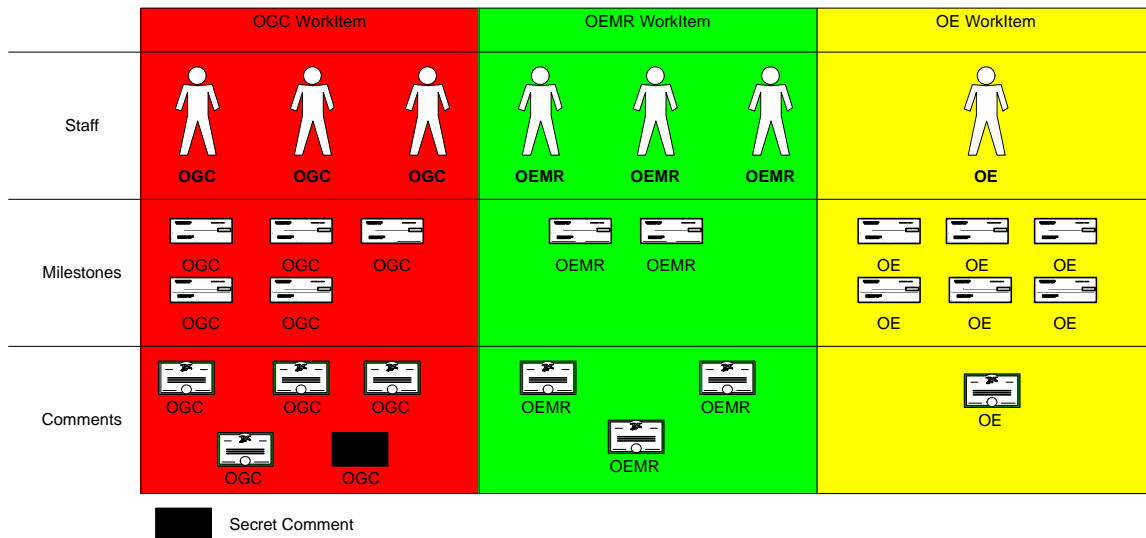


# ATMS Paradigm Shift

The decision to share WorkItems between program offices and the subsequent requirements to secure elements within a WorkItem has severe design consequences that will significantly impact the schedule for ATMS Version 2.0 (e.g. Milestones).

## The Original Design

The approved design for ATMS put the burden of security at the WorkItem level. As such, security was designed at the form level; if you have rights to a WorkItem, you can see and manipulate it and its related elements in the WorkItem form. The WorkItem form was designed with multiple tabs, each containing various elements, based on the paradigm of security by access to the form.



**Figure 1: In the original design, each Program Office has its own WorkItem and security is enforced by assignment to it.**

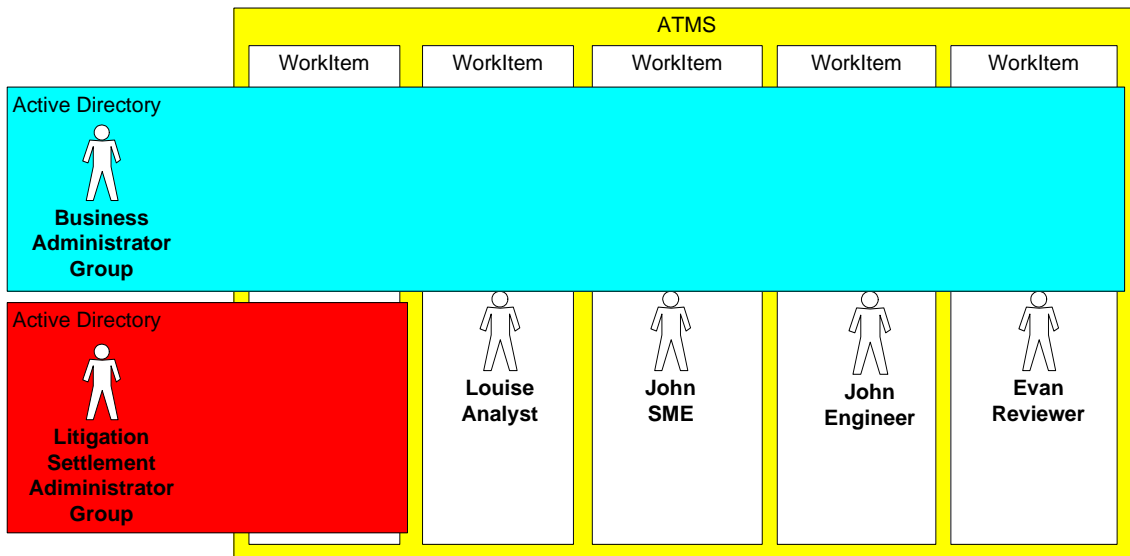
Form access was designed to be controlled by dynamic assignment of rights to designated staff by the assignment of roles. This dynamic assignment reduced the administrative cost of the system by removing the need for significant, continuous static group maintenance in Active Directory. The dynamic assignment of WorkItem access and security rights dramatically reduces the security schema maintenance and provides a more flexible solution which allows end-users the capability to administrate access.

Although at a glance security access via static group membership appears to be less burdensome, with the influx of additional security groups, the assurance of accurate group membership and the maintenance of overall data over time makes this solution less secure.

## Design Dilution

Working within the one “WorkItem per Program Office” paradigm, ATMS, additional WorkItem form tabs were created in order to accommodate specific groups, and new static security groups were created Active Directory for access to these specific tabs, but access to all other tabs was defined by assignment of FERC Staff to the WorkItem.<sup>1</sup>

The Correspondence Administrator and Litigation Settlement Administrator groups were implemented to allow specific members of OEA and OAL specifically access to the screens that were designed for their Program Office specific needs and to ease their transition to ATMS.



**Figure 2: Additional static groups were added to the original design to accommodate specific Program Office needs.**

The method employed for these specific cases was not intended as a precedent for creating other specialty screens and additional ongoing maintenance requirements. The implementation of the needed functionality was to be revisited and migrated, where appropriate, into the standard ATMS methodology.

Based on the findings from the recent Training Role Mapping Analysis exercise and the Program Office Specific Screen sessions, the form based security model no longer matches expectations.

---

<sup>1</sup> The only exception to this rule is a strict separation between Advisory and Litigation work. Litigation WorkItems cannot be viewed by Advisory staff, but Advisory WorkItems can be viewed by Litigation staff.

## Paradigm Shift: Access Privileges

The object ownership issue is further compounded by access privileges granted to the staff of the different program offices.

The original design of ATMS planned for Business Administrators to assign Team Leaders to a WorkItem, who in turn would assign Team Members to that WorkItem. The assigned staff would then track the progress of the WorkItem by entering Milestone and Comment information. This was the vision conceived by the ATMS Working Group during the Phase I Requirements and Design sessions.

During an exercise to determine the number of people who would need to be trained at the various pre-defined security levels<sup>2</sup>, it was determined that the generic security groups did not align to the various program offices in the same way. While some program offices envision using the system as designed, other program offices have more restrictive access with respect to WorkItem participants in combination with one or more static groups to perform data entry on the participants' behalf.

### Access Priviledges Shift Example



















In Figure 4 below:

- Three program offices (A, B, and C) have identified that their WorkItem participants have read only access
- Two program offices (D and E) grant their staff full access to the WorkItems.<sup>3</sup>
- Program Office A has established three static administrative groups to perform various system activities on Program Office A WorkItems.
- Program Office B has established a static group to perform data entry functions for Program Office B staff.

---

<sup>2</sup> Business Administrator, Team Leader, Team Member, and Read Only Member were identified in the Phase I Requirements and Design sessions as generic security levels.

<sup>3</sup> Full access for team members allows for the ability to create and maintain Milestones and Comments.

ATMS					
	Read Only Program Office A WorkItem	Read Only Program Office B WorkItem	Read Only Program Office C WorkItem	Full Access Program Office D WorkItem	Full Access Program Office E WorkItem
Active Directory Business Administrator					
Active Directory Read Only Program Office A Group 1 Has all rights to Program Office A WorkItems only	All Rights				
Active Directory Read Only Program Office A Group 2 Has rights to assign staff in Program Office A WorkItems only	Staff Assignment only				
Active Directory Read Only Program Office A Group 3 Has data entry rights to Program Office A WorkItems only	Data Entry only				
Active Directory PO B Group 1 Has data entry rights to all WorkItems where Program Office B staff are assigned	Data Entry only	Data Entry only	Data Entry only	Data Entry only	Data Entry only
 Participant from Read Only Program Office A  Participant from Read Only Program Office B  Participant from full access Program Office	  	  	  	  	  

**Figure 3: Who Has Rights to Which WorkItems?**

Figure 3 illustrates the situation where personnel from two read only program offices and one from a full access program office are assigned to five WorkItems. Table 1 illustrates the security quandary.

<b>Who Has Access?</b>	<b>Read Only Program Office A WorkItem</b>	<b>Read Only Program Office B WorkItem</b>	<b>Read Only Program Office C WorkItem</b>	<b>Full Access Program Office WorkItem</b>
<b>Active Directory Read Only Program Office Group 1 Has all rights to Program Office A WorkItems only</b>	All Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem
<b>Active Directory Read Only Program Office A Group 2 Has rights to assign staff in Program Office A WorkItems only</b>	Assignment Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem
<b>Active Directory Read Only Program Office A Group 3 Has data entry rights to Program Office A WorkItems only</b>	Data Entry Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem
<b>Active Directory PO B Group 1 Has data entry rights to all WorkItems where Program Office B staff are assigned</b>	Data Entry Rights to WorkItem or No Rights to WorkItem because not specifically assigned?	Data Entry Rights to WorkItem	Data Entry Rights to WorkItem or No Rights to WorkItem because not specifically assigned?	Data Entry Rights to WorkItem, All Rights to WorkItem, or No Rights to WorkItem because not specifically assigned?
<b>Assigned Participant from Read Only Program Office A</b>	No Rights to WorkItem	No Rights to WorkItem (Who does their data entry?)	No Rights to WorkItem (Who does their data entry?)	All Rights to WorkItem or No Rights to WorkItem?
<b>Assigned Participant from Read Only Program Office B</b>	No Rights to WorkItem	No Rights to WorkItem	No Rights to WorkItem	All Rights to WorkItem or No Rights to WorkItem?
<b>Participant from full access Program Office</b>	All Rights to WorkItem, or No Rights to WorkItem?	All Rights to WorkItem, or No Rights to WorkItem?	All Rights to WorkItem, or No Rights to WorkItem?	All Rights to WorkItem

Table 1: Who Has Access?

**Scenario 1: Read Only Program Office A WorkItem**

The first column illustrates a WorkItem for Program Office A. This program office does not allow WorkItem participants to enter information. That function is performed by static administrative groups for Program Office A WorkItems. At issue are:

- The Program Office B participant is also only granted Read Only access to ATMS. There is a static group assigned to do data entry for him, but that static group is not assigned to the WorkItem. **How is this participant's information entered into ATMS?**

**Does the full access participant have full access to the Program Office A WorkItem? If not, how is this participant's information entered into ATMS? Scenario 2: Read Only Program Office B WorkItem**

The second column illustrates a WorkItem for Program Office B. This program office also does not allow WorkItem participants to enter information. That function is performed by a static administrative group for Program Office B personnel. At issue here are:

- The Program Office A participant is only granted Read Only access to ATMS. The static group assigned to do data entry for her only has access to Program Office A WorkItems. **How is this participant's information entered into ATMS?**
- **Does the full access participant have full access to the Program Office B WorkItem? If not, how is this participant's information entered into ATMS?**

**Scenario 3: Read Only Program Office C WorkItem**

The third column illustrates a WorkItem for Program Office C. This program office also does not allow WorkItem participants to enter information. At issue here are:

- The Program Office A participant is only granted Read Only access to ATMS. The static group assigned to do data entry for her only has access to Program Office A WorkItems. **How is this participant's information entered into ATMS?**
- The Program Office B participant is also only granted Read Only access to ATMS. There is a static group assigned to do data entry for him, but that static group is not assigned to the WorkItem. **How is this participant's information entered into ATMS?**

**Scenario 4: Full Access Program Office WorkItem**

The fourth column illustrates a WorkItem for a full access Program Office where WorkItem participants are expected to enter information themselves. At issue here are:

- The Program Office A participant is only granted Read Only access to ATMS. The static group assigned to do data entry for her only has access to Program Office A WorkItems. **How is this participant’s information entered into ATMS?**
- The Program Office B participant is also only granted Read Only access to ATMS. There is a static group assigned to do data entry for him, but that static group is not assigned to the WorkItem. **How is this participant’s information entered into ATMS?**

**Summary**

Table 2 Summarizes the Access Privileges Issue.

Who Can Enter Data?	PO A (Read Only)	PO B (Read Only)	PO C (Read Only)	Full Access PO
PO A Admin Group	Yes	No	No	No
PO A Assignment Group	Yes	No	No	No
PO A Data Entry Group	Yes	No	No	No
PO B Data Entry Group	?	Yes	?	?
PO A Participant	No	No	No	?
PO B Participant	No	No	No	?
Full Access PO Participant	?	?	?	Yes

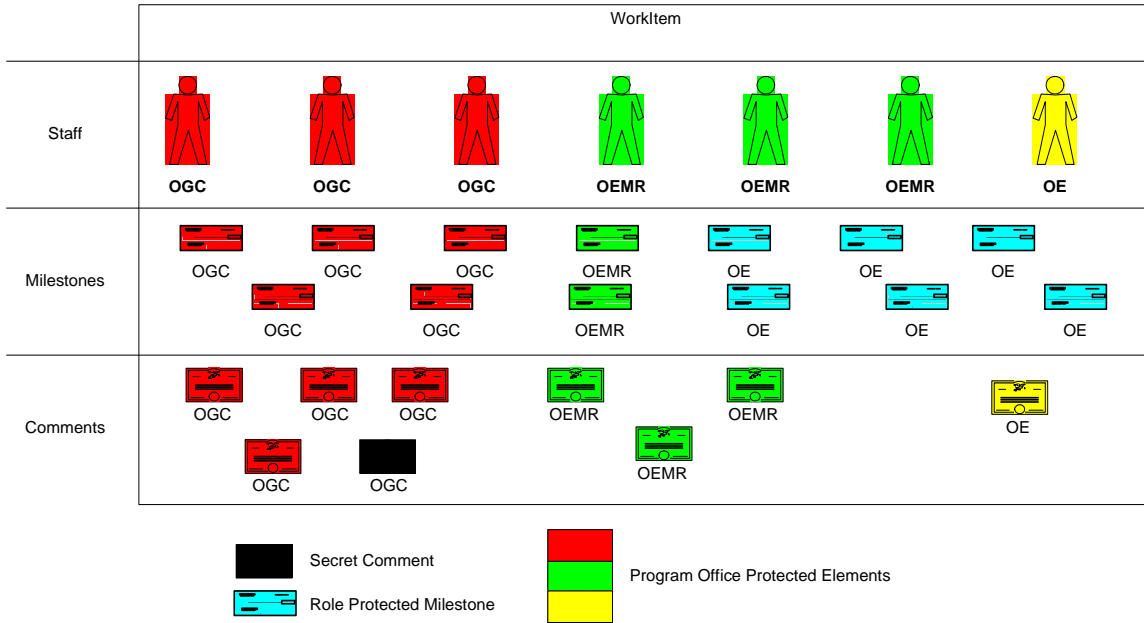
Table 2: Access Privileges Issue Summary

**Paradigm Shift: Object Ownership**

The Access Privileges Issue is compounded by the much more granular security approach suggested by the following requirements:

- The system shall provide the ability to mark certain Milestones as public.
- The system shall allow a Milestone type to be associated with specific ATMS roles such that these Milestones can only be edited by the personnel assigned that role.

These requirements have a broad impact on the system design as illustrated in Figure 4.



**Figure 4: Program Office Protected Data Elements add additional levels of complexity to the security model.**

Using this more granular security approach, individual data elements could be exclusively controlled by ATMS Roles, Program Office assignment<sup>4</sup>, or Active Directory group membership, and would require a significant system administration effort to maintain.

### Paradigm Shift: The Complete Picture

When the Access Privilege and Object Ownership Paradigm Shifts are combined, the result is an untenable security quagmire. As illustrated in Table 3.

<sup>4</sup> Program office assignment is controlled by MAPS.

Who Has Access?	PO A WorkItem			PO B WorkItem			PO C WorkItem			PO E WorkItem		
	PO A Milestone	PO B Milestone	PO D Role-Based Milestone	PO A Milestone	PO B Milestone	PO D Role-Based Milestone	PO A Milestone	PO B Milestone	PO D Role-Based Milestone	PO A Milestone	PO B Milestone	PO E Role-Based Milestone
PO A Admin Group	Yes	?	?	?	No	No	?	No	No	?	No	No
PO A Assignment Group	Yes	?	?	?	No	No	?	No	No	?	No	No
PO A Data Entry Group	Yes	?	?	?	No	No	?	No	No	?	No	No
PO B Data Entry Group	?	?	?	?	Yes	?	No	?	No	No	?	?
PO A Participant	No	No	No	No	No	No	No	No	No	No	No	?
PO B Participant	No	No	No	No	No	No	No	No	No	No	No	?
PO E Participant (assigned Role)	?	?	?	?	?	?	?	?	?	?	?	Yes
Full Access PO Participant (not assigned Role)	?	?	?	?	?	?	?	?	?	?	?	?
	?	= one or more rules in conflict										

**Table 3: The Complete Paradigm Shift Picture**

Program Office A	WorkItems are Read Only to Team Members. Active Directory Groups allow editing of Program Office A WorkItems Only.
Program Office B	WorkItems are Read Only to Team Members. Active Directory Group allows editing of all WorkItems Program Office B personnel are assigned to.
Program Office C	WorkItems are Read Only to Team Members.
Program Office E	Team Members have full rights to edit WorkItems.
PO A Participant	Has Read-Only access to ATMS.
PO B Participant	Has Read-Only access to ATMS.
Full Access Participant	Has full rights to edit WorkItems.

## Appendix A: Original CRUD Table

ATMS Functional Processes Mapped by Forms/Screens

Functional Processes	Security Groups							
	Sys Admin	OSEC Admin	Business Admin	Correspondence Admin	Litigation Settlement Admin	Team Leader	Team Member	Read Only Member
Maintain Lookup Tables	C, R, U, D	-	-	-	-	-	-	-
Maintain Milestone	C, R, U, D	-	-	-	-	-	-	-
Maintain Milestone Business Rules	C, R, U, D	-	-	-	-	-	-	-
Comment	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
Milestone	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
Product Category	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R	R	R
Product SubCategory	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R	R
Staff	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R	R
Role	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R	R
WorkItem Create	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	-	-	-
WorkItem Detail	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	R, U	R, U	R
WorkItem Complete	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	R	R	R
Docket Workset Create	C, R, U	C, R, U	-	-	-	-	-	-
Non-Docket Workset Create	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	R	R	R
Docket Workset Detail	C, R, U	C, R, U	R	R	R	R	R	R
Non-Docket Workset Detail	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	R	R	R
Correspondence Workset Create	C, R, U	C, R, U	-	C, R, U	-	-	-	-

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

Functional Processes	Security Groups							
	Sys Admin	OSEC Admin	Business Admin	Correspondence Admin	Litigation Settlement Admin	Team Leader	Team Member	Read Only Member
Correspondence Workset Detail	C, R, U	C, R, U	R	C, R, U	R	R	R	R
Litigation Comments	C, R, U	C, R, U	R	R	C, R, U, D	R, U	R	R
Litigation Detail	C, R, U	C, R, U	R	R	C, R, U, D	R, U	R	R
Litigation Complete	C, R, U	C, R, U	R	R	C, R, U	R	R	R
Settlement	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

## Appendix B: Revised CRUD Matricies

<b>Business Admin</b>	ATMS	OGC	OEP- DG2E	OEP- DPC	OEP-M & O	OEMR Case Tracking	OEMR Admin	OEMR Case Assigners
Maintain Lookup Tables	-	-	-	-	-	-	<b>C, R, U, D</b>	-
Maintain Milestone	-	-	-	-	-	-	<b>C, R, U, D</b>	-
Maintain Milestone Business Rules	-	-	-	-	-	-	<b>C, R, U, D</b>	-
Comment	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D
Milestone	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D
Product Category	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	<b>R, U</b>
Product SubCategory	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	<b>R, U</b>
Staff	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D
Role	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D
WorkItem Create	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	<b>R, U</b>	<b>C, R, U, D</b>	<b>R</b>
WorkItem Detail	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	<b>C, R, U, D</b>	<b>C, R, U, D</b>	C, R, U
WorkItem Complete	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	<b>C, R, U, D</b>	<b>C, R, U, D</b>
Docket Workset Create	-	-	-	-	-	-	-	-
Non-Docket Workset Create	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	<b>C, R, UD</b>	<b>R</b>
Docket Workset Detail	R	R	R	R	R	<b>C, R, U</b>	<b>C, R, U, D</b>	R
Non-Docket Workset Detail	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	C, R, U	<b>C, R, U, D</b>	C, R, U
Correspondence Workset Create	-	-	-	-	-	-	-	-
Correspondence Workset Detail	R	R	R	R	R	R	<b>C, R, U</b>	R
Litigation Comments	R	-	-	-	-	R	R	R
Litigation Detail	R	-	-	-	-	R	R	R
Litigation Complete	R	-	-	-	-	R	R	R
Settlement	C, R, U, D	C, R, U, D	-	-	-	-	C, R, U, D	C, R, U, D

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

Correspondence Admin	ATMS	OGC	OEP-M & O	DRS	OEMR
Maintain Lookup Tables	-	-	-	-	-
Maintain Milestone	-	-	-	-	-
Maintain Milestone Business Rules	-	-	-	-	-
Comment	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
Milestone	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
Product Category	C, R, U, D	R	C, R, U, D	C, R, U, D	R
Product SubCategory	C, R, U, D	R	C, R, U, D	C, R, U, D	R
Staff	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
Role	C, R, U, D	C, R, U, D	C, R, U, D	C, R, U, D	R
WorkItem Create	C, R, U	R	C, R, U	<b>C, R, U, D</b>	-
WorkItem Detail	C, R, U	R	C, R, U	<b>C, R, U, D</b>	R
WorkItem Complete	C, R, U	R	C, R, U	<b>C, R, U, D</b>	R
Docket Workset Create	-	-	-	????-	-
Non-Docket Workset Create	C, R, U	R	-	<b>C, R, U, D</b>	R
Docket Workset Detail	R	R	-	<b>C, R, U, D</b>	R
Non-Docket Workset Detail	C, R, U	R	-	<b>C, R, U, D</b>	R
Correspondence Workset Create	C, R, U	R	C, R, U	<b>C, R, U, D</b>	-
Correspondence Workset Detail	C, R, U	R	C, R, U	<b>C, R, U, D</b>	R
Litigation Comments	R	-	-	R	R
Litigation Detail	R	-	-	R	R
Litigation Complete	R	-	-	R	R
Settlement	C, R, U, D	R	R	C, R, U, D	R

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

Team Leader	ATMS	OGC	OEP-DHL and DHAC	OEMR
Maintain Lookup Tables	-	-	-	-
Maintain Milestone	-	-	-	-
Maintain Milestone Business Rules	-	-	-	-
Comment	C, R, U, D	<b>C, R, U</b>	C, R, U, D	<b>R</b>
Milestone	C, R, U, D	R	C, R, U, D	<b>R</b>
Product Category	R	R	<b>R, U,</b>	R
Product SubCategory	C, R, U, D	R	C, R, U, D	<b>R</b>
Staff	C, R, U, D	R	C, R, U, D	<b>R</b>
Role	C, R, U, D	R	C, R, U, D	<b>R</b>
WorkItem Create	-	-	<b>C, R, U, D</b>	-
WorkItem Detail	R, U	R	<b>C, R, U, D</b>	<b>R</b>
WorkItem Complete	R	R	<b>C, R, U, D</b>	R
Docket Workset Create	-	-	-	-
Non-Docket Workset Create	R	R	R	R
Docket Workset Detail	R	R	R	R
Non-Docket Workset Detail	R	R	R	R
Correspondence Workset Create	-	-	-	-
Correspondence Workset Detail	R	R	R	R
Litigation Comments	R, U	-	-	R
Litigation Detail	R, U	-	-	R
Litigation Complete	R	-	-	R
Settlement	C, R, U, D	R	-	R

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

Team Member	ATMS	OGC	OEP-DHL and DHAC	OEMR
Maintain Lookup Tables	-	-	-	-
Maintain Milestone	-	-	-	-
Maintain Milestone Business Rules	-	-	-	-
Comment	C, R, U, D	<b>C, R, U</b>	C, R, U, D	R
Milestone	C, R, U, D	R	C, R, U, D	R
Product Category	R	R	R	R
Product SubCategory	R	R	R	R
Staff	R	R	R	R
Role	R	R	R	R
WorkItem Create	-	-	-	-
WorkItem Detail	R, U	R	R, U	R
WorkItem Complete	R	R	R	R
Docket Workset Create	-	-	-	-
Non-Docket Workset Create	R	R	R	R
Docket Workset Detail	R	R	R	R
Non-Docket Workset Detail	R	R	R	R
Correspondence Workset Create	-	-	-	-
Correspondence Workset Detail	R	R	R	R
Litigation Comments	R	-	-	R
Litigation Detail	R	-	-	R
Litigation Complete	R	-	-	R
Settlement	C, R, U, D	R	-	R

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.

Read Only	ATMS	OGC	OEP- DG2E	OEP-DHL/ DHAC	OEP- DPC	OEMR
Maintain Lookup Tables	-	-	-	-	-	-
Maintain Milestone	-	-	-	-	-	-
Maintain Milestone Business Rules	-	-	-	-	-	-
Comment	R	<b>C, R, U</b>	R	R	R	R
Milestone	R	R	R	R	R	R
Product Category	R	R	R	R	R	R
Product SubCategory	R	R	R	R	R	R
Staff	R	R	R	R	R	R
Role	R	R	R	R	R	R
WorkItem Create	-	-	-	-	-	-
WorkItem Detail	R	R	R	R	R	R
WorkItem Complete	R	R	R	R	R	R
Docket Workset Create	-	-	-	-	-	-
Non-Docket Workset Create	R	R	R	R	R	R
Docket Workset Detail	R	R	R	R	R	R
Non-Docket Workset Detail	R	R	R	R	R	R
Correspondence Workset Create	-	-	-	-	-	-
Correspondence Workset Detail	R	R	R	R	-	R
Litigation Comments	R	-	-	-	-	R
Litigation Detail	R	-	-	-	-	R
Litigation Complete	R	-	-	-	-	R
Settlement	R	R	-	-	-	R

C = Create, R = Read, U = Update, D = Delete

The Gray column illustrates the rights granted by the original design.

The Yellow cells indicate changes from the original design.

Rights in bold indicate new rights to be assigned.