# Quick EPM Security Guide

Purpose: This document was created to serve as a quick reference for security operators. It is intended to discuss how an EPM user will use the system and how the security was developed to restrict the user's page and data access.

Functionality: The EPM tool is contains a number of Reporting Tables that were developed by the EPM team. These Reporting Tables are denormalized versions of delivered PeopleSoft tables. The idea was to make it easier for users to develop reports by consolidating that data into fewer tables.

They will use the delivered PS Query Tool to develop their reports. To do so the will follow this navigation:

REPORTING TOOLS > QUERY > QUERY MANAGER
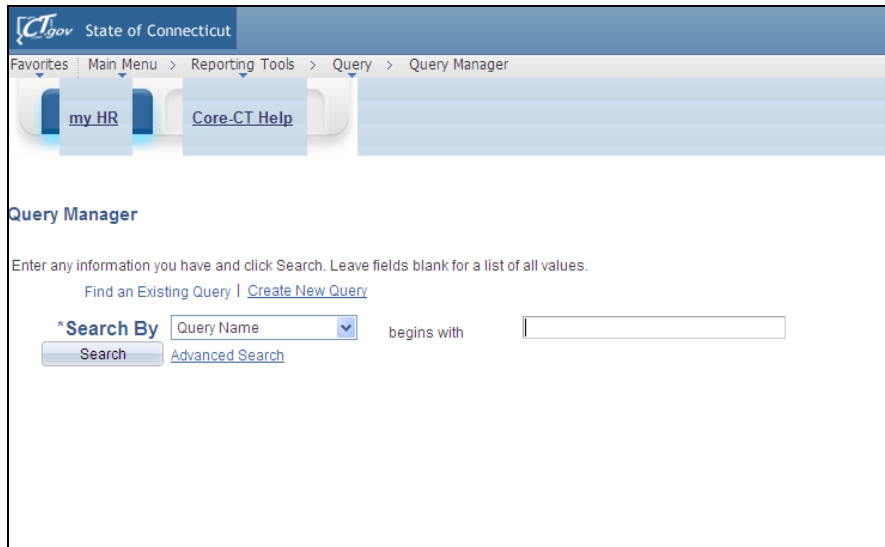
Another tool the users will be using is the EPM Data Dictionary. This allows the users to research the data on all the new reporting tables. A screen shot of this tool is below. Users will access this tool using the following navigation:

REPORTING TOOLS > EPM DATA DICTIONARY

epm_quick_sec_guide9_1.doc
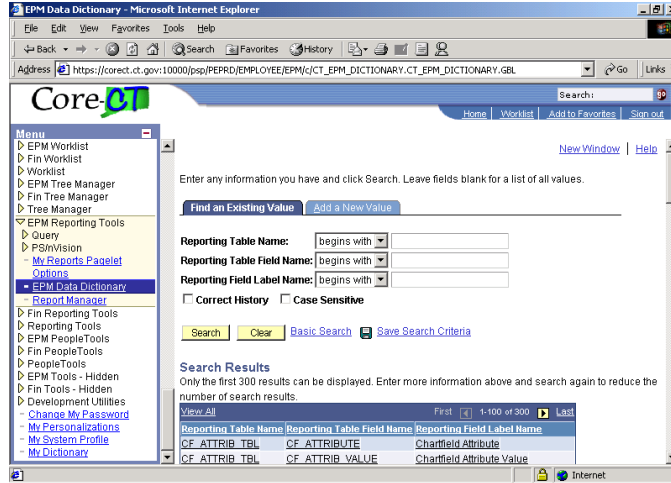
Security: Data and Pages are secured through a variety of ways.

All EPM users will receive the following two roles in EPM which drive their page and non-page access:

CT EPM USER -- Grants access to all Non-Page Permissions (Web Libraries, Component Interfaces etc), the EPM Data Dictionary and the PS Query tool.

CT EPM PRIVATE -- Allow a user to create only Private Queries. This means no other user will have access to see, modify, run or delete this users report.

The user will be given access to data based on the Financials Roles they have and based on their Primary Permission List.

The principle used to determine what tables a user has access to query is the following:

> *If a user has the ability to navigate to any page within a given module that user will be granted the ability to query off every Reporting table in that module.*

For instance if a user has the Vendor Viewer Role, they have access to all Accounts Payable Reporting Tables.

This access was given by create Query Tree and granting certain nodes of the query tree to Permission Lists.

Those permission lists were assigned to the appropriate Financials Roles which are sent to EPM via the Portal synchronization Application Engine. For example: Take the Vendor Viewer Role we spoke about earlier. In Financials, the permission lists in that role grant page access to view Vendors whereas in EPM that same role was given the CTAPREPORTING permission list which grants access for that user to query off AP tables.

Finally now that a user was granted access to records, their row level security must be enforced. Just as in Financials a user will be granted a Primary Permission List with identifies what Business Units they can view. This permission list will restrict the results of the queries to these Business Units only.