COPYRIGHT & TRADEMARKS

Copyright © 1998, 2009, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS
Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

SYSTEM POLICIES
The tasks in this documentation provide end users with the tools to enter data and collect data in system. It is the responsibility of the agencies to comply with State Statutes, Federal Rules and Regulations, and State policies. For further information concerning State Statutes and policies, please refer to both internal agency resources and the Department of Administrative Services website.
Table of Contents

Request Revisions to Existing User ID - Role Assignments ................................................. 1
  Request Revisions to Existing User ID - Role Assignments Overview ................................. 1
  Request Revisions to Existing User ID - Role Assignments Lesson .................................... 1
Request Revisions to Existing User ID - Role Assignments

Request Revisions to Existing User ID - Role Assignments Overview

Authorized Agents (AA20) manage requests for revisions to User IDs and their roles through this application. Revision requests include: additions, revisions, and removal of roles for existing User IDs.

Authorized Agents ONLY have access to User IDs in Agencies for which they are assigned as Authorized Agents. This access is driven by the Address Book Number of the User and the Agency with which the Address Book Number and Security Business Unit are associated.

Business Process Owners will review role assignment requests as appropriate.

Authorized Agents will receive e-mail notification when requests are completed and should use the Security Request Inquiry application to check that their employees’ User IDs have the correct functional roles assigned.

Request Revisions to Existing User ID - Role Assignments Lesson

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Click the State of Nebraska link.</td>
</tr>
<tr>
<td>2.</td>
<td>Click the Authorized Agents link.</td>
</tr>
<tr>
<td>3.</td>
<td>Click the Authorized Agent Request link.</td>
</tr>
</tbody>
</table>
4. Use the Query by Example (QBE) line to narrow search for an existing User ID.

5. To populate grid, click the **Find** button.

   Authorized Agent will only be able to view User IDs associated with Employees in their Agency of responsibility.
### Step 6
Indicate the User ID to revise by clicking the radio button in one of the rows containing the User ID.

![Radio button]

### Step 7
Click the **Select** button.

![Check mark]
8. **User ID** and **Address Number** populate with User information. Grid populates with ALL roles associated with the User ID.

Authorized Agent can request the following revisions from this screen:

- Change an existing Security Role for a Security Type to a different Role; e.g. change an PT20 to a PT30
- Remove an existing Security Role for a Security Type
- Request a new Security Role for which an end user does not currently have the Security Type

9. **Note**: A User ID can only be assigned one Role within a Security Type. For example, a User ID cannot have both a PT10 role and a PT30 role assigned.

10. **Decision**: Revise Roles assigned to a User ID - Change Existing Role, Remove Existing Role, Add a new Role to a User ID

   - Change Existing Role
     Go to step 11 on page 5
   - Remove Existing Role
     Go to step 23 on page 8
   - Add new Role/Security Type
     Go to step 32 on page 11
### Step 11.
**Request to Change an existing Security Role for a Security Type to a Different Role**

### Step 12.  **REQUESTED ROLE**
- Enter requested changes to the User ID; System allows only one Role per Security Type (SEC TY)
- All roles are prefaced with “N000.”
- Changes to levels within a Security Type must be initiated within the ROW currently assigned to the Security Type

Enter the desired information into the **REQUESTED ROLE** field.

### Step 13.
Press [Tab].
### Training Guide

**Request Revisions to Existing User ID - Role Assignments**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 14. | **STATUS CODE**  
Automatically populates based on transaction:  
o A = Approved – if there is no requirement for approval by a Business Process Owner, then this request will automatically advance to an Approved Status; sends e-mail to NIS Security for NIS Security Change  
o P = Pending – A BPO must review the request and take action regarding the request (Approve, Deny); sends e-mail to Business Process Owner(s) for review & action |
| 15. | **REQUEST ORIGIN**  
Automatically populates with A = Authorized Agent Requested |
| 16. | **COMMENTS**  
Free text for sharing information throughout the Authorized Agent/BPO process  
*Note:* Take advantage of the Comments section. This information will be available through an Audit Table. |
| 17. | Submit requested revisions to User ID and User Roles, click the **OK** button. |
| 18. | **Decision:** Select the appropriate option:  
- Revisions Complete  
  Go to step 19 on page 7  
- Continue with Revisions  
  Go to step 10 on page 4 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>19.</td>
<td>To review requested changes for specific User IDs, search the Work with Role Request grid by using the QBE.</td>
</tr>
<tr>
<td>20.</td>
<td>Click the <strong>Find</strong> button.</td>
</tr>
<tr>
<td>21.</td>
<td>Click the <strong>Close</strong> button.</td>
</tr>
<tr>
<td>22.</td>
<td><strong>End of Procedure.</strong> Remaining steps apply to other paths.</td>
</tr>
</tbody>
</table>
### Training Guide

**Request Revisions to Existing User ID - Role Assignments**

#### Step 23
**Request to Remove an Existing Security Role for a Security Type**

#### Step 24
Click the radio button on the Grid Row containing the Security Role to be removed from the User ID.

Click the option.

#### Step 25
Click the **Role** button.

#### Step 26
Click the **Remove Access** menu.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 27.  | Authorized Agent Request - Remove window appears.  
     | Click the **OK** button. |
### Step 28

**REQUESTED ROLE** field on the Grid Row populates with the word "REMOVE".

If the request to remove a specified Security Role is incorrect, delete the word "REMOVE" from the populated field.

### Step 29

**STATUS CODE**

- Automatically populates: as A = Approved
- There is no requirement for approval by a Business Process Owner
- Sends e-mail to NIS Security for NIS Security Change

### Step 30

**REQUEST ORIGIN**

- Automatically populates with A = Authorized Agent Requested

### Step 31

**COMMENTS**

Free text for sharing information throughout the Authorized Agent/BPO process

Go to step 17 on page 6
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>32.</td>
<td>Request a New Security Role/Security Type</td>
</tr>
<tr>
<td>33.</td>
<td>As end user responsibilities change, they may require additional Security Types. If the end user does not already have a Security Role for a Specific Security Type, add a Requested Role to the grid.</td>
</tr>
<tr>
<td>34.</td>
<td>New requests are added to the first available blank Row in the grid.</td>
</tr>
<tr>
<td>35.</td>
<td>REQUESTED ROLE</td>
</tr>
<tr>
<td></td>
<td>Enter requested roles; all roles are prefaced with “N000.” You may use the lookup button if you need to find a role or you would prefer to autopopulate the Requested Role field instead of entering the role manually.</td>
</tr>
<tr>
<td>36.</td>
<td>Click the REQUESTED ROLE object.</td>
</tr>
<tr>
<td>37.</td>
<td>Enter the desired information into the REQUESTED ROLE field.</td>
</tr>
<tr>
<td>38.</td>
<td>Press [Tab].</td>
</tr>
<tr>
<td>39.</td>
<td>SEC TY – Security Type</td>
</tr>
<tr>
<td></td>
<td>Defaults to the Alpha Digits based on the REQUESTED ROLE</td>
</tr>
</tbody>
</table>
### Step 40: STATUS CODE

Automatically populates based on transaction:

- **A = Approved** – if there is no requirement for approval by a Business Process Owner, then this request will automatically advance to an Approved Status; sends e-mail to NIS Security for NIS Security Change
- **P = Pending** – A BPO must review the request and take action regarding the request (Approve, Deny); sends e-mail to Business Process Owner(s) for review & action

### Step 41: REQUEST ORIGIN

- Automatically populates with **A = Authorized Agent Requested**

### Step 42: COMMENTS

- Free text for sharing information throughout the Authorized Agent/BPO process

*Note:* Take advantage of the Comments section. This information will be available through an Audit Table.

Go to step 17 on page 6