**Generating Security Access Report - [ SEC001I ]**

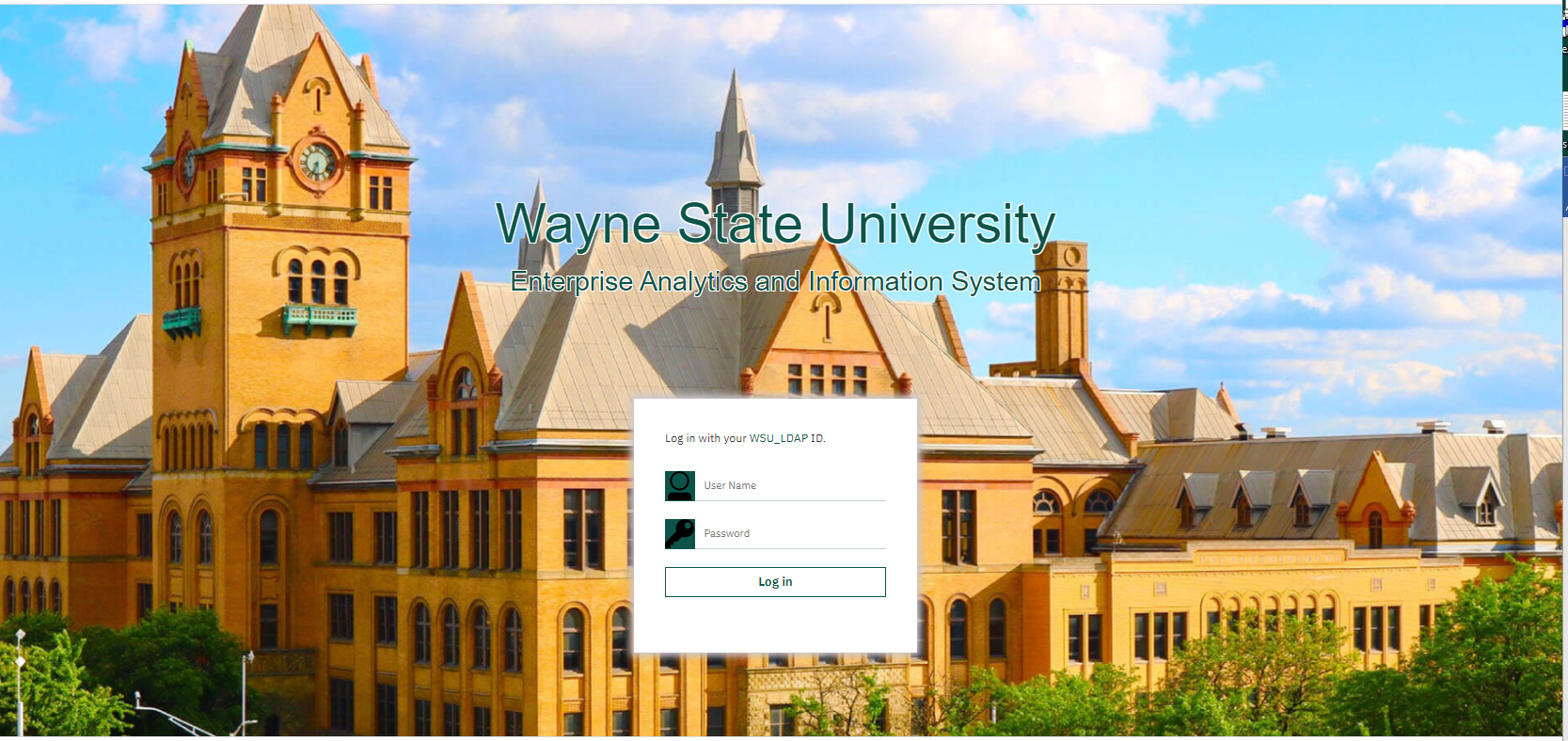
**Purpose**

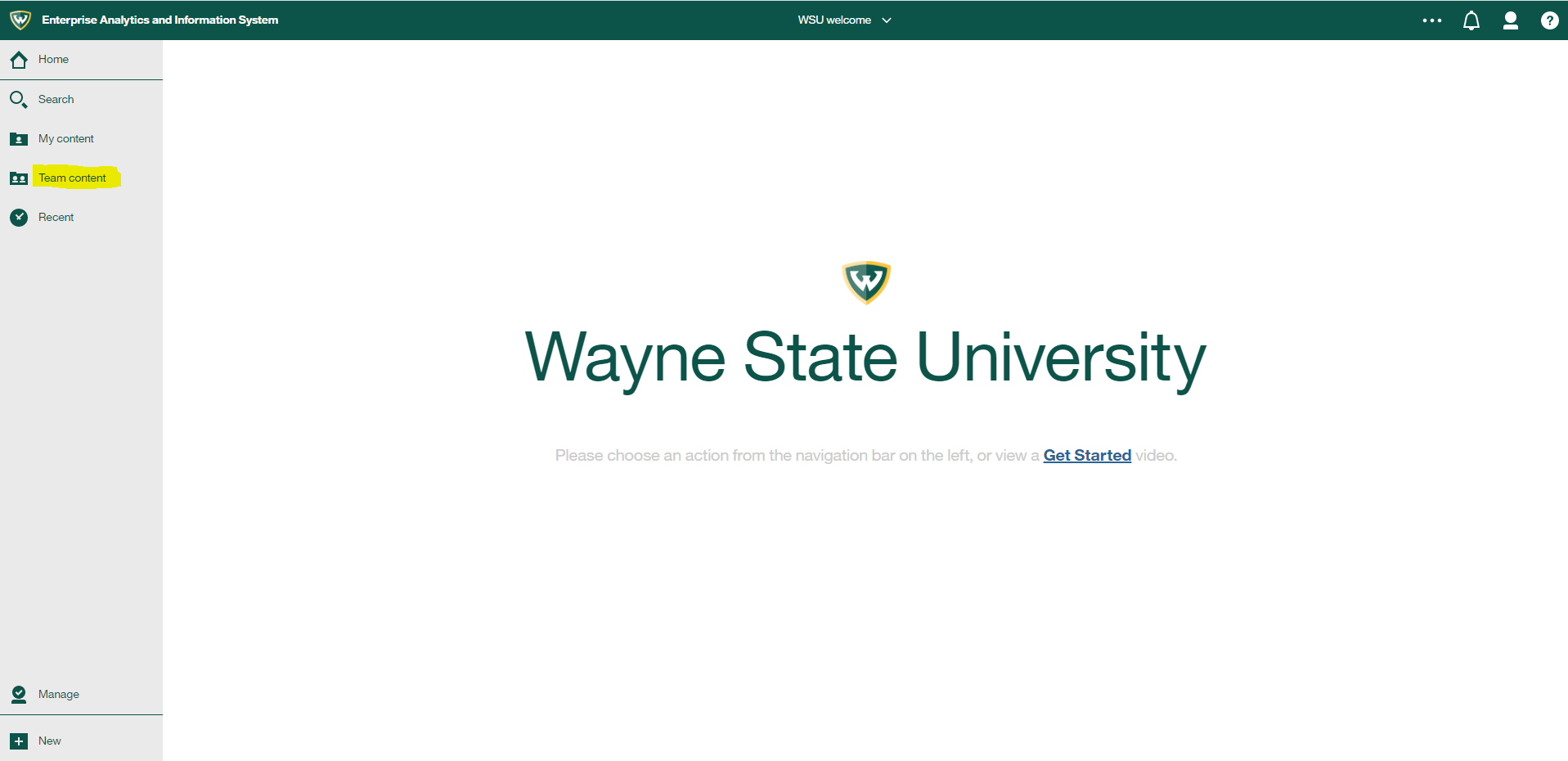
These instructions will cover how to generate and use the Security Access Report. This report will provide the ability to view the access permissions on your staff Position account within the applicable C&IT managed Enterprise Administrative Applications below:

**(Banner, WAYNEBUY, Cognos, ODS, Xtender (Imaging), Workflow, Webtailor, SMARTi, STARS 2.0)**

**Log On to Internet Explorer:** [**https://bireporting.wayne.edu/crn/bi/**](https://bireporting.wayne.edu/crn/bi/) **[Direct URL]**

1. **Log on using your Academica password. Then select Team content folder**

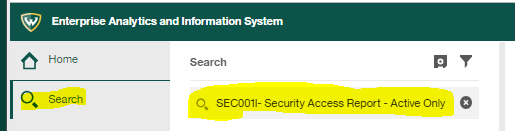




Public Folder Tab: Security Folder

1. Search the **SEC001I - Security Access Report – Active Only**.

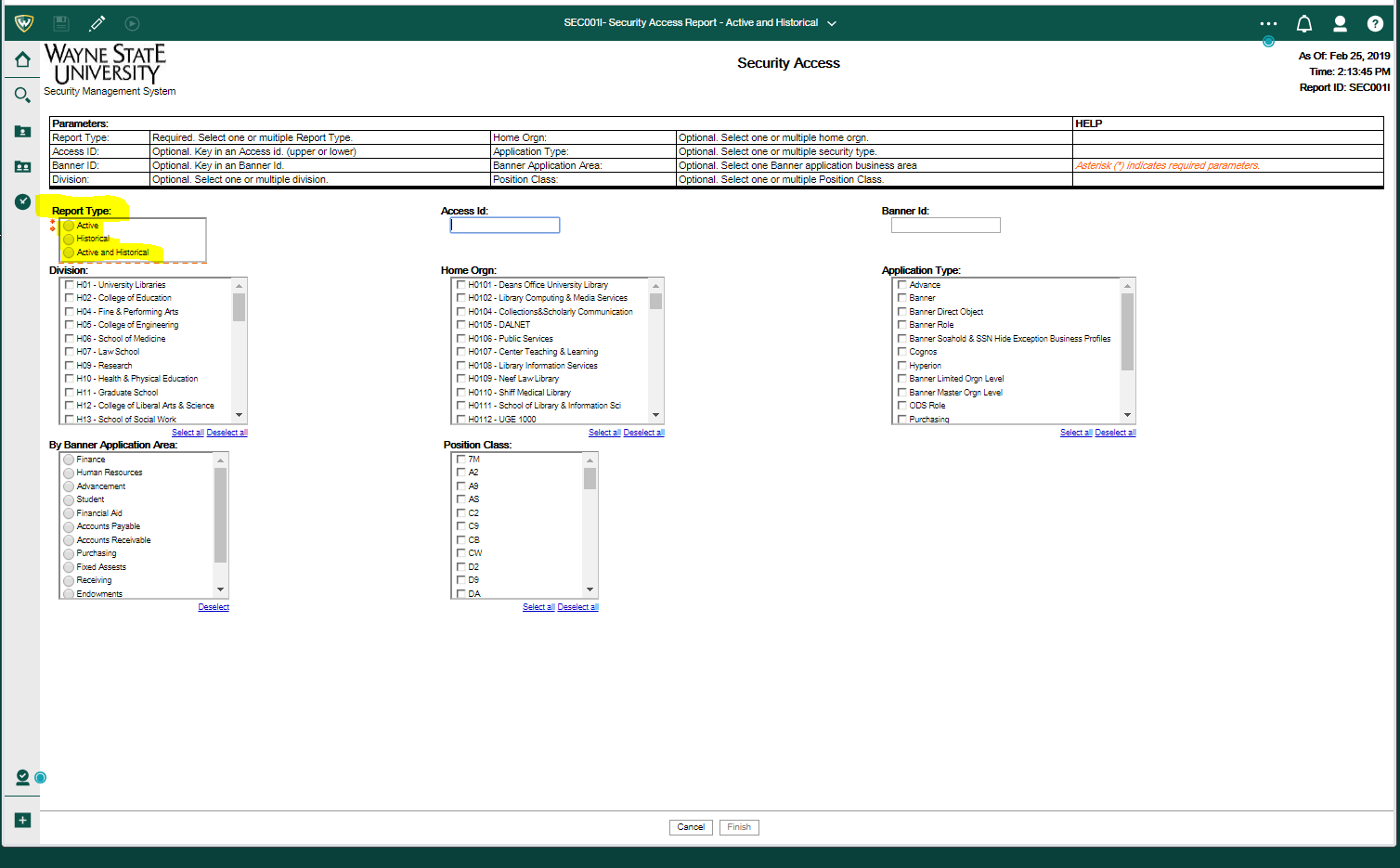




**Report Name: SEC001I**

1. Enter the Parameters instructed below, then select Finish to run report  **SEC001I- Security Access Report – Active Only**

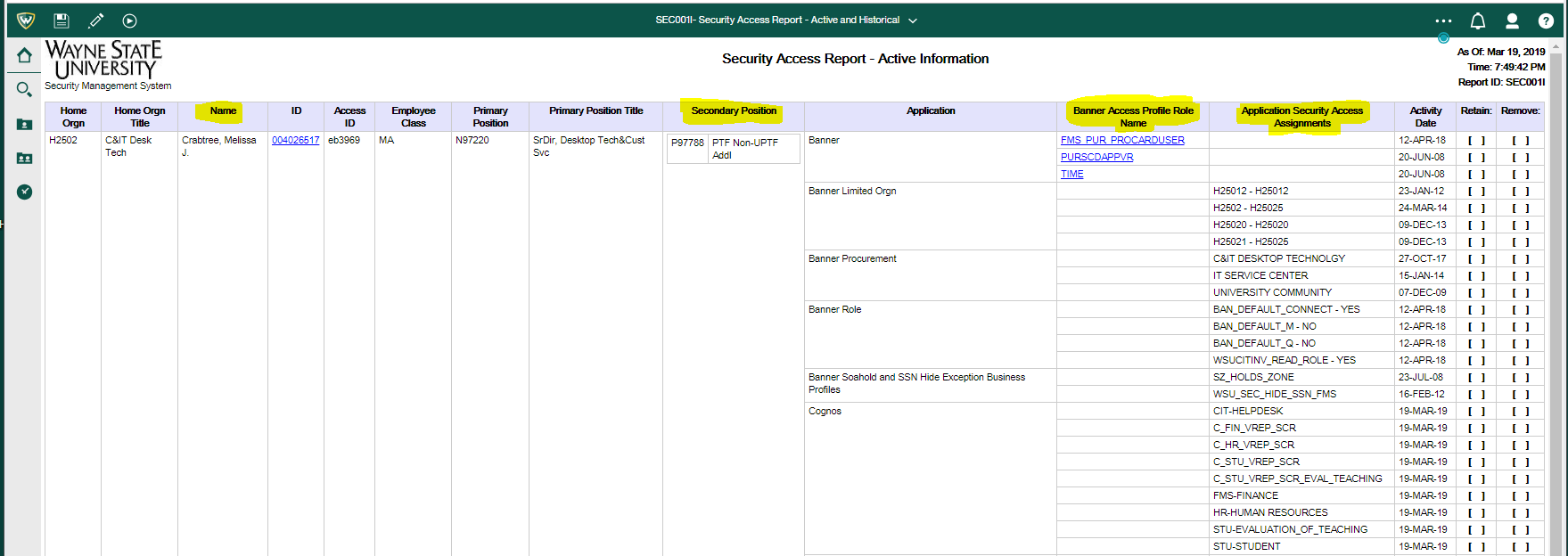
**Report Parameters**



1. **Report Type: Allows 3 difference selections types to run the report: Active, Historical, or both Active and Historical information.**
2. **Access ID: key in an Access ID *(lowercase)* when making an individual selection.**
3. **Banner ID – (Optional): key in a Banner ID when making a selection on a specific Banner ID.**
4. **Division – (Optional): select one *or* multiple Division Home Organization Code(s).**
5. **Home Organization – (Optional): select one *or* multiple Home Organization.**
6. **Application Type – (Optional): default all; when making a specific application selection -- key in one *or* multiple Application areas.**
7. **By Banner Application Area – (Optional): select one preferred data application area.**
8. **Position Class – (Optional): select one position class type.**
9. **Run the report [Finish].**
10. **Save the Security Access Report. [Keep this version]: Email Report**

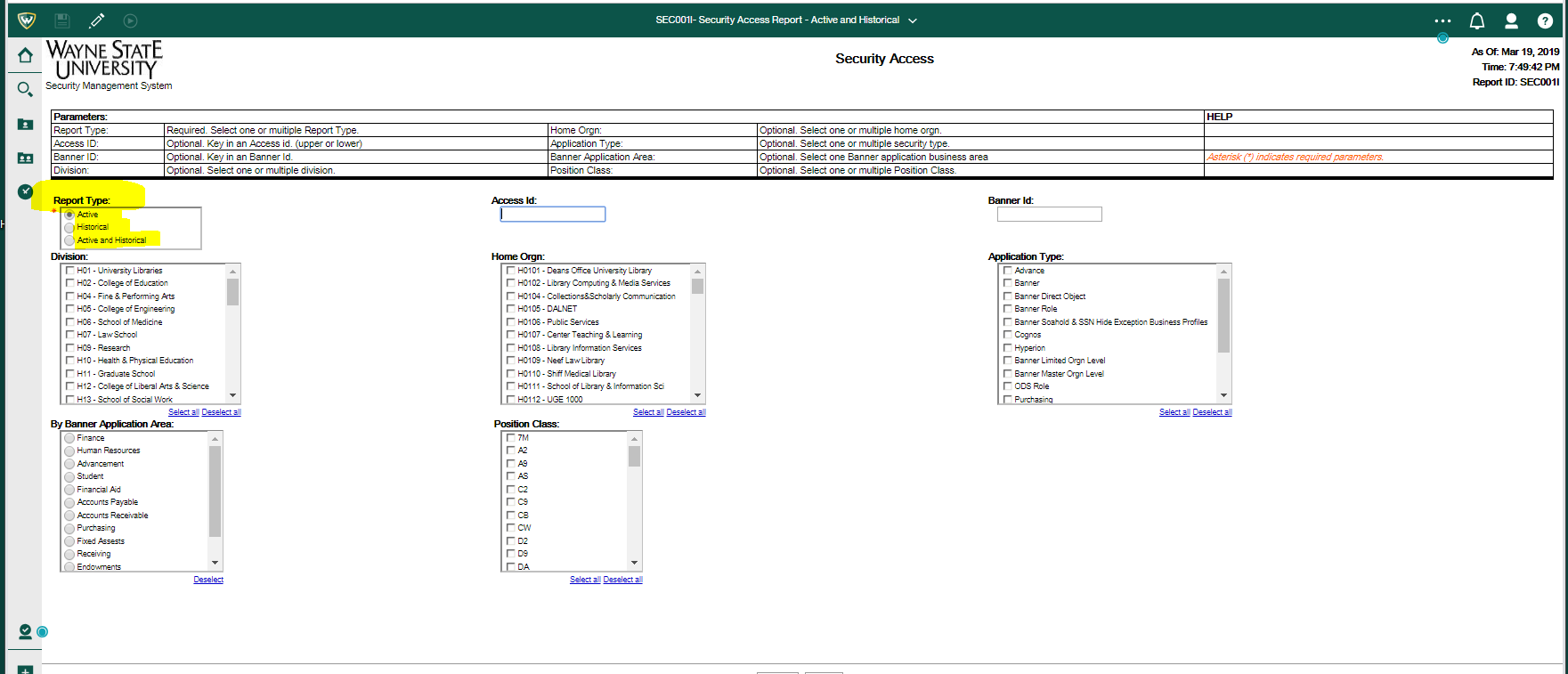
**Report Output Display – See next example screen prints**

* **Home Orgn – Primary Department Organization Code** *[i.e., H49 Human Resources]*
* **Home Orgn Title – Primary Organization Department Name** *[i.e., Asst VP Human Resources/Office]*
* **Name – Employee User Legal Name and Preferred Name, if applicable.**
* **Banner ID – WSU HR Employee ID** *[i.e., 000123456]*
* **Access ID – WSU Academica ID** *[i.e., AA1234]*
* **Employee Class – Employee Job Classification** *[i.e., EX, MA, ]*
* **Primary Position Number – Employee Primary Position Number** *[i.e., N96555]*
* **Primary Position Title – Employee Job Position Title** *[i.e., Associate Vice President]*
* **Secondary Position – Employee Secondary *(or more)* Position / Title**
* **Application – Listing of multiple Administrative Applications assignments.**
* **Banner Access Profile Role Name: Lists the Banner Management Systems - Profile Names as identified on the Access Request Forms.**
* **Application Security Access Assignments - The information behind this column only applies to the Administrative Application Type – Banner Only.**
* **Below are the Administrative Application Types that are currently managed by C&IT Information Security & Compliance - Identity and Access Management:**
* **Advance - Alumni Management System [No longer requested-Contact: Development & Alumni Affairs Office]**
* **Banner - Management System**
* **Banner Direct Object – Object/Form**
* **Banner FMS Accounting - Rule Code Groups [FOMUSRG]**
* **Banner Procurement - Approval Queue [FTMAPPQ]**
* **Banner FMS Default Orgn**
* **Banner FMS Procurement**
* **Banner FMS User Indicator [FOMPROF]**
* **Banner HRS Limited Orgn Levels – Division /Department / Timesheet(s)**
* **Banner HRS User Rule**
* **Banner Master Orgn Level – Can See All Orgns**
* **Banner Role - (Object/Form function: BAN\_DEFAULT\_’Q’uery or ‘M’ Maintenance/Modify)**
* **Banner SOAHOLD and SSN Hide Exception Business Profiles**
* **Banner System Privileges – (C&IT EA Developers Access)**
* **Cognos – Reporting System**
* **Cognos LDAP Group - COGNOSUSERS**
* **Hyperion – REPLACED with Adaptive Insight – managed by Budget Office**
* **LDAP Group Member**
* **ODS - Social Security Number - SSN MASK – Authorization to view SSN reports**
* **ODS Role - Operational Data Store; Banner Applications View Roles**
* **FERPA Acknowledgement Form – DIGITAL FORM ACCEPT [Academica -** [**https://academica.aws.wayne.edu/link/4ep**](https://academica.aws.wayne.edu/link/4ep) **]**
* **SMARTi – COLD-Computer Output to Laser Disc storage by data group**
* **STARS 2.0 - *Roles:* Reporter / Staff / Front Desk / Manager / Advisor**
* **WebTailor**
* **Workflow**
* **Xtender / Imaging**



**EXAMPLE OF IMPROVEMENTS TO SECURITY ACCESS REPORT [SEC001I]**

**#1 – Report Type – There are 3 options: 1) Active; 2) Historical; and 3) Active and Historical.**



**#2 – These column headings have been updated or are new:**

**BEFORE                                                                                   AFTER**

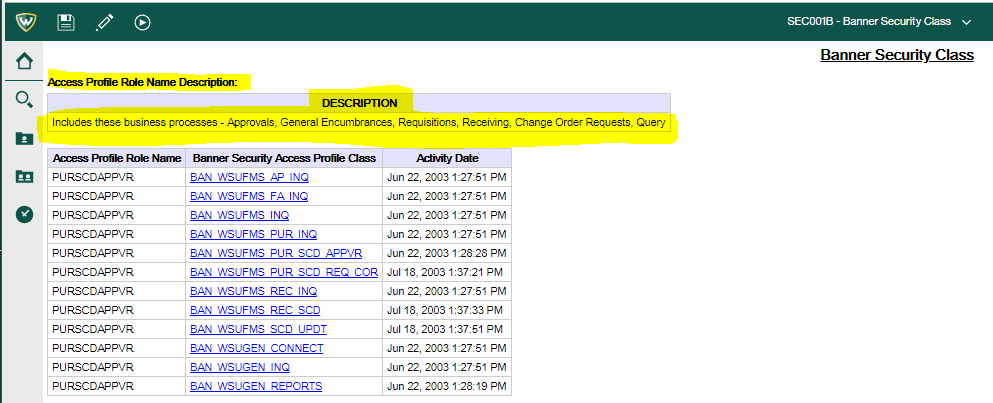
**(NEW) Secondary Position**

**(NEW) Banner Access Profile Role Name**

**Security Class                                             =     Application Security Access Assignments**

**#3 - Example below of description for PURSCDAPPVR and**

**Banner Security Access Profile Classes**



**#4 - Example below of PURSCDAPPVR – Banner Security Access Profile Class:**

**BAN\_WSUFMS\_PUR\_SCD\_APPVR – Objects/Forms Assignment**

