Understanding Kuali Access – For Senior Business Officers and Access Coordinators

Catherine Maddaford
Kuali Access Manager
Office of the Comptroller
Part 1- Starting at the Beginning, How does access in Kuali work?

I - USER ACCESS – THE BEGINNING
• When services are set up for employees in ITS, Kuali receives the appropriate identifying information to create the “person” or KIM record.
• KIM, Kuali Identity Management, uses KFS tables, Kuali security, and roles and permissions to manage access rights in Kuali.
The “Person” identity in Kuali is the unique identifier that links your login credentials to your roles and permissions in Kuali.

Catherine Maddaford, 1/13/2016
How is the principal name used?

- You see the principal name in the edoc status tab and in the route log.
- You see the principal name when you are using the search icon to find or identify someone.

At the top of the edoc

In the route log

For ad hoc routing
Assigning Roles

I - KUALI IDENTITY AND ROLES
 Roles

• Give the principal (user) specific access to perform functions in Kuali.

• Are grouped by namespace, which identifies the module or the group of business processes that are associated with the roles.

• Contain permissions that are specific definitions of what the role allows the user to do.

• Can have qualifiers or security that work together with the role to further define the way a role works for that specific user.
Roles
Group together one or more permissions that allow you to perform specific functions required in a particular process.
Are assigned to a principal or a group to allow that principal or group to perform a particular function or task.
Can be directly assigned in KIM or derived from other sources.

Permissions
Are very specific steps that are needed to perform a particular function in a business process.
Can be grouped together and assigned to a role to allow the various steps to be executed in the process.
Are more generic in nature than roles.
The same permissions can be assigned to multiple roles.
Examples

• Permissions
  – Open a document
  – View a document’s attachments
  – Approve a document
  – Edit an accounting line

• Roles
  – Reallocation reviewer for procurement card
  – JV approver
  – General Ledger viewer
Assigned Roles

• Assigned roles have numbers and are attached directly to the user’s KIM record.
• The membership tab in the KIM record displays the assigned roles – see person lookup.
• The security module in Kuali also creates and assigns roles containing the security definition and values.
Derived Roles

• Are often used in routing edocs for approval.
• Are not displayed in the KIM record membership.
• May or may not appear in the user security reports.
• May come from sources within Kuali, such as tables within Kuali, or may come from information fed into Kuali.
Some examples of derived roles:

- KEW Chart of Accounts - SBO and VP
- JV initiators and approvers
- Fiscal Officer
- Supervisor for eStatements and DVQE’s.
- Account Managers and Account Supervisors
- PET approvers
- Pcard holders
• Most roles are assigned to individuals, but some roles can be assigned to groups.
• Groups in Kuali are a collection of users who are taking on actions in Kuali as a group rather than as individuals.
• When a role is assigned to a group, the group performs as one individual, usually requiring the action of only one member.
• Roles assigned to groups don’t change, but the members are added or deleted from the group.
Role Qualifiers

- Role qualifiers further define which records or documents are included in the actions allowed, acting as a filter for routing or viewing of specific documents.
- Users can be assigned the same role, but may have different role qualifiers.
- When viewing a role with a role qualifier in the person lookup, membership tab, the role qualifier will be displayed as another row beneath the role number and description.
Kuali@USC

Qualifiers - Examples

• Organization codes
• Department codes
• Campus codes
• Account numbers
• Dollar threshold
• Unit codes
Roles with Qualifiers

- Pcard reallocation
- SPA budget reallocation approver
- Accounting reviewer
- Business Office reviewer (eStatements)
- BC Processor
- KC award roles
- FAA Reviewer
- SBO Reviewer (eStatements)
- VP approval (DV/DVQE.)
- Cashiering
How does Kuali security impact your access rights?

I - KUALI SECURITY
Kuali@USC

Kuali Security

• KFS security is a separate module used to assign specific account or org code security definitions that work together with certain Kuali, eMarket, or BI roles.

• The security definitions are different from the role qualifier, because they are not attached to one specific role, but rather can be associated with multiple roles.

• Security parameters determine which processes are defined by security and which are not.
The security definitions, once assigned to a user, are updated to the KIM record with a role number - namespace KFS-SEC.

The KFS-SEC roles in KIM will also have a name that may help identify the module to which it is applied, such as Requisitioner.

You cannot understand the security restrictions without understanding the role(s) with which the definition is paired.
Examples of some processes that use Kuali security definitions together with assigned roles:

- eMarket
- Payroll Expense Transfers - PET
- BI reports
- Internal Billing – IBR
- Disbursement Voucher – DV
• Many processes share the same list of accounts to use as the security definition for viewing and/or adding accounting lines.

• This general account security can be defined at the account level or at the organization code level.

• When using account or org code security, accounts can be selected and filtered by identifying the org code or org code mask, or by the account number or account mask.
• This “default” security definition uses account and account masks, referring to the account numbers in the general ledger.

• Only account numbers and account masks are listed as the property values for the ETL default definition.

• Account masks always include the starting digits, such as 123456*, with the * representing the missing digits for all of the 10-digit account numbers to be included.
See Person lookup – membership tab

- The Property values listed will be the accounts and account masks referring to the general ledger account numbers, separated by a semicolon (;).
- The role number assigned in KIM for ETL default accounts does not work alone, but must be paired with another assigned role.
• Organization codes or org code masks appear in the **KFS Org** Security Definition.

• Org code security works in the same way as account security for the same processes.

• By listing your org codes, or the org code masks, you are adding all of the GL accounts that belong to those org codes.

• When org code security is paired together with the ETL default definition accounts to allow or deny access to accounts or account masks.
Why use KFS Org?

- You avoid listing account masks that may not be exclusive to your school/division.
- You get access to accounts that only belong to your org codes, regardless of the account number or mask, even if the account number is moved to a different school or division.
- You avoid the necessity of updating account security whenever new accounts are added or moved to another org code.
• ETL default and KFS Org security are used to define accounts when adding or viewing accounting lines for the following:
  – Internal Billing Requisitions (IBR)
  – Disbursement Vouchers (DV)
  – SPA Budget Reallocation (SBR)
  – General Budget Change
  – General Ledger Viewer (Balance Inquiries)
  – BI reporting, GL and payroll labor ledger
The following modules use their own specific org code or account security definitions.

- eMarket, all roles requiring security
- Special approvers for DV/DVQE
- Account delegates for DV/DVQE
- CAMS by org

The special security definitions are identified with names that help you associate them with the module and role, and update the KIM record with a unique role number associated with KFS-SEC.
• If you want to update your account or org code security, you must complete an access request that identifies the following:
  – The module where the security applies.
  – The role that is paired with the security you are updating.

• ETL Default Definition and KFS Org code security apply to numerous modules, and can be requested simply by selecting the category add account or add org code on the application.
• The following are some of the processes that do not apply any role qualifier or account or org security for the edoc initiator:
  – DVQE
  – General Journal Voucher
  – Internal Billing Journal Voucher

• When you are requesting changes to a user’s authorized accounts, you would not need to request any change for roles that do not use KFS security.
Understanding roles in Kuali

I - WHAT DOES THE ROLE DO?
How do I pick roles?

• There are so many roles in Kuali that you must be able to identify and select roles by the following criteria:
  – What system do I need to use?
  – What module within that system do I need to use?
  – What process do I need to use within that module?
  – How does what I need to do relate to others using the same processes within my department/unit?
Roles are grouped by system and module

• Systems
  – Kuali Financial System
  – TARA
  – Business Intelligence
  – eMarket

• Modules
  – Journal Vouchers
  – Procurement Card
  – Purchasing/Payments (from eMarket)
  – Disbursements
• The Namespace in Kuali indicates the system and/or module.
• Each role belongs to a Namespace to help segregate it from other roles in Kuali, especially those that may contain similar permissions.
• If you view your assigned roles as they relate to the namespace codes it will help you identify what that specific role allows you to do, what module you are using, and what are the constraints on those permissions.
Kuali@USC

Ex: Namespace Codes

• KFS-FP: Financial processing
• KFS-GL: General ledger
• KFS-PURAP: Purchasing/Accounts Payable
• KFS-SEC: Kuali account and org code security
• KFS-SYS: Financial System
• KC-SYS: Kuali Coeus System (TARA)
• KR-KEW: USC KEW Workflow
KFS-PURAP namespace includes eMarket

<table>
<thead>
<tr>
<th>Role</th>
<th>Namespace Code</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>131271</td>
<td>KFS-PURAP</td>
<td>eRequisitioner</td>
</tr>
<tr>
<td>131391</td>
<td>KFS-PURAP</td>
<td>eFinancial Approver</td>
</tr>
<tr>
<td>131272</td>
<td>KFS-PURAP</td>
<td>eInvoice Approver</td>
</tr>
</tbody>
</table>

• In the above example, the roles shown are for eMarket, and they all contain the same Namespace Code.

• Note also the small “e” in front of each role name helps to associate these with eMarket.
To better understand roles, you can break them down by type into a few basic categories.

- Initiator
- Viewer
- Approver
- Reviewer

When choosing a role, decide what business process the user will need to perform, select the system or module that contains the process, and then select the type of roles required.
The initiator of a Kuali edoc is the one who starts the edoc from the beginning, inputs all of the necessary information, and hits the submit button to put the edoc into workflow.

Most initiator roles must be individually assigned to the user in the KIM record.

A few edocs can be initiated by any Kuali user, and therefore do not need an assigned role in KIM.

- General purpose workflow edocs.
- Kuali access request workflow edocs.
- DVQE edocs.
• The most common example of view only access is the General Ledger Viewer role for Kuali inquiries.
  – Kuali Security assigns access to accounts or organization codes. This restricts what can be viewed.
  – The GL Viewer role allows the user to open and view edocs when using the drill down feature within the Kuali inquiries and lookups.
• Approver is a very generic term that applies to many different types and levels of approval in Kuali.
• An approver views an edoc already created by an initiator and approves the transaction and/or accounting detail included in the edoc.
• Some approvers can make changes in the edoc before approving.
• Approvers must have an assigned role or a derived role in order for Kuali to route the edoc to them for approval automatically.
• Reviewers have the approval function (approve button) on the edocs, but they are reviewing and approving in addition to another approver, either after or in addition to another approver.
• Examples of reviewer roles:
  – Pcard eStatement Business Office Reviewer.
  – DV/DVQE Organization Reviewer.
What sets Workflow?

• Workflow access originates with the roles and security as identified in KIM and KFS Security, or as a result of a derived role in KFS.

• Each business process has its own design for workflow, so you must understand how the process works to be able to follow the workflow and associated roles and security.

• The basics of workflow are the same for all roles, the edoc starts with the initiator, and must pass one approver node before it can go to the next approver node, and changing that routing requires changing the role assignments.
PART 2 - Using lookups to find information about access

II - USING PERSON LOOKUP
Find “Person”

- Go to Administration tab>Security>Person.
- There are several fields to search by in the person lookup, but you should need only one or two to complete the search accurately.
- After populating the appropriate field, click on search and view the results.
- Click on return value for the correct selection to view the KIM record.
- Click on the membership tab to view the roles assigned to you or the KIM record you are viewing.
• This role example appears in the membership tab and is a security definition that works with eMarket.
  – The PURAP in front of the Name of the role identifies it as a security definition for one or more Purchasing/Accounts payable processes.
  – The name of the role gives you more information as to how this security it applied.
• Once an employee is inactive the KIM record becomes inactive and the user cannot log in.
• Assigned roles are deactivated and removed from the KIM record within a short time after the user is deactivated, but the inactive user may not be removed from other tables within Kuali used for derived roles.
• Departments should be sure to request changes to those derived roles as soon as possible in order to prevent workflow routing issues.
• To find and view an inactive KIM record, select BOTH at the bottom to view both active and inactive records.
Finding the information for Derived Roles

II - LOOKUPS FOR DERIVED ROLES
Separate Lookups

• Since the derived roles come from another source, you must know what that source is and where to find the information.

• Most tables within Kuali can be accessed through various “lookup” searches located in different sections on the Kuali menus according to the modules associated with the lookups.

• Other sources may be outside of Kuali and therefore may or may not have a corresponding Kuali lookup.
• The Financial Maintenance tab contains many of the maintenance tables associated with the financial processes used in KFS, and therefore also contains the lookups associated with the information in those tables.

• Locate the category for the information.

• Find the best description for the information you wish to find.

• You may need appropriate security to allow you to use the lookup.
Finding Lookups – Ex.

FINANCIAL MAINTENANCE TAB

Section/Category

• Purchasing and Accounts Payable
• Financial Processing
• Labor Distribution

Lookup Example

• Employee Supervisor Lookup
• General Journal Voucher Users
• Payroll Expense Transfer Department Approver
Employee Supervisor lookup

• Three fields for three supervisors
  – Supervisor = eStatement Supervisor
  – Tab Supervisor (not used or updated)
  – PURAP Supervisor = DVQE Supervisor
• Initiators or approvers can be viewed by either entering the JV number or the user ID.
• Each JV number is assigned to a school or a department, and then the initiators and approvers are assigned to the JV number.

Financial Processing

- Balance Sheet Code
- Budget Control Group
- Budget Change Object Exception
- Facilities Improvement Rate
- Disbursement Voucher Cash Advance Type
- Disbursement Voucher Cash Advance Status
- Financial Report Schedule
- Freeze Process Maintenance
- Fringe Benefit Rate
- Fringe Benefit Rate Code
- General Journal Voucher Type Lookup
- General Journal Voucher Users
Main Menu Lookups

• Some lookups are located on the Financial Main Menu
  – Balance Inquiries – General Ledger
    • Account Lookup (no security required)
    • Other balance inquiries – security required
    • Most balance inquiries contain Fiscal Officer and Account Manager information
  – Lookup and Maintenance – Chart of Accounts
    • Account Delegate
    • Contains Primary and Secondary account delegate information
See Chart of Accounts, Account Delegate

Enter the account or enter the principal name, and then select Search.

If there are no values found, then there are no delegates assigned to that account.
Part 3 - Understanding Role Types

III - APPROVAL ROLES
There are many types of approvers in the Kuali workflow, but the following are the most common.

- **A financial approver**
  - approves a transaction that will post to the general ledger, so account or org code security is necessary.

- **A special approver**
  - approves the content of the transaction for various reasons, but is approving in addition to a financial approver.

- **A supervisor approver**
  - approves a transaction for their subordinate, but is approving in addition to a financial approver.
Examples: Approvers

• Financial Approver
  – eMarket financial approvers, various definitions.
  – Fiscal officers or account delegates for DV’s and DVQE’s.
  – Pcard reallocators and reallocator approvers.

• Special Approvers
  – Organization (Accounting) reviewer for DV/DVQE.
  – Special approver for eMarket and DV/DVQE.
  – Business Office Reviewer for pcard eStatements.

• Supervisor Approver
  – DVQE reimbursements are approved by the reimbursee’s supervisor.
  – Pcard eStatements are approved by the card holder’s supervisor.
Fiscal Officer

- Kuali’s default approver.
- Usually the Senior Business Officer.
- Associated with an account in the general ledger.
- Not visible in KIM because it is derived from the chart of accounts.
- Only one fiscal officer per account.
- Some processes use other roles instead of fiscal officer for edoc approvals.
Kuali@USC

Duties of Fiscal Officer

• Approves Disbursement edocs, both DV and DVQE
• Business rules requiring the Senior Business Officer (SBO) approval in both Disbursement and eMarket transactions will route to the fiscal officer for approval.
• Fiscal officer may update a general ledger budget in Kuali Budget Construction for eligible accounts.
• Identified as the default SBO for organizations.
• Assigned approvers must have a specific role with or without role qualifiers assigned to the KIM record.

• The most important issue in assigning an approver role is to determine how and when that approval is requested and how it affects the workflow of your business processes.

• Choose the correct approval type, and be sure to assign appropriate dollar thresholds, where applicable.
eMarket Approvals

- eMarket approvers – examples of assigned roles
  - Financial approver
  - Special approver
  - Invoice exception approver
  - Requisitioner with self-approval

- Security definitions specify the security and dollar thresholds for approvers in eMarket.
  - Approvals can be designated by account or by org code.
  - Have unlimited or limited thresholds defined.
• **Examples**
  – Procurement card holder
  – Supervisors
  – JV approvers
  – PET approvers
  – COA change request approvers

• Be sure to understand the source of your derived roles so that you can trace back to that source to identify issues or make changes.

• Use lookups in KFS to monitor, where available.
• Table Source – Chart of Accounts Workflow.
• Process located on Workflow Main Menu
• Lookup located on Workflow Maintenance Menu.
  – Use Department to look up the Department Code.
  – SBO and VP are assigned by department code.
  – Only one SBO and one VP (optional) assigned for each code.
PET Approver - Source

Lookup in Financial Maintenance menu, Labor Distribution

- Payroll Expense Transfer Department Approvers.
- Set up by org code only.
- Include workgroup or individual approvers, but not both for the same org code and same role.
- Include pre-approvers, approvers, and to-line approvers.
• Supervisor for eStatements and DVQE’s.
• Derived from Workday or KFS Employee Supervisor Table.
  – Default supervisors come from Workday and are updated to the KFS Employee Supervisor table automatically.
  – The KFS supervisor table can be directly updated and the update flag turned off to prevent replacement from Workday updates for either or both supervisors.
KFS Chart of Accounts

Derived from the chart of accounts tables

- Fiscal Officer
- Account Managers
- Account Supervisors
- Account Delegates (updated using security)

Financial Main Menu, Lookup and Maintenance

Chart of Accounts

- Account
- SPA Account
- SPA Code
- SPA Agency
- Account Global
- Account Delegate
- Account Delegate Global
• JV approvers
  – Assigned by JV number in a JV table
  – Can be viewed only from the JV user lookup

• Level 1, 2, and 3 approvers will be identified in the JV lookup by JV number.
Approval Roles

III - UNDERSTANDING ACCOUNT DELEGATES
Account delegates for fiscal officer

- Delegate the fiscal officer approvals for DV and DVQE financial approval only.
  - Primary delegate – only one per account.
  - Secondary delegate – can have multiple per acct.
- Both primary and secondary delegates can be assigned by account or by organization code.
- Account delegates **cannot** approve for the senior business officer/fiscal officer when an edoc is routed for approval per a business rule.
Primary Delegate

• Is acting as the fiscal officer, receiving all action list items instead of the fiscal officer for those edocs that can be approved by a delegate.
  – The fiscal officer will not see the edocs in his/her action list without specifically selecting the delegate.
  – The route node in the edoc indicates delegate for fiscal officer.

• Should be chosen as the person who should be approving the transactions on a routine basis.

• The primary delegate’s backup is the fiscal officer or the secondary delegate.
• The fiscal officer is always able to approve the edoc even if there is a primary or secondary delegate assigned.

• The fiscal officer can set the Primary Delegate Filter to show items for the primary delegate.
• On Action List Page select the primary delegate by name from the available list, or select all delegates.
Secondary Delegates

- Serve as the backup to the primary delegate and the fiscal officer.
- Cannot receive action list items or notifications by default, but can set preferences and actively use filter option to see those edocs in his/her action list.
- Accounts can have multiple secondary delegates, when needed.
• The *secondary delegate* chooses the fiscal officer’s name from the pull-down list “Choose Secondary Delegation”.

• The “delegator” appears on that list and is the fiscal officer, because that is the person passing on authority, or delegating to another person.
• The action list item is routed to the primary delegate, or to the fiscal officer if there is no primary delegate assigned.

• The annotation in the route log identifies the account number and describes the role, either fiscal officer or primary delegate.

• If there is a secondary delegate, the lower portion of that tab will show the secondary delegates - “Delegation of: KFS-SYS Fiscal Officer SC....”, so you must expand the tab to see that annotation.
The column “Account Delegate Primary Route” will contain “Yes” for primary delegates and “No” for secondary delegates.

A start date also applies to indicate when the delegate was updated, which should be every day that the update process is run.

Each delegate is listed twice, once for DV document types, and once for DVQE document types.
Part 4- Alternates and Backups

IV - CREATING AN ALTERNATE OR SUBSTITUTE FOR A ROLE
How to delegate

- Ways to delegate:
  - Add other members who “share” the role as backup to each other.
  - Delegate the role by assigning a substitute from within the process.
  - Assign a specific delegate role.

- Not all roles can be delegated.
  - Supervisors cannot be delegated.
  - Some roles allow only one member per qualifier.
Backup security

• Assigning the same security and exactly the same specifications to more than one person can create backup role assignments.
• Not all roles allow more than one member.
• It is important to know if a role designed for approval will require each and every member to approve a single edoc.
  – If each member must approve, you can assign the role to a group and only one member of the group must approve, because the group acts as one person.
  – Group members need to work out their own method for who will be approving which edocs and when.
Setting up a backup

• Using the same security and exactly the same specifications for more than one user can be effective when used as a backup, as long as it is designed and used correctly.

• Users with the same roles and security may receive the same action list items so they need to understand who approves what and when.

• Effective backup means anyone in the group of users can approve, but only one of them is required to approve the edoc.
• eFinancial Approver Sequential
  – intended for assignment to a group of users who will be required to provide up to three consecutive approvals for certain dollar amounts.
  – First approval must begin at $0.

• eFinancial Approver Shared
  – intended for assignment to one or more users who are each authorized to provide approval of certain dollar amounts for which only one approval level is required.
  – Do not apply dollar thresholds that overlap one another, as this will create redundant approvals.
• Choose either shared or sequential and follow the same approval model for everyone within the budget unit.
• Can be set at account or org code levels and at various dollar thresholds.
• When an approver is going to be absent, he/she can delegate their approvals on a temporary basis within eMarket to someone else with the appropriate approver roles.
Groups vs Individuals

• Some roles can be assigned to more than one user without requiring that each user take action, which works well for backup role assignments.

• For other roles that require each user to approve, the role can be assigned to a group and users can be members of the group, so that only one member of the group must approve.

• Pcard reallocation is a good example where duplicated org codes and roles assigned to more than one individual can work effectively as backup, because users can use the edoc descriptions to choose the edocs to approve.
Multiple Users setup

• The following are examples where multiple users can have the same role, but only one is required to take action.
  – JV users.
  – eStatement SBO Reviewer
  – eStatement Business Office Reviewers.
  – VP approvers
  – DV/DVQE Organization Reviewer.
  – Pcard reallocators.
Group Assignments

• When group assignments are chosen, it is usually because the role requires that each principal with that role must approve the edoc.

• Group role assignments - Examples
  – PET approvers
  – SBR approvers

• It is important that the same role is not assigned to both a group and individual users.

Catherine Maddaford, 1/13/2016
Avoid Overlapping

- The following are examples of overlapping approval setup that can cause redundant or confusing approvals.
  - Assigning account and org approver to the same person where the account belongs to the assigned org codes.
  - Using account masks and 10-digit accounts in the same security that cover the same accounts.
  - Assigning primary delegates by org and then again by account for the accounts within that same org.
  - Assigning a fiscal officer as account delegate.
Some roles have only one choice and do not have an option to delegate.

- Supervisor roles cannot be delegated or substituted, but there can be different supervisors assigned for pcard eStatements and DV/DVQE approval.
- SBO approver - chart of accounts requests.
- SBO approvals - Fiscal officer
Part 5 – Making changes

V – TIPS FOR REQUESTING CHANGES
Planning

- All roles can be widely varied with different purposes, so know your processes and modules well.
- Set up a plan for backup of approval roles when someone is out for longer periods of time.
- Add notes and communicate clearly on the User access request documents.
- Work directly with your users in your department to help them understand and identify their access needs.
How do we change fiscal officer?

- Must be the Senior Business Officer (SBO) or someone designated by the SBO with sufficient knowledge and authority to perform duties, and they must be “hands on” in the system to take action when needed.
- Can be assigned to all accounts by org codes or to individual accounts.
- Use Chart of Accounts change request to change individual accounts.
- Use the user access request to change accounts by org code, attaching a list of accounts and instructions for the change.
• When deciding to add a user as an account delegate:
  – Who is the fiscal officer?
  – Are there already delegates assigned?
  – Who is to be primary and who is to be secondary?
• You can assign delegates by organization code, which means they will be set for all account in that organization code, or by account, which means you need to list account numbers or account number masks on the access application.
• Do NOT overlap primary delegates by choosing both account and org code delegates that cover the same accounts.
• Verify that there is not already a primary delegate for that account.
• Do not assign the same person as primary delegate who is already the fiscal officer, since that is redundant.
• Remove a primary delegate before you add a new one because the system will show and add another delegate but only the first one added will actually work.
• Use the delegate lookup to verify by person or by account.
• Most errors in access applications happen because the person completing the application does not carefully review what access the applicant already has.

• Make sure your application contains only the access that you need to either add or delete, nothing else.

• If you copy a previous application be sure to delete what was already processed.
Run access reports

- Security reports in Kuali are helpful to look up groups of users by home department, or to look up access for a specific account or org code.
- If you are an access coordinator or SBO and do not have the KIM report viewer role, submit an access request for the role, using “other” as the category and listing the role name, and number, if known.