | <b><u>PAGE</u></b> |
|----------------------------------------------------------------------------------------|--------------------|
| <b>A - CEFMS Access Request Life Cycle .....</b>                                       | <b>A-1</b>         |
| <b>B - How To Query The Database For ARMS<br/>Request Data .....</b>                   | <b>B-1</b>         |
| <b>C - CEFMS Access Request Management System (ARMS)<br/>Email Notifications .....</b> | <b>C-1</b>         |

# CEFMS ACCESS REQUEST

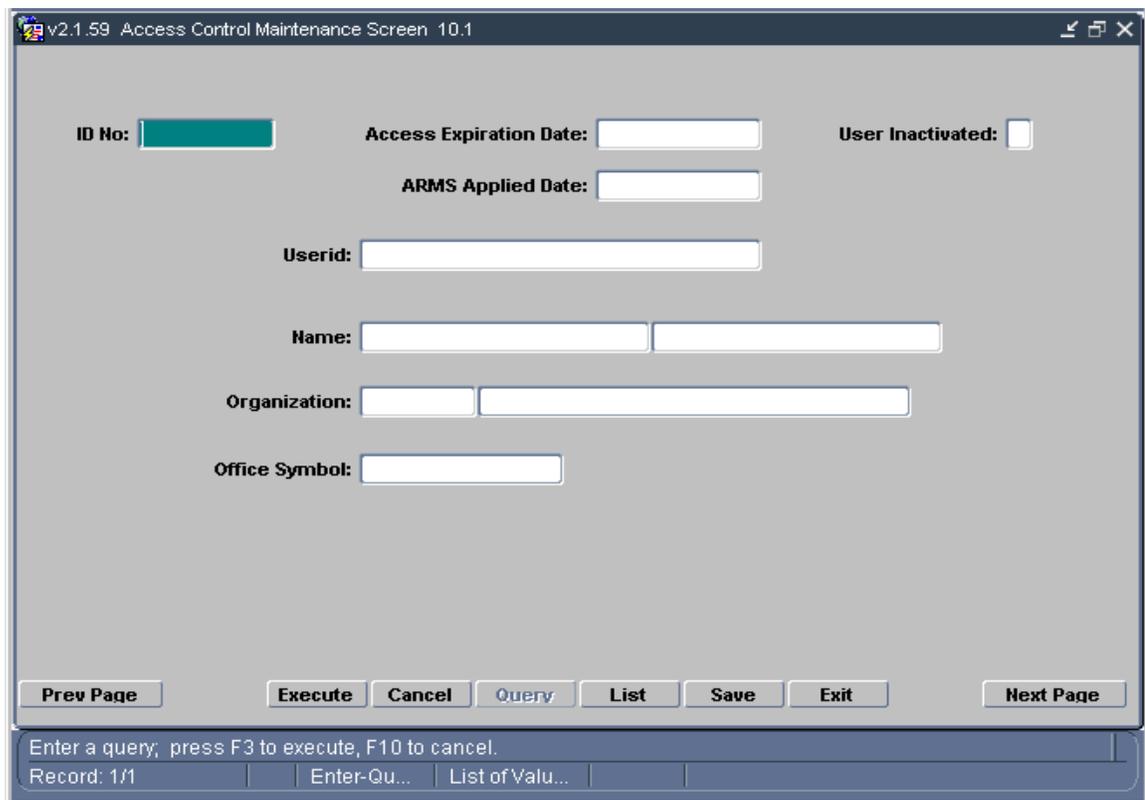
## OVERVIEW

---

This document addresses the procedures used to request access to a Corps of Engineers Financial Management System (CEFMS) site and to make modifications to a current user's access. These two scenarios are addressed on the pages that follow. Reference Appendix A for a diagram of the CEFMS Access Request Life Cycle.

## SECTION 1. ADD AND CHANGE CEFMS ACCESS TO A REMOTE SITE

CEFMS **logon** access to a site is initiated via the Website. If the site grants logon access, a skeleton record is **inserted** in Access Control. Reference the Access Control Maintenance Screen (10.1) that follows.



The screenshot displays the 'Access Control Maintenance Screen 10.1' with the following fields and controls:

- ID No:** A text input field with a green background.
- Access Expiration Date:** A date input field.
- User Inactivated:** A checkbox.
- ARMS Applied Date:** A date input field.
- Userid:** A text input field.
- Name:** Two adjacent text input fields.
- Organization:** Two adjacent text input fields.
- Office Symbol:** A text input field.

At the bottom, there is a row of buttons: **Prev Page**, **Execute**, **Cancel**, **Query**, **List**, **Save**, **Exit**, and **Next Page**. Below the buttons is a status bar with the text: 'Enter a query; press F3 to execute, F10 to cancel.' and 'Record: 1/1 | Enter-Qu... | List of Valu...'.

**Access\_approval\_date** is the date of the most recent approved and applied request. This date is utilized to compile the 12-month expiration of an access request.

The user enters the requested CEFMS accesses in the CEFMS Access Request and Approval Screen (10.16.5) that follows.

**NOTE:** The following files were modified: accreqst.fmb (while out on a different PR), accsctrl.fmb (10.1), and rolectrl.fmb (10.16), so that when screens 10.1 and 10.16 are called from 10.16.5 they automatically query-up the id\_no of the request displayed on Screen 10.16.5. If no ARMS request is queried by 10.16.5 when querying 10.1 or 10.16, the id\_no of the user of 10.16.5 is queried by 10.1 and 10.16.

## **1.1 CEFMS ACCESS REQUEST AND APPROVAL SCREEN**

The CEFMS Access Request and Approval Screen (Screen 10.16.5) is used to set both ACCESS\_CONTROL indicators and to grant and revoke CEFMS Application Roles.

Changes to CEFMS Access are applied by completing the following three steps:

1. Enter and complete requested changes to a user's current CEFMS Access
2. Approve a completed CEFMS Access Request
3. Apply completed and approved CEFMS Request.

This process starts by generating a new request sequence. This CEFMS Request Sequence is marked as COMPLETED by the requestor. After the request has been completed, an approving official reviews the request and approves the request. An applying official then applies the request. The approving official has the option to reject the request and the applying official has the option to refuse to apply the request.

### **1.1.1 ENTERING A CEFMS ACCESS REQUEST**

To generate a new request sequence, select the <New\_Req\_Seq> option. For Local request, CEFMS access will appear under the 'Access Requested' column of Screen 10.16.5.

1. To add new CEFMS ACCESS:
  - Highlight the desired CEFMS Access under the 'Available Access' column.
  - Select <Request>.
2. To remove (revoke) currently held CEFMS Access:
  - Highlight the desired CEFMS Access under the 'Access Requested' column.
  - Select <Revoke>.

3. Continue to grant and revoke the CEFMS access desired. The user may <Save> the request at any time to exit this screen before completing the request. Once the access requested is correct, select <Complete>, then <Save>.
4. The user may cancel this request sequence at any time (before it is applied) by selecting <Cancel Req>.
5. The emp\_email\_addr can not be nulled out if populated, but can be modified. This was modified to ensure no one removes an email address without inserting a new one. The user can enter the email address into 10.16.5. It uses the same table because the email address is stored only once in the system.

The user can enter a new request although he does not have an email set up at the time. When the user clicks <Complete> or <Save>, a message appears requesting the user to enter an email address and complete/save the transaction in Screen 10.16.5. The user does not have to access Screen 10.131 to enter the email; it can be entered in Screen 10.16.5. The email address is stored in the employee table record.

The logic in Screen 10.165 is modified so the requestor can not mark a request as 'Complete' until the email address on the screen is populated. An Applier may create a request and populate the email address for a user.

### 1.1.2 APPROVING A COMPLETED CEFMS ACCESS REQUEST

The approving official **must** have the ACC\_MAINT\_MGR application role granted to his user ID.

1. Query CEFMS Access Requests searching for the completed requests desired.
2. Review the list of requested CEFMS access under the 'Access Requested' column. This column shows how the CEFMS access will appear after this request sequence is applied.
3. Once the approving official is satisfied with the requests and justifications, select <Approve>. If not satisfied with the request, the approving official has the option to reject the request by selecting <Reject>.

4. Once the user has selected <Approve> or <Reject>, he will be asked to enter the justification. This is optional when approving a request, but mandatory if rejecting a request.
5. Select <Save> to commit the request approval.

### 1.1.3 APPLYING AN APPROVED CEFMS ACCESS REQUEST

The applying official **must** have the ACCS\_MAINT application role granted to his user ID. **A user cannot serve as approver and applier.**

1. Query CEFMS Access Requests searching for the approved request.
2. Review the list of requested CEFMS access under the 'Access Requested' column.
3. Once the applying official is satisfied with the requests and justifications, select <Apply>. If not satisfied with the request, the applying official has the option to refuse to apply this request by selecting <Refuse>.
4. If the applying official selects <Refuse>, he will be asked to enter the justification for refusing this request. The requesting user will be notified by e-mail. The rejected request can be modified to satisfy the concerns of the applier.
5. If the applying official selects <Apply>, the Access\_Control Electronic Signature will be verified and the request sequence marked to be applied.
6. Select <Save> to commit and apply the access request.
7. The request should now be applied and the sequence completed.

v2.1.8 Role Query Screen 10.16

ID No:       Userid:       User Status:

Name:             Access Expiration:

Report Access Level:       Report View Level:       Budget Formulation Level:       RGA Mail Code:

**Available Roles**

|                          |
|--------------------------|
| ACCS_MAINT               |
| ACC_MAINT_MGR            |
| APPMS_HANDRECEIPT        |
| APPMS_PBO                |
| APPMS_RCS                |
| APPROP_EXP_AUTH_APPROVAL |
| APPROP_EXP_AUTH_ESTIMATE |
| ASSET_BATCH              |
| AUTH_COLLECTOR           |
| BILLING_AUTH             |
| BUDGET_APPROVAL          |
| BUDGET_CONTROL           |
| CC_CERT_AUTH             |
| CERT_GOV_TRNG_BILL       |

**Granted Roles**

|                      |
|----------------------|
| ACCRUAL_AUTH         |
| ACPERS_AUTH          |
| AGENCY_RATE_AUTH     |
| APPRV_WHSE_ADJ       |
| ASSET_MGR_AUTHORITY  |
| AUTH_RECEIVER        |
| CARD_APPR_AUTH       |
| CEFMS_USER           |
| COST_TRNS            |
| CO_TECH_APP          |
| DM_RESOLVE_ESIG_AUTH |
| GO_ACCEPT            |
| INCOME_TRNS          |
| JOURNAL_ENTRY_AUTH   |

Prev Page      Prev      Next      Query      List      Save      Exit      Next Page

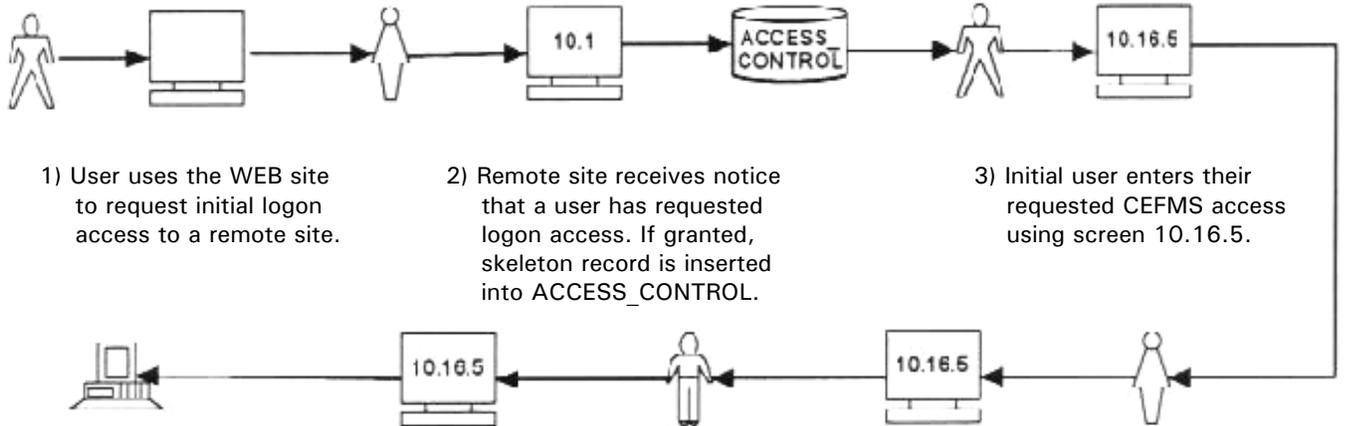
Enter unique user identification. F4 for list.

Record: 1/?

**NOTE:** Role Maintenance (Screen 10.16) is now a View Only Screen. Updates must be made through Screen 10.16.5.

### 1.1.4 ACCESS REQUEST SUMMARY

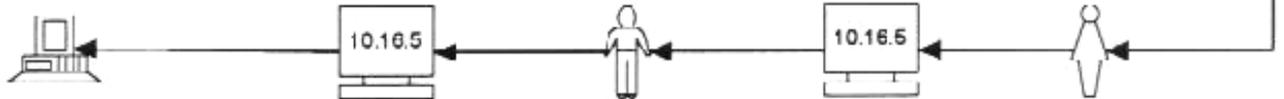
The diagram below summarizes the user request for CEFMS access to a remote site.



1) User uses the WEB site to request initial logon access to a remote site.

2) Remote site receives notice that a user has requested logon access. If granted, skeleton record is inserted into ACCESS\_CONTROL.

3) Initial user enters their requested CEFMS access using screen 10.16.5.

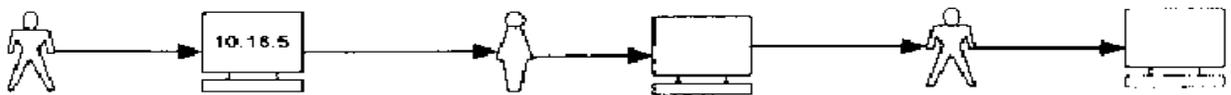


6) User now has the requested CEFMS access at the remote site.

5) Applier at the remote site applies the request and updates ACCESS\_CONTROL and grants the roles requested.

4) Approver at the remote site reviews the request and either APPROVES or REJECTS the request. If the request is rejected, the user may modify their request to satisfy the concerns of the remote site.

The diagram below provides a summary of the process to request modifications to current access at a site.



1) User generates a new Request Sequence Number by selecting the New Reg. Seq. button on 10.16.5. After the new request sequence has been generated, the user modifies their access by requesting new access or revoking their current access.

2) Approver at the site either APPROVES or REJECTS the request. User is notified of the decision via e-mail.

3) Applier at the site either Applies or Refuses to Apply the Approved request. User is notified by e-mail.

## 1.2

## REQUEST STATUS CODE

The status of each requested access is displayed in the 'Status' field. Refer to the table below for a list of valid status codes. Press F4 to obtain a pick list of status codes.

### CURRENT REQUEST\_STATUS\_CODES IN ARMS AS OF 24-OCT-2003

| STATUS | DESCRIPTION                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| -----  | -----                                                                                                                                             |
| A      | Access Request Has Been Approved By The Approving Official                                                                                        |
| AB     | Request Is Approved But Modified By Both The Approver And The Applier                                                                             |
| AM     | Approving Official Has Modified And Then Approved The Access Request                                                                              |
| AP     | Request Is Approved But Modified By The Applier                                                                                                   |
| C      | Access Request Has Been Completed By Requestor                                                                                                    |
| CM     | Access Request Has Been Completed By Requestor And Then Modified By The Approving Official                                                        |
| E      | Access Request Still Being Entered By Requestor                                                                                                   |
| NA     | Not Applicable. An id_no of the ARMS request is not on the Remote Access_Control Table. Therefore, the request was not copied to the remote site. |
| P      | Access Request Has Been Applied                                                                                                                   |
| PA     | Access Request Has Been Modified By The Approving Official And Then Applied                                                                       |
| PB     | Access Request Has Been Modified By Both The Approving And Applying Officials And Then Applied                                                    |

|    |                                                                                                                                                                                                            |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PM | Access Request Has Been Modified By The Applying Official And Then Applied                                                                                                                                 |
| PR | Remote Access Request Has Been Applied By All Requested Sites                                                                                                                                              |
| R  | Approving Official Has Rejected The Access Request                                                                                                                                                         |
| RM | Applying Official Has Refused To Apply The Request That Was Modified By The Approving Official                                                                                                             |
| RP | Applying Official Has Refused To Apply The Request                                                                                                                                                         |
| X  | Access Request Has Been Canceled                                                                                                                                                                           |
| XA | Request Was Approved And Then The Requestor Made Additional Changes So This Original Request Was Archived To Allow Historical Tracking, And A New Request Sequence Started                                 |
| XC | Request Was Completed But The Approver Modified The Completed Request So This Original Was Archived To Allow Historical Tracking, And A New Request Sequence Started                                       |
| XP | Applying Official Refused To Apply The Original Request And Then The Requestor Modified The Request So This Original Request Was Archived To Allow Historical Tracking, And A New Request Sequence Started |
| XR | Request Was Rejected By The Approving Official And Then The Requestor Modified The Request So This Original Request Was Archived To Allow Historical Tracking, And A New Request Sequence Started          |

**NOTE:** The user can double click the 'Status' field of an Access Requested to verify who requested the role or generated the request and when the request was made. If the 'Access Requested Status' column contains 'Current Role', this means the user had that role or level when the request sequence was originally generated. If the status shows something other than 'Current Role', then the role or level was requested by the request sequence.

### 1.3

### ACCESS REQUEST ORGANIZATION CORRELATION

Screen 10.16.3 controls the Organization Codes for which each Approver and Applier has authorization. The Approver and Applier need an entry for an Organization Code before they are allowed to Approve or Apply a request for that organization. Screen 10.16.3 can also be used to control if the Approver and Applier wants to receive either Instant Email Notification (generated when the request is actually Completed or Approved) or the Daily Email Notification which is generated once a day.

Screen 10.16.5 verifies if the Approver and Applier has authorization for the Organization Code of the requesting employee entered in screen 10.16.3. The edits "walk the chain". This means the edit checks to see if there is an entry for that Organization Code or an Organization Code higher up on the organization structure than the organization code entered for the requestor.

If the Approver or Applier is authorized to approve or apply for ALL organizations, an entry can be made in screen 10.16.3 that just has the Approver or Appliers ID No and the Organization Code remains NULL. A null organization code in screen 10.16.3 indicates the Approver or Applier is authorized to Approve or Apply for all organization codes.

v2.1.5 CEFMS Access Request Organization Correlation 10.16.3

| Approver or Applier ID No | Org Code | Disable Org Code Subordinates For Email Notification | Disable Instant Email Notification  | Disable Daily Email Notification    |
|---------------------------|----------|------------------------------------------------------|-------------------------------------|-------------------------------------|
| COLLR4667                 | A000000  | <input type="checkbox"/>                             | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| HUNTR6336                 | A000000  | <input type="checkbox"/>                             | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| JOHNA5664                 | A000000  | <input checked="" type="checkbox"/>                  | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| REAVD3542                 | A000000  | <input checked="" type="checkbox"/>                  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| RICHR0015                 | A000000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| ROBIQ0773                 | A000000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| TYNEP1412                 | A000000  | <input checked="" type="checkbox"/>                  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| TYNET5824                 | A000000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| COLLR4667                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |
| HUNTR6336                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |
| JOHNA5664                 | G600000  | <input checked="" type="checkbox"/>                  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| REAVD3542                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |
| RICHR0015                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |
| ROBIQ0773                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |
| TYNEP1412                 | G600000  | <input type="checkbox"/>                             | <input type="checkbox"/>            | <input type="checkbox"/>            |

Del ID No      All Orgs      All Email      All Daily

Prev Page      Prev      Next      Query      List      Save      Exit      Next Page

Enter Approver or Applier ID No

Record: 1/?      ...      List of Valu...

**NOTE:** Added 'Help' lines for the indicator columns which are accessed by double clicking on any of the three indicator check boxes. The new Org\_code\_chain\_disabled\_ind is on Screen 10.16.3 under the heading of 'Disable Org Code Subordinates For Email Notification'. By checking this box, the Approver/Applier is indicating that he does not want to receive any CRON Email concerning requests that need to be approved or applied from the Org\_code or any subordinate of that Org\_code (if checked, the logic to send the CRON Email message will NOT walk-the-chain for that Org\_code). The email will be sent if the Org\_code for the Id\_no is the explicit Org\_code indicated (e.g. if an Org\_code is entered on Screen 10.16.3 and that Org\_code has 10 subordinate Org\_codes and the check box for that Org\_code is checked. CRON Email will NOT be sent for any children of that Org\_code (subordinate Org\_codes), but will be sent if the requestor is for that Org\_code).

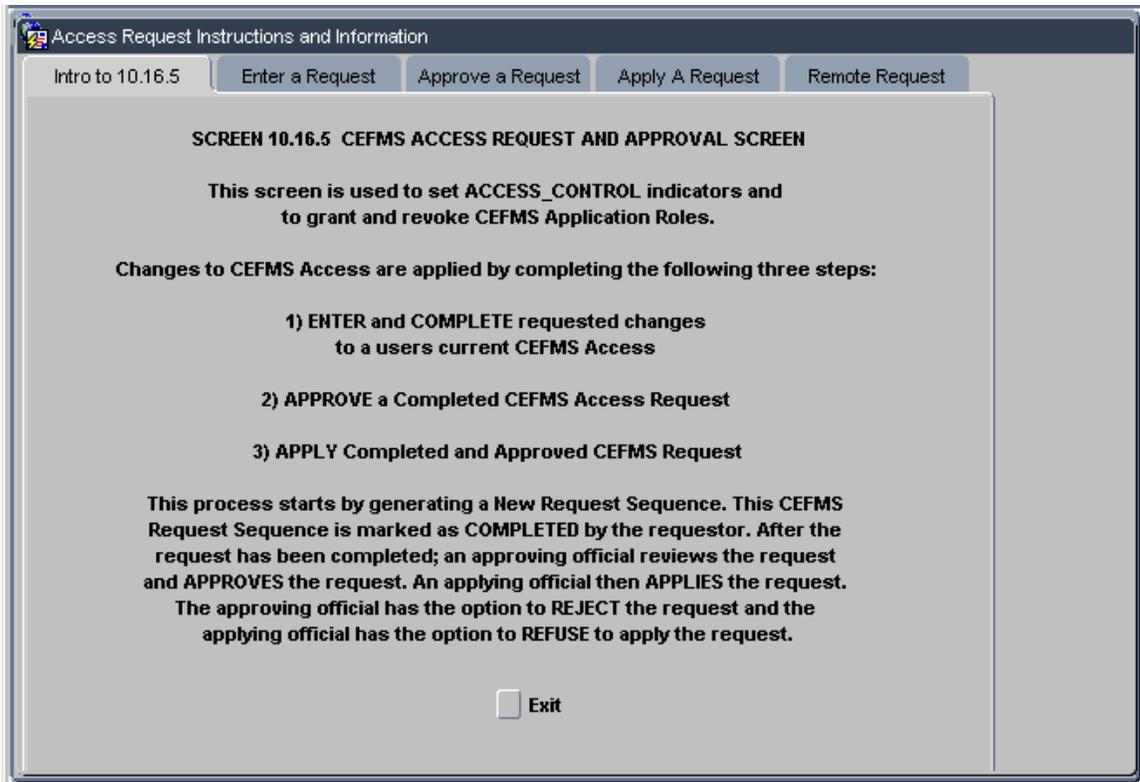
The other two indicators, 'Disable Instant Email Notification' and 'Disable Daily Email Notification', turn off the instant Email notification of the CRON notification. The instant Email notification that is generated when a request is marked as 'Complete' or

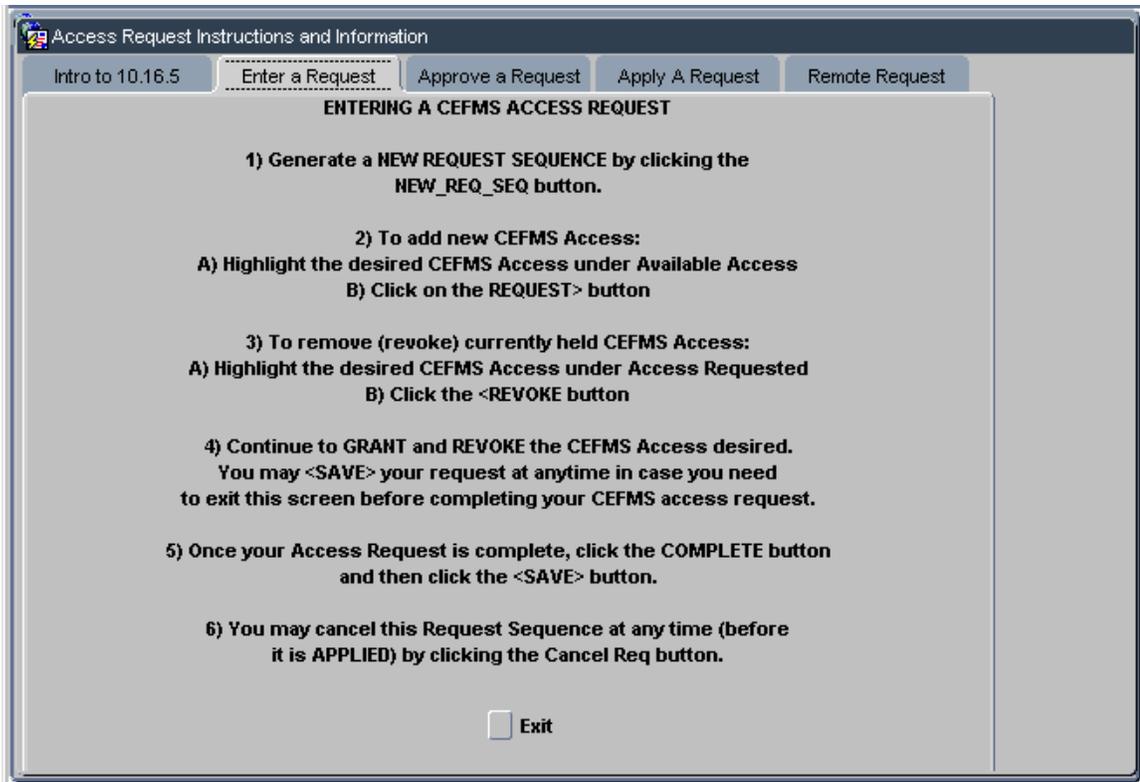
'Approved' from Screen 10.16.5 does NOT walk-the-chain for Email, but DOES walk-the-chain to determine if the Approver/Applier has authority for a particular Org\_code.

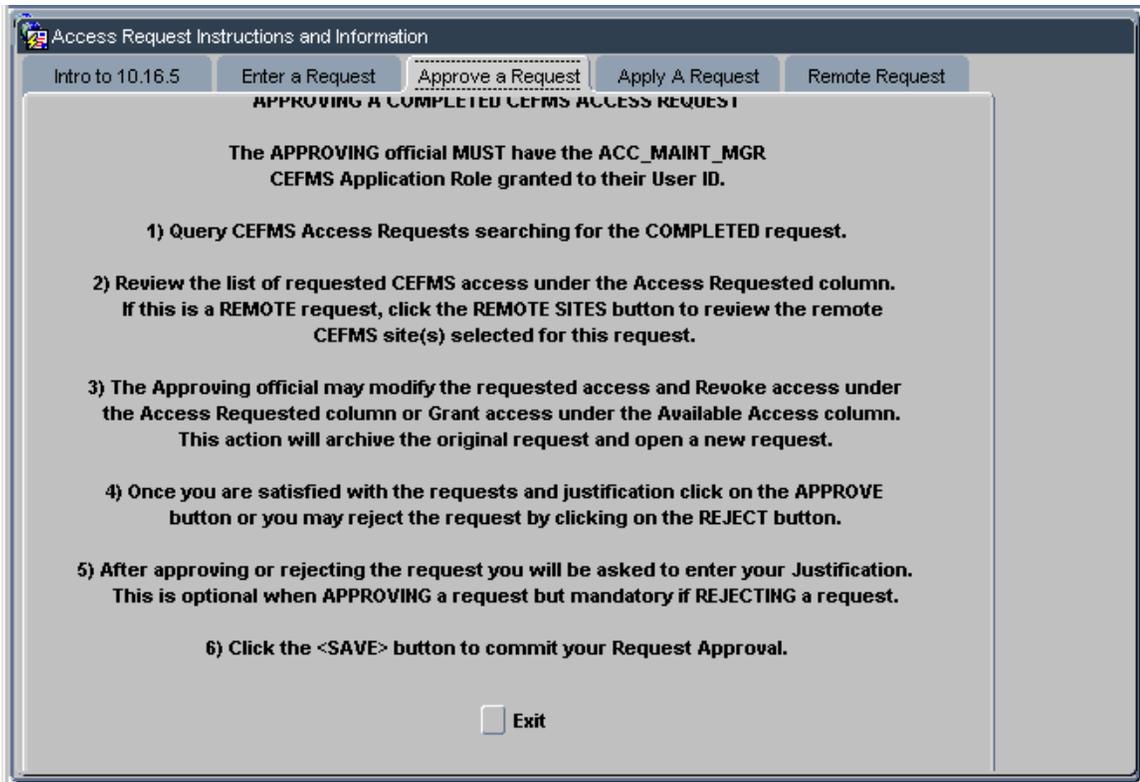
## **SECTION 2. ACCESS CONTROL REQUEST MANAGEMENT SYSTEM (ARMS)**

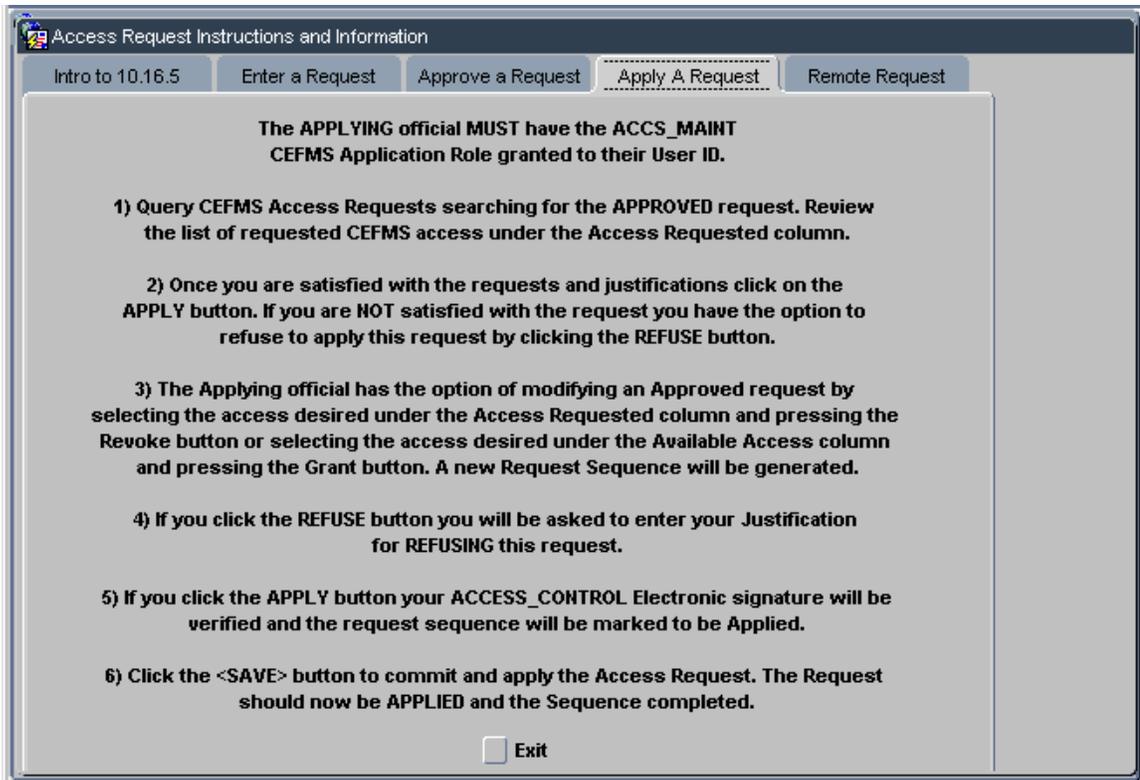
1. The Access Control Request Management System (ARMS) is an internal functionality of CEFMS and will be available 15 May 2002. This new functionality provides an automated means to manage requests and approvals for access to your CEFMS Application. This new functionality addresses AAA recommendations for records management of access control. At this time the new functionality is optional and the current access screens will be available. All users should become familiar with the new procedures, as the current screens will be obsolete in the future.
2. To utilize the system, sites will need to grant roles to the users delegated the responsibility for approving and applying access requests. CEFMS users will make their requests on-line and the users granted the responsibility through the role, `acc_maint_mgr`, are then required to approve or reject the request. If the request is approved, the final step is for the user granted the `Accs_maint` role to apply the request. The `Accs_maint` role currently provides update/insert to the current access control screens. With the new system, this role also allows a user granted the role to apply a new request to your database. We recommend that you review users currently assigned `accs_maint` role to ensure the appropriate users have this role. Another new role, `Remote_access_request_auth`, will be implemented with ARMS. This role should be granted to users with the responsibility for copying employee records from a remote site through screen 10.181. The current grant role screen, Role Maintenance 10.16, is available for granting these roles.
3. Current CEFMS users may use the system to request access to one, multiple or all sites at once. When the approver approves the request, the request is automatically pushed to the remote site(s). When a remote site receives a remote request, the remote site has the option to apply or reject the request. A record is maintained in the remote database of all requests received and any additional action taken for the requests. Additionally a record is maintained on the user's home database of changes made to their home access control record, which approved and applied the changes and the dates the changes were done. This feature is in response to the AAA finding that sites were not maintaining records of changes made to access control records.

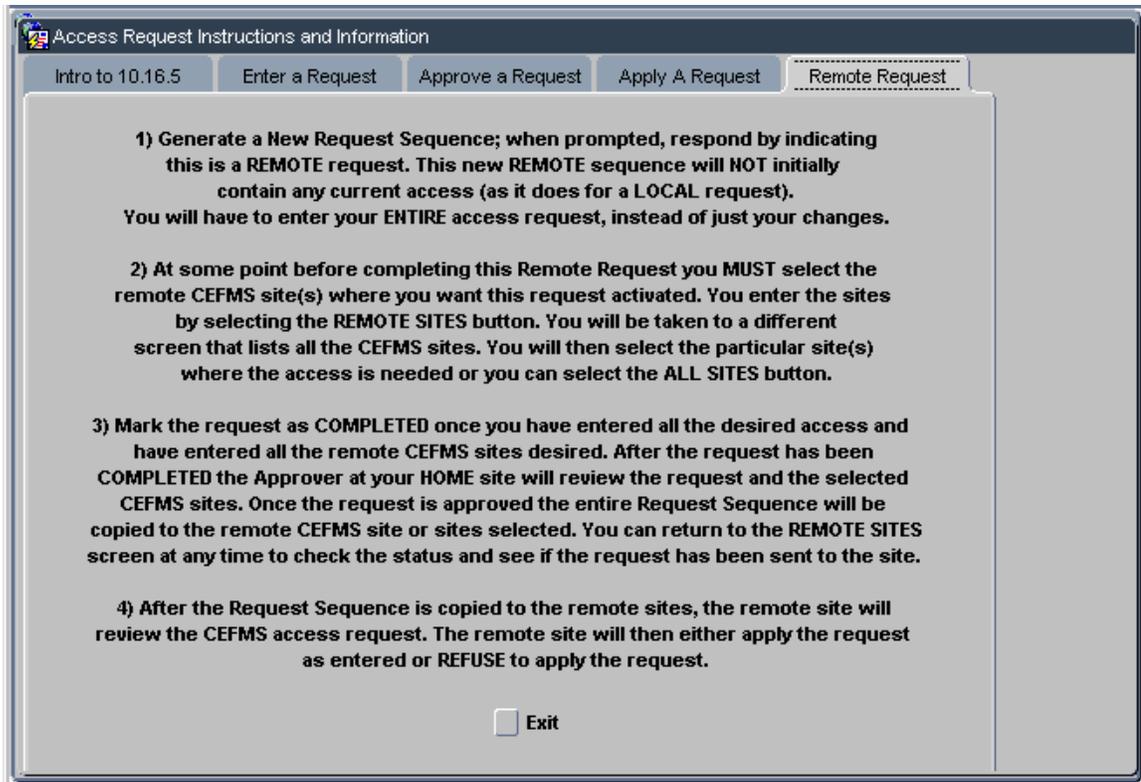
4. If a user requests access from multiple sites and one or more sites are not available then the requests will be sent to the available sites and the system will continue to send the remaining requests until all are successfully sent. Note, the timing required to send requests for various situations like database availability should be considered. Do not report lost requests until you have verified your system has not been available for at least 1 hour since the requests were sent and that the request was approved at the local site. Simply requesting remote access does not send a request; it must be APPROVED locally first.
  
5. Screen 10.16.5 allows a user to request, approve and apply permission requests without needing to know which are roles or access indicators. Automatic email notifications are sent utilizing the email addresses currently stored in CEFMS for each stage of the process. Email distribution to Approvers and Appliers is accomplished per definitions in Screen 10.16.3. New access records as of this date are set to expire 12 months from their apply date.
  
6. ARMS contains on-line user instructions. These instructions may be reviewed from the Access Request screen (10.16.5) by selecting the <Instructions> button. The Access Request Instructions Information screen is displayed on the page that follows. Users may also select the access control fields within this form to review descriptions for the various access permissions. Simply place the cursor on the access permission and double click the left mouse button. Additional online instructions are provided via the CEFMS Users Manual at <http://rmf31.usace.army.mil/cefmsdoc/>.
  
7. ARMS allows the Approving and Applying officials to exercise a "Line Item Veto." The Approving and/or Applying officials can modify a request by deleting or adding a role(s) to the request before they Approve or Apply the request. The Approving/Applying official indicates their desire to use a "Line Item Veto" by Revoking or Requesting a role for the request. The screen then gives them the option to open a new modified Request. The Approver/Applier then re-makes the modification, saves the request and then Approves or Applies. Email notification is sent to the requestor (and Approver if the Applied modified an Approved request).











## 8. Overview of Access Control Requests Management System (ARMS) Steps:

This screen may be accessed through the Smartscreen option of the CEFMS menu by inputting screen number 10.16.5. Access may also be granted through the data manager pages or by selecting the Access Request Management System from the first CEFMS menu page followed by the Access Request and Approval option (screen path AGA).

a. The first step is to initiate or receive a new access request from a user. New requestors must already have a valid USACE UPASS account and be granted cefms\_user to enter CEFMS and make a request.

(1) If a user is a current employee on a remote site database their employee and access control header record may be copied through 10.181 or selecting the <REMOTE EMP> option from Screen 10.16.5. The employee may request a remote access request at anytime but the acct\_maint\_mgr/approver from the user's home site must approve the remote request before it will be pushed to the remote site. The employee header record must exist before the request may be applied at the remote site. The user with remote\_access\_request\_auth role at the remote site must pull the employee record to their database utilizing Screen 10.181 or selecting the <REMOTE EMP> option from Screen 10.16.5. Then the acct\_maint may apply the request in Screen 10.16.5, which will activate and complete this request. Note: In most cases it's presumed the user with acct\_maint role will also have remote\_access\_request\_auth role granted.

(2) If the user is a new USACE employee they will need a UPASS account established first by the UPASS administrator and the cefms\_user role granted.

Then their employee record will be generated through the personnel interface as currently done. Acc\_maint\_user must create the header access record in Screen 10.1. Once the headers are created, the user will be required to enter a detailed access request in Screen 10.16.5 and submit the request through the approval process.

(3) If they are a new user and not an USACE employee (possibly a contractor employee) they will need a UPASS account established first by the UPASS Administrator and the cefms\_user role granted. Then the acper\_auth user will need to create an employee header record in Screen 10.224 and the acct\_maint user will need to create a header access record in Screen 10.1 for this user request. Once the headers are created the user will be required to enter a detailed request in Screen 10.16.5 and submit through the approval process.

- b. A user granted the acc\_maint\_mgr role approves the request. The approver electronically signs this record.
  - c. A user granted the accs\_maint role allowing them to apply the approved request applies the approved request to the database. The applying official signs this record. Within this step the approved roles are actually granted and the approved indicators are actually assigned to the requestor within the database. It is transparent to users within 10.16.5, the access request form, whether the requested permission is a database role or an access control indicator.
9. Email is automatically sent to the requestor, approver and applying official during each step of the process if they have an email address loaded into CEFMS. If no address is loaded the system will function properly but no mail will be sent. Currently the email addr is maintained in Screen 10.131, Employee Travel Information Screen.
10. The buttons named Remote Sites is new and links to the new screen 10.16.7, CEFMS Remote Access Request Screen, see on the page that follow. The buttons 'Accs Ctrl' links to Screen 10.1, Access Control; 'Role Maint' links to screen 10.16, Role Maintenance Screen; 'Remote Emp' links to Screen 10.18.1, Remote Employee Access Retrieval.
11. New Req Seq is the button to initially select to input a new request.
12. Request Types are listed in paragraph 1.2, Request Status Code, of this document.

13. The justification field must be entered when a user is requesting access. The approved remarks field must be entered when a request is being rejected or refused. Double click your left mouse button to expand and complete this field.
14. The Complete button is clicked when the requestor is ready to commit their request. Therefore the user clicks New Req Seq and chooses the appropriate access and when complete clicks the button indicating they are finished with this request. The user must then choose Save.
15. The Cancel Req button is used when a requestor wants to cancel their request. This request can be canceled anytime before the request is applied. It can be cancelled if it has been approved.
16. Remote Access: You must have a remote request record loaded on Screen 10.16.5, Access Request and Approval, to select the button named Remote Sites. The Remote Sites button takes you to Screen 10.16.7, Remote Access Request Screen. When this screen appears you may choose Add All to select all sites that you wish to send a request for access to; you may remove or select one or more sites; or you may remove all sites from your request. You must save your selection to save the changes you selected before exiting this form.
17. The Approving and/or Applying official can modify the request before the request is approved or applied. Email notification will be sent to the requestor (and Approver if the request is modified by the Applier).

v2.1.2 CEFMS Remote Access Request Screen 10.16.7

Req: 844 ID No: CES Home FOA: M2 Status: ALL REQ SITES RESPONDED

Name: CAROL WRIGHT Completed: 11-APR-2003 Approved: 11-APR-2003

| Available Site   | Selected Site   | Req Sent To Site? | Remote Req Status | Date Applied | Remote Remarks |
|------------------|-----------------|-------------------|-------------------|--------------|----------------|
| A0 HUNTSVILLE EM | R0 SOUTH ATLANT | SENT              | APPLIED           | 14-OCT-2002  |                |
| B0 MISSISSIPPI V |                 |                   |                   |              |                |
| B1 MEMPHIS DIST  |                 |                   |                   |              |                |
| B2 NEW ORLEANS I |                 |                   |                   |              |                |
| B3 ST. LOUIS DIS |                 |                   |                   |              |                |
| B4 VICKSBURG DIS |                 |                   |                   |              |                |
| B5 ROCK ISLAND I |                 |                   |                   |              |                |
| B6 ST. PAUL DIST |                 |                   |                   |              |                |
| E0 NORTH ATLANT  |                 |                   |                   |              |                |
| E1 BALTIMORE DIS |                 |                   |                   |              |                |
| E2 WASHINGTON AC |                 |                   |                   |              |                |
| E3 NEW YORK DIST |                 |                   |                   |              |                |
| E4 NORFOLK DIST  |                 |                   |                   |              |                |
| E5 PHILADELPHIA  |                 |                   |                   |              |                |

Record: 8/?

18. As of this date, no reports have been developed for this new access request functionality. However, below are the tables you may query to obtain the data your site needs to maintain these records.

- user\_access\_request - The initial request. This request and each consecutive request are stored in the database by sequence number.
- user\_access\_request\_detail - Contains request details by request sequence number.
- user\_access\_request\_site - For each remote request sequence number this table identifies the request to the home database site and remote database sites.
- access\_control - The current approved/applied access record for each CEFMS user in your database.

19. Additional Business Rules:

- A user should not be an approver and an applying official
- A user can not approve or apply their access request.
- A user can not submit a new request (new sequence no) until previous request (sequence no) for that user is canceled, approved and applied or rejected.
- A previous access control record that was not signed must be remac'd before a new request can be approved.
- Users must have a valid ESIG card and login with their ESIG card to sign an approval or apply access control record.
- Users must be granted the appropriate roles to approve or apply a request and to copy remote employee records.
- You must create a header access control record for new users if their record is not being copied in from a remote site.
- You must copy or create an employee record for user's requesting remote access.
- The system will allow a user to request access for another user.
- Once any new records are created from this date the record will expire within 12 months and the user must submit a new request.
- Multiple Remote requests for the same requestor must be applied in sequence (based on the Request Number).

## **SECTION 3.**

### **ACCESS DEACTIVATION IN ARMS (As of 01-AUG-2003)**

A new version of ARMS was promoted to production on 31-JUL-2003 that incorporated a new algorithm to remove all CEFMS access and deactivate an individual's userid access\_control record. The ARMS Access Deactivation process follows the same process as an access request (Generate new request, Complete, Approve, and Apply the request).

The ARMS methodology that refers to a request sequence as either Local or Remote is also referenced by the Deactivation process. When a LOCAL Deactivation request is Applied, the request is changed to a REMOTE request and an ARMS Deactivation request is sent to all CEFMS sites where the userid is currently active on ACCESS\_CONTROL. An ARMS request is made for each CEFMS site. A separate process checks each site to determine if the user is active at that site. If active, the request is sent to the remote site where the deactivation request will be Applied and the user marked inactive on access\_control. If not active, the request status for that site is marked NA for Not Applicable. Once all remote sites have responded or have been marked as NA, the request status of the Local request will be changed to indicate it has been Applied by all requested sites.

Once ARMS is fully implemented at the site, an access history can be determined by reviewing the entries in the USER\_ACCESS\_REQUEST and USER\_ACCESS\_REQUEST\_DETAIL tables. There should be entries for the last Access request and the Deactivation request.

After the Deactivation request has been applied, the ID\_NO should have no roles granted. The report levels should be blank and the access\_control inactive\_ind set to Y. The employee\_mstr inactive\_ind is NOT modified by the ARMS Deactivation routine. The following paragraphs provide a detailed explanation of the Deactivation process.

The autoarms SQR is activated in the CRONRUN package. This SQR identifies those employees whose local or remote access is due for annual review. If the local review date is within 14 days of the annual review, an ARMS request is automatically generated and marked as 'Complete'. This local request will contain the current CEFMS access. The CEFMS user can reopen and modify the request if necessary. Appropriate email notification will be sent to the respective user. If a CEFMS user has an applied request for a remote site that was 'Applied' either within fourteen or seven days of a year earlier, an email reminder notification will be sent.

If the CEFMS user has not entered a new request for a remote site more than a year after the last request was applied, an automatic Remote Deactivation request will be generated and marked as 'Complete'. Once this deactivation request is approved locally and applied remotely, the user will lose remote access to the site. The user has the option of changing the Remote Deactivation request to a regular request for access (by adding the required roles) or allowing the deactivation request to be processed. Once again, appropriate email notification is sent concerning the remote deactivation request.

### 3.1 LOCAL ACCESS DEACTIVATION

#### I. ENTERING A DEACTIVATION REQUEST

1. When using ARMS to remove all CEFMS roles and deactivate access\_control records, the first step is to generate a New Request Sequence. This is accomplished by clicking the New Req Seq (New Request Sequence) button on the upper left hand section of Screen 10.16.5.
2. A new screen will pop-up asking if this is for a Local or Remote request. If the userid to be deactivated is on the local CEFMS database, select <Local>. **NOTE:** After the userid is deactivated on the Local CEFMS database, a request will be automatically generated to also deactivate the userid on ALL CEFMS databases where they are currently active in access\_control. If the userid needs to be deactivated on a limited number of sites, select <Remote>.
3. No action is required for the explanation screen that will be displayed next. Click <YES> to return to Screen 10.16.5.
4. The user will be prompted to enter the ID\_NO of the user to be deactivated. (Be sure to enter the ID\_NO and NOT the userid). After entering the ID\_NO of the user to be Deactivated, click the <SAVE/RETURN> button immediately below the ID\_NO window.
5. Once back to Screen 10.16.5, select <<Revoke ALL> to have all CEFMS roles and access\_control levels revoked and the access\_control record deactivated for the user selected.
6. A Warning Message will appear reminding the user that ALL roles are being revoked. Select <<Revoke ALL> to continue the deactivation process.

7. Once all roles have been revoked and the Access Requested column on the right hand side of Screen 10.16.5 is empty of roles, select <Complete> on the bottom left hand side of the screen.
8. Again, the user will be reminded that the execution of this request as currently marked will remove roles and access from the userid. Click 'Yes' to continue the process.
9. Enter a Request Justification for this request. Click Save/Return immediately below the justification window.
10. Save the request by selecting <SAVE>.

## **II. APPROVING A DEACTIVATION REQUEST**

1. As with regular ARMS requests, the request must be approved by an authorized approver with the ACC\_MAINT\_MGR role for the user's Org Code.
2. While the request sequence to be deactivated is displayed on Screen 10.16.5, the approving official will select <Approve> .
3. Another warning message is displayed that alerts the Approver that if no roles have been selected and if this request is Approved and Applied, the user will have all roles revoked and access\_control records deactivated. To continue the deactivation request, the Approver clicks the Approve Deact button (by selecting the Return button, control is returned to Screen 10.16.5 without approving the request).
4. Once the Approve Deact button is selected, the Approver's ACCESS\_CONTROL\_CAT signature is verified and a window appears for the Approver to enter an Approval/Disapproval Reason. Once again, a decision is entered and the approver clicks the SAVE/RETURN button beneath the decision box (or the Approver can click the SAVE/RETURN button without entering a decision).
5. The Approver selects <Save> . WINSIG will now ask the Approver to sign the ACCESS\_REQUEST\_CAT electronic signature which documents the ARMS request sequence.
6. If the e-mail option is selected for a particular site, e-mail is sent to the user notifying them that the request to be deactivated has been approved.

7. The Deactivation request has now been Entered, Completed, and Approved.

### **III. APPLYING A DEACTIVATION REQUEST**

1. As with regular ARMS request, the request must be Applied by an authorized approver with the ACCS\_MAINT role for the user's Org Code.
2. The Applier selects <Apply>.
3. Once again, a warning message will appear stating that by this Apply request all roles will be revoked and the access\_control record will be deactivated. However, now an additional message warns that when the request is applied, a request will be sent to all CEFMS sites where the user is active, asking to 'apply' a similar request at each applicable site. The Applier selects <Deactivate> to continue the request.
4. The Approver's ACCESS\_CONTROL\_CAT record will be verified and the ACCESS\_REQUEST\_CAT record will be verified.
5. The Applier is now prompted to enter an Apply decision (the decision is optional). After entering a decision (if desired), the Applier clicks the SAVE/RETURN button immediately below the decision window.
6. The Applier now selects <Save>.
7. Once <Save> is selected, all roles will be revoked, all access\_control levels will be nulled, and the access\_control inactive\_ind will be set to 'Y'.
8. PLUS (this is new ARMS methodology) once a userid is deactivated at their home site, access should be deactivated at ALL CEFMS sites where there was an active status. Therefore, the request will automatically be changed from LOCAL to REMOTE and a request will be entered on the USER\_ACCESS\_REQUEST\_SITE table for ALL current CEFMS sites.
9. A separate DBMS\_JOB routine runs every 10 minutes. This separate routine will find the remote requests and copy the request to the remote site IF THE USERID IS CURRENTLY MARKED AS ACTIVE ON THE REMOTE SITE.
10. The remote site will eventually see the deactivation request and will Apply the request at their remote site.

11. The DBMS\_JOB routine that runs every 10 minutes will send data back and notify the Home FOA SITE of the request of the action of each remote site.
12. Once all sites have responded (where the userid is active), the request status code of the request will be changed to PR and the request status description on Screen 10.16.5 will indicate that All Remote Sites Have Responded.
13. The process is now complete.

## **3.2 REQUEST TO DEACTIVATE A LIMITED NUMBER OF REMOTE SITES**

### **I. Entering a REMOTE DEACTIVATION REQUEST**

1. Select the New Req Seq (New Request Sequence) button on Screen 10.16.5.
2. When prompted, select <Remote>, indicating this request is a remote request and NOT a local request.
3. Click the continue button when the process is explained.
4. The remaining Completion and Approving process is the same as for a Local request except the user selects the Remote sites for which this request is being generated – as in a typical ARMS Remote request.

### **II. Approving a REMOTE DEACTIVATION REQUEST**

1. The Approving official marks the request as Approved and enters comments if desired.
2. Once the Remote request is Approved, the request is copied to the Remote sites selected.

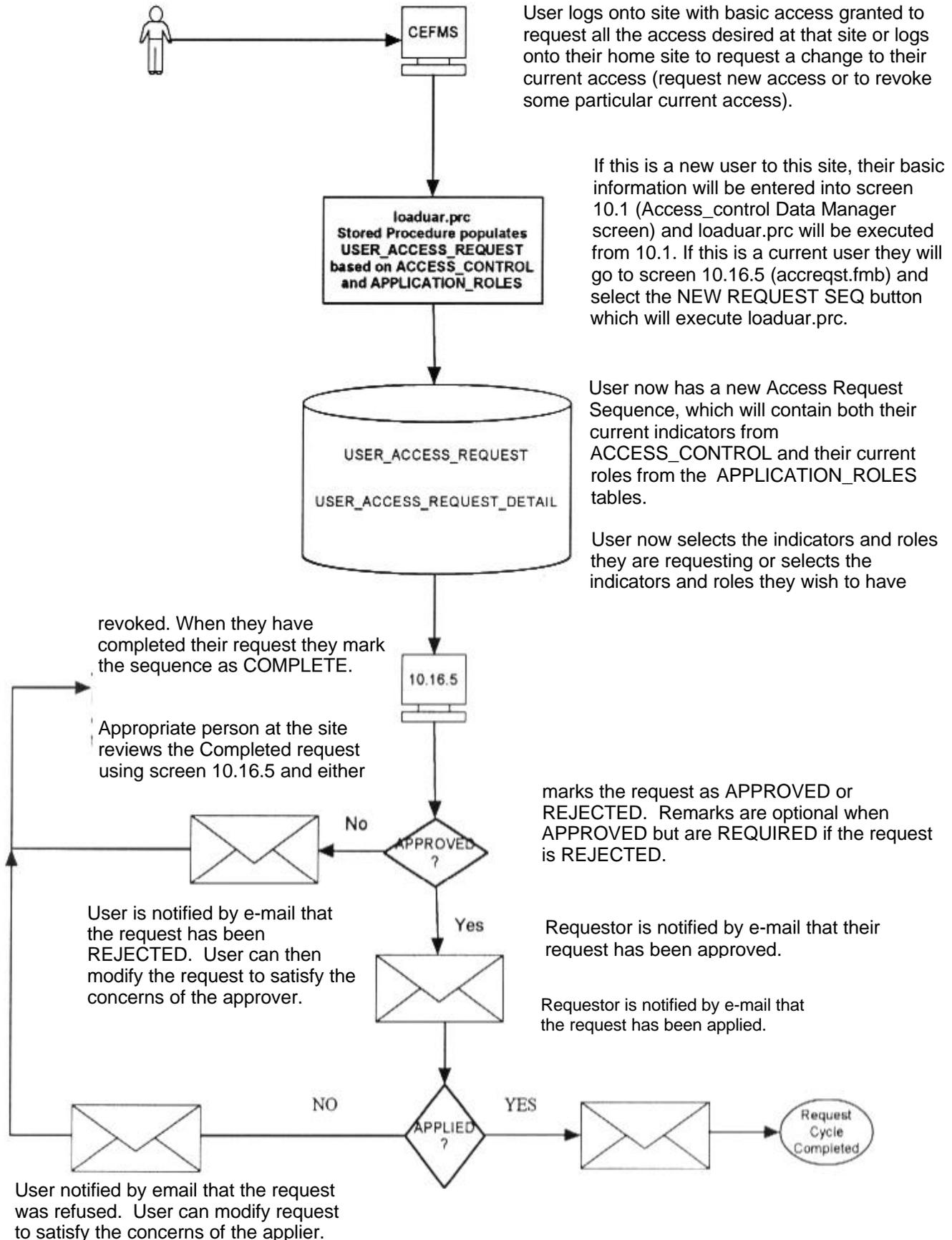
### **III. Applying a REMOTE DEACTIVATION REQUEST**

1. Each remote site selected will then have to Apply the request (same process as for a Local request).
2. After each site selected has Applied the request, the home database will be appropriately updated with the remote site status.

# APPENDIX A

# CEFMS Access Request Life Cycle

(as of 07-Nov-2001)



# APPENDIX B

## HOW TO QUERY THE DATABASE FOR ARMS REQUEST DATA

The header table is `user_access_request`. The specific roles and levels requested are in `user_access_request_detail`. Connect the two tables together using `request_seq_no` and `home_foa_code` as the keys.

For instance:

```
SELECT uar.request_seq_no, uar.home_foa_code, uar.id_no,  
uar.request_status_code, uard.access_request_text,  
uard.access_level_code, uard.rga_mail_code  
FROM user_access_request uar,  
user_access_request_detail uard  
WHERE uar.request_seq_no = uard.request_seq_no  
AND uar.home_foa_code = uard.home_foa_code  
AND uar.request_seq_no = 3004  
ORDER BY uard.access_request_text
```

Change or add to the WHERE clause to suit your needs (eg. match on `ID_NO` instead of `request_seq_no`).

# APPENDIX C

## CEFMS Access Request Management System (ARMS) Email Notifications

Users with the local dm role can turn off **ALMOST ALL** ARMS email per site database.

**WARNING** - if you choose these options, it impacts every ARMS action on your database and you will not receive notification of impending actions. Go to Screen 10.CP.

**To set the parameter off, the options are:**

- arms\_approver\_applier\_email\_off (Y turns off email for **ALL** approvers and appliers at your database)

- arms\_requestor\_email\_off (Y turns off email for **ALL** requestors/users for email informing them that their request was Approved and/or Applied.)

....A null value means turn ON email.

You can also go to Screen 10.16.3 and turn off email per individual user assigned to approver(acc\_maint\_mgr) or applier(accs\_maint) by organization code assigned.

**EXCEPTION NOTE:** The CRON job that sends out the notice to users that their access is about to expire can **NOT** be turned off.

Also, the rules in Outlook provide the option for a user to define whether they want to receive specific incoming emails.