SECURITY REPORTS

from the

CONNECTIONS
DATA WAREHOUSE

Staff Security Report

Business Function Report

Unit Approver Report

Assignee/Designee Report

Overview

and

Instructions

Security Reports Overview

Security reports have been developed in the Data Warehouse to provide users with the ability to monitor staff access to CONNECTIONS. There are four pre-formatted Security Reports that are available from the CONNECTIONS Data Warehouse using Cognos.

These reports are valuable tools for the maintenance of CONNECTIONS security. As a security coordinator performs security maintenance duties, it is important to be able to track which agency staff are in CONNECTIONS, what business functions each staff member has, which staff is a Unit Approver, and whether a staff person is an Assignee or Designee.

There is no automated way for a security coordinator to obtain this information within the CONNECTIONS application. A local security coordinator would have to access three different windows to view the Staff Detail, Staff Security and Unit Detail, and even then could not see, at one time, all of the business functions assigned to a particular worker. Also, the local security coordinator has no way to see more than one worker's Business Function Profile (BFP) at the same time. Seeing more than one worker's BFP at one time would enable the security coordinator to more easily determine the appropriate mix of business functions for a particular unit. (Note: A business Function Profile, or BFP, is the complete list of Business Functions assigned to a staff person.)

The Security Reports address these issues by allowing local security coordinators to see information in pre-formatted reports. An agency can only generate reports on its own staff. The data from which the report is drawn is updated weekly. The reports can be sorted, filtered, and exported to Excel, which will look different from the report as it appears in Cognos. They can also be saved in PDF format, where it appears the way it appears in Cognos.

An Office of the State Comptroller audit recommended that CONNECTIONS "provide local district Security Coordinators with reports that can be used to monitor CONNECTIONS security locally and/or amend the CONNECTIONS application to allow the local Security Coordinators to generate such reports." These reports fulfill that recommendation.

Please note that all sample reports use fictitious data and the fictitious Mohawk County.

Instructions on how to access the reports using Cognos will follow an overview of the four reports.

To access Cognos and the Data Warehouse, a staff person needs a Cognos password. To obtain a Cognos password, have your supervisor send an email to Joe Delucia through Outlook or Exchange. This password is different than your NT password and will enable you to access all the information in the Data Warehouse regarding your agency. Each agency should have a designated specialist who can generate reports from the Data Warehouse. Page 7 of this document details how to request a report from your designated specialist, or from your CONNECTIONS Regional Office liaison if your agency does not have a designated specialist. These reports can be generated at any time through the Data Warehouse.

Staff Security Report

As a security coordinator performs security maintenance duties, it is important to be able to track which agency staff is in CONNECTIONS, what business functions each staff member has, which staff is a Unit Approver, and whether a staff person is an Assignee or Designee.

The Cognos Staff Security Report available through the Data Warehouse addresses these issues by allowing local security coordinators to see this information in one pre-formatted report as seen below.

The Staff Security Report includes the following information:

Staff Name:	Worker's name as it appears in CONNECTIONS.
NT Logon:	Worker's logon ID assigned through WEBSTAR.
Unit Approver:	Yes or No – Is the worker a Unit Approver for any unit?
Staff Role:	The worker's role in the unit – Worker, Supervisor, Maintainer, Manager.
Business Functions:	All business functions assigned to the worker.
Assignee or Designee:	Yes or No – Is the worker an assignee or designee for anyone else?

The report also includes the agency name and code, the site code, the unit code, and the date of the report. When requesting the report, the Agency code will be required. The report is sorted by site, then by unit, and then alphabetically by worker's last name.

Please note: The report will only display In-Assignments. Since the worker's BFP is the same regardless of In- or Out-Assignments, it would be redundant to list both on this report.

Business Function Report

As a security coordinator performs security maintenance duties, it is important to be able to track which agency staff has a particular business function. Such a listing would enable the security coordinator to more easily determine the appropriate mix of business functions for a particular unit and to be sure that all workers' BFPs accurately reflect their responsibilities.

In order to obtain this information within the CONNECTIONS application, a local security coordinator has to review the *Maintain Staff* window for each worker, one at a time, to see if that worker has the particular business function. The local security coordinator would also have to check assignees and designees to determine if any worker has given another worker the rights to that business function.

The Cognos Business Function Report available through the Data Warehouse addresses these issues by allowing local security coordinators to see this information in one pre-formatted report as shown below. This report, together with the Assignee/Designee Report, provides information on all workers who have a particular business function, either as part of their own BFP or as a designee of someone who has it. A sample report is shown below.

The Business Function Report includes the following information:

Agency:	Name of Agency
Agency Code:	The Agency's Code
Business Function:	The business function in question
Staff Name:	Workers' names as they appear in CONNECTIONS.
Unit:	The unit code to which the worker is In assigned.
Assignee of:	The name of the worker's designees
Designee's Unit:	The unit code for the worker's designees.

The report also includes the office type, the site code, and the date of the report. When requesting the report, the Agency code will be required. Office Type will automatically be filled in for the agency. The requester can then specify from the list of business functions available for that Office Type which business functions are to be reported on. The report is sorted by site, then by unit, and then alphabetically by worker's last name.

Assignee/Designee Report

For reasons mentioned for the previous two reports, it is important for a security coordinator to be able to track which agency workers are assignees or designees of another worker. Such a listing would enable the security coordinator to more easily determine which staff has the ability to perform which business functions.
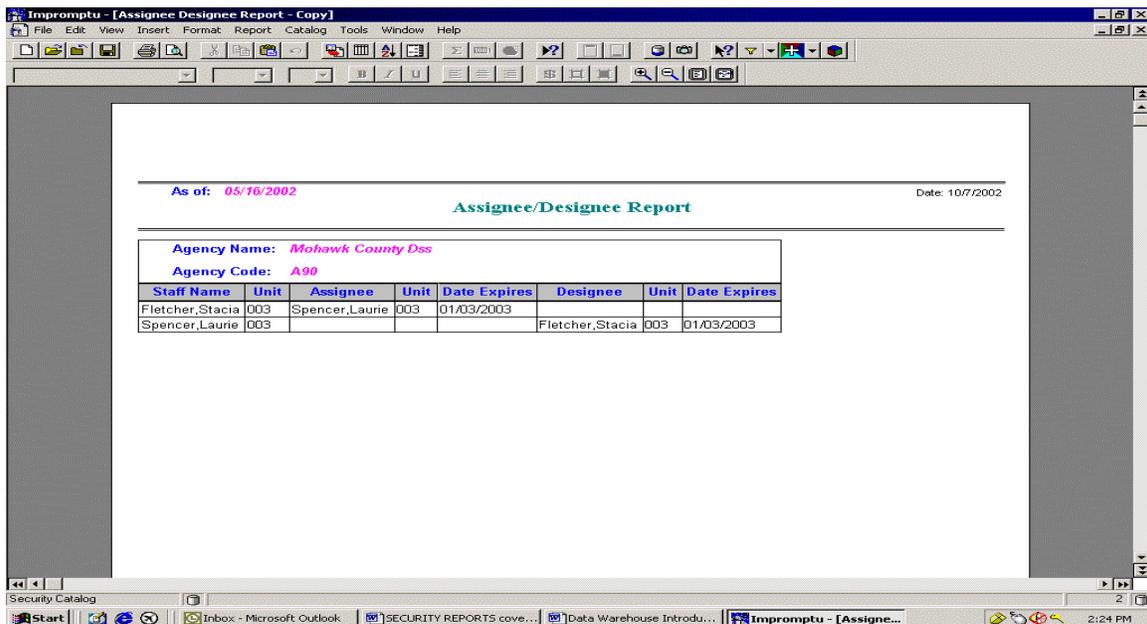
There is no automated way for a security coordinator to obtain this information within the CONNECTIONS application. A local security coordinator has to review the *Maintain Designee* or *Staff Security* window for each worker, one at a time, to see if that worker is any other staff's designee or assignee.

The Cognos Assignee/Designee Report available through the Data Warehouse addresses these issues by allowing local security coordinators to see this information in one pre-formatted report. This report, together with the Business Function Report, provides information on all workers who have a particular business function, either as part of their own BFP or as a designee of someone who has it. A sample report is shown below.

The Assignee/Designee Report includes the following information:

Staff Name:	Workers' names as they appear in CONNECTIONS.
Unit:	The unit code to which the worker is In assigned.
Assignee of:	The names of the worker's designees.
Unit:	The unit code of the worker's designees.
Date Expires:	The date that each assignment expires.
Designee for:	The names of the worker's assignees.
Unit:	The unit code of the worker's assignees.
Date Expires:	The date that each designee's assignment expires.

The report also includes the agency name, agency code, and the date of the report. When requesting the report, the agency code will be required. The report is sorted by site and then alphabetically by worker's last name.

Unit Approver Report

There are instances in which it is very helpful for a security coordinator to be able to easily see who is the Unit Approver for any unit in his or her agency. A Unit Approver cannot be end-dated in CONNECTIONS until he or she is replaced as a Unit Approver. This report also allows the security coordinator to determine all units for which a worker is the Unit Approver.

There is no automated way for a security coordinator to obtain this information within the CONNECTIONS application. A local security coordinator has to review every unit individually, using the *Maintain Unit* window for each unit, to determine the approver for that unit. There is no way for the security coordinator to see this information for all units at one time. The Cognos Unit Approver Report available through the Data Warehouse addresses these issues by allowing local security coordinators to see this information in one pre-formatted report as shown below.

Please note: The Unit approver Report includes both the In and Out Unit Approver assignments for each Unit Approver.

The Unit Approver Report includes the following information:

Staff Name:	Workers' names as they appear in CONNECTIONS.
Approver of Unit:	The unit codes of units for which the worker is the Unit Approver.
In/Out Assigned:	The type of assignment to the unit (In/Out).

The report also includes the agency name, the agency code, and the date of the report. When requesting the report, the Agency code will be required.

The report is sorted alphabetically by the worker's last name.

Requesting Security Reports

Reports are generated from the CONNECTIONS Data Warehouse using an application called Cognos. Each agency should have at least one designated specialist – a staff member trained in the use of Cognos to generate reports form the Data Warehouse. Check with your supervisor to determine the specialist for your agency. Depending on which security report you are requesting, you will be asked for certain information.

Report	Required Information
Staff Security	Agency code
Business Function	Agency code
	Business functions to be reported on
Assignee Designee	Agency code
Unit Approver	Agency code

If your agency does not have a Cognos specialist, please contact your CONNECTIONS Regional Office liaison to request an initial set of the four reports. For future reports to be generated as needed, each agency should have at least one person who can access Cognos. Instructions on requesting a Cognos password are on page 2.

Queries can be run against the data in the reports, to, for example, just get information for one unit or site. Pages 8 – 15 of this document contain detailed instructions for a Cognos user to get into the application and run the reports.

OCFS Data Warehouse Security Report Instructions

The four pre-formatted reports described in the Security Report overview are available through Cognos. There are several steps that have to be taken in order to access these reports and save them.

- ❑ The first step is to get a Cognos password, which can be obtained by having your supervisor send an email to Joe Delucia through Outlook or Exchange. This will be a different password than your NT password and will be used only to access the Data Warehouse.
- ❑ The T: drive must be mapped.
- ❑ A Data Warehouse folder must be created to specify where reports should be saved.

I. Map Your T: Drive

When using CITRIX, you will not be able to save reports directly to your desktop (C: drive). A **T:** drive path will be provided to allow you to save reports while in CITRIX. The T: drive is accessible to you both in CITRIX and from your desktop. In order to access this drive, you must first map your local desktop to this 'T:' drive location. You will need the pathname to your location on the T: drive to accomplish the mapping, which you receive when you receive your Cognos password. Although you can accomplish the mapping in a variety of ways, we will give you, what we believe, is the easiest way. Once you have completed these steps, the path will be mapped and you will not have to repeat them.

<u>Steps to Map your T: drive:</u>

- From your desktop, double click on My Computer.
- From the Menu, click on Tools.
- From Tools dropdown list, select Map Network Drive. Make following choices:
    - o Drive: = T:
    - o Folder = pathname (provided at the same time as your Cognos password).
    - o Reconnect at logon is checked.
    - o Click FINISH.

After mapping your drive, you should then create a folder on your T: drive to hold reports you will be saving while in the Data Warehouse. These reports are created in PowerPlay and Impromptu.

<u>Steps to Create a new folder:</u>

- While in the newly created T: drive, select File from menu.
- From File dropdown list, select New then Folder.
- While the cursor is on the new folder, right click for dropdown menu.
- Select Rename and rename your folder 'OCFS Datawarehouse'.
- Hit the Enter key when name change is completed.
- Close out of T: drive windows by clicking on 'X' in upper right hand corner.

You can save an Impromptu.imr report to your T drive so that it can be re-run at a later date. Reports should be saved to the user's T: drive in .PDF (Adobe Acrobat) or .XLS (Excel) format so that they can be printed and shared by any user, independent of their access to the Cognos software. Please refer to printing instructions later in this document on how to print these reports whether in CITRIX or on local desktop.

II. Start the Impromptu Application

The Data Warehouse is accessed through the CITRIX environment. Follow these steps to connect:

1. Double click the **Internet Explorer** icon on your desktop.

2. Click the **Favorites** button on the Internet Explorer menu bar.

3. Select "**Data Warehouse Login**" from the drop down-list and continue to step 10.

4. If "Data Warehouse Login" is not listed on the Favorites list, continue with step 5.

5. In the Address line at the top of the Internet Explorer screen, type http://OCFSDATAWAREHOUSE.

6. Click the **Go** button to the right of the Address box and wait for the page to load.

7. With the **Favorites** list in view, click on **Add to favorites** button to include the Data Warehouse site to the list.
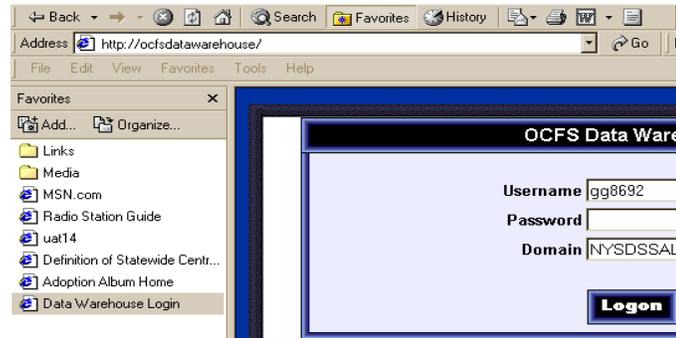

8. In the Add Favorites dialog box, type "**Data Warehouse Login**" in the Name field.
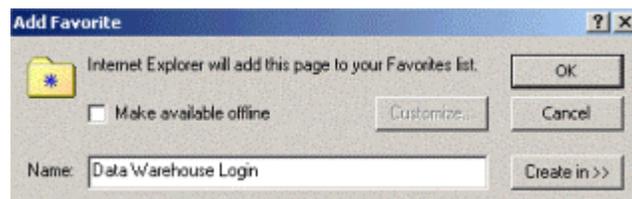
9. Click **OK** on the Add Favorites dialog box.

10. Enter your **NT User ID**, **NT Password**, and **NT Domain** in the OCFS Data Warehouse Login dialog box.

11. Click the **Logon** button at the bottom of the dialog box.

12. Read the Confidential Warning and then click **OK.**

13. The OCFS Data Warehouse welcome screen is displayed. On the left of the screen are icons for T: Drive, PowerPlay, Impromptu, Data Warehouse, and Training Database. Double click the **Cognos Impromptu** icon to launch the application.
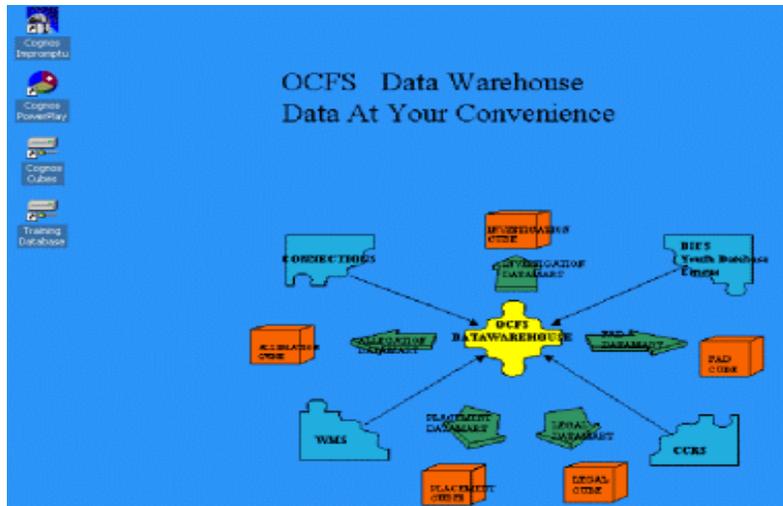
III. Open the Predefined Report

While in the Cognos application, you can open a predefined report. Follow these steps:

1. Click **File → Open** from the menu bar **OR** click the **Open** button on the toolbar.
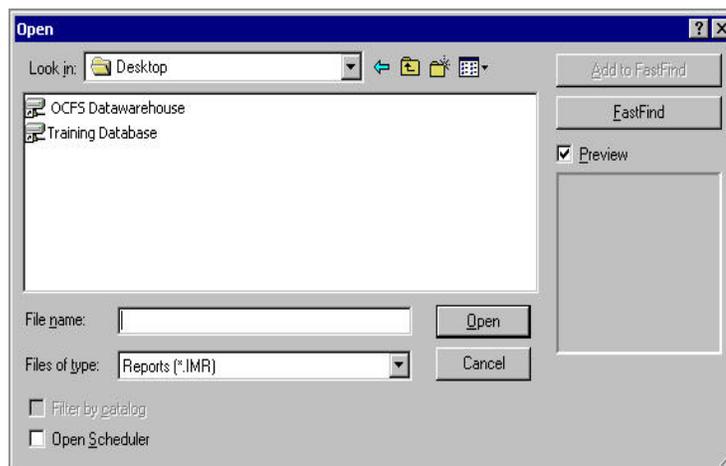
2. Navigate to the **Security - Impromptu** folder as follows, double clicking at each level to move to the next:
- **OCFS Data Warehouse**
  - **Data Warehouse**
    - **Pre-defined User Reports**
      - **Security - Impromptu**

3. Open the Security Reports folder by double clicking on it. (Please note that details about the four reports and fictional Mohawk samples are in the Overview section of this document).

4. Select a report from the listing and double click on it to open it.

> A message screen will pop up notifying you that this report is read-only and that a copy will be made. This is a security measure to prevent users from changing the user reports. Click **OK**.


5. The **Cognos Common Logon** box appears. Enter your **NT User ID** and C**ognos Password** in the boxes provided. Please keep in mind that this password is different from the NT user password. Click the Log On button.

IV. How To Save A Report

After you have run an Impromptu.imr report, you will have the option of printing, saving or closing the report. The following steps will take you through the save process.

Steps to Saving a report:

- While in the Report, click on File from the Menu.
- From the File Menu, click on Save As. This will open a Save As window.
- Click on the dropdown box labeled "Save in:" to select "My Home Drive (T:). Double click on the T: drive to open.
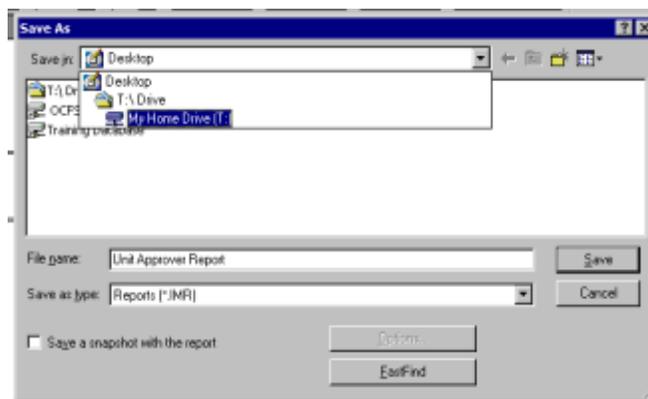
- The Save In: dropdown allows you to choose the folder you wish to save your document in. Select OCFS Datawarehouse for all Cognos reports.
- Enter a File name for your report.
- Click on the dropdown list for 'Save as type' and, if you intend to print this document at a later time, select either of the following types:
    - Adobe Acrobat (.pdf) or
    - Excel (.xls)

- Both of the above document types are conducive to printing the report at a later time.
- If you intend to rerun the report at a later date (eg. weekly reports or monthly reports) you should save it in:
    - Impromptu Query (.imr) format (within Impromptu) or
    - PowerPlay (.ppr) format (within PowerPlay).
- Once all required areas are completed, click the Save button.
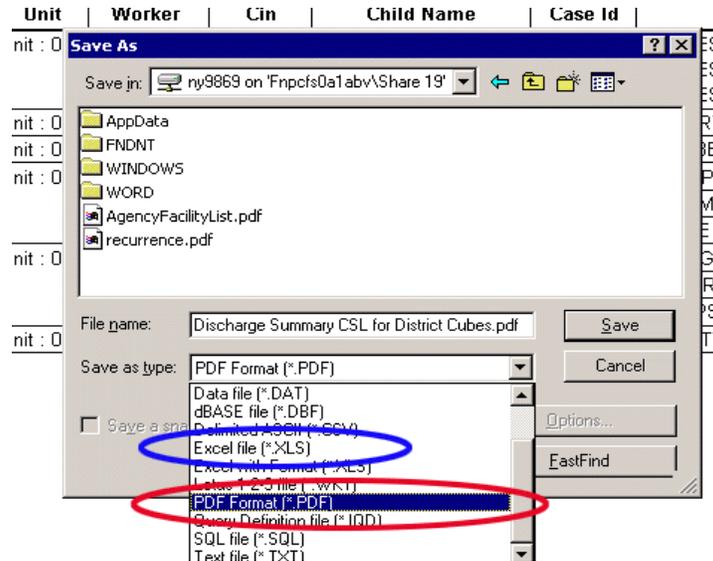
- After you have created all necessary reports and have saved them you can now exit from CITRIX.
- You must close out the current catalog before closing out of the Data Warehouse. On the Menu, select Catalog; then Close. This will close the report.
- To return to the CITRIX desktop, click on **File → Exit** .
- To close out of the application, click on the **Start** menu and choose **Log Off (user name).**

** YOU SHOULD NEVER CLOSE OUT THE WINDOW BY CLICKING ON THE "X" LOCATED AT THE UPPER RIGHT HAND CORNER OF THE WINDOW AS THIS MAY RESULT IN LOSS OF ALL REPORTING THAT WAS DONE DURING THAT SESSION.

V. Open and Print a Saved Report From the T Drive

You may print from an opened report by selecting **File** ➔ **Print** from the Menu bar. This process is a standard Word function. Keep in mind that these reports are lengthy so you should pay particular attention to the number of pages you wish to print.

However, if you have saved a report to your T: drive, you can print the report both in CITRIX and from your local desktop. Once the reports are opened from the respective environments, printing is the same. Therefore, follow the directions on how to open the saved reports from either CITRIX or the desktop and then follow the printing instructions.

**<u>To open a saved report from within the CITRIX environment:</u>**

- From CITRIX desktop, double click on the T: drive icon.

**<u>To open a saved report from your regular desktop:</u>**

- From regular desktop, open **MY COMPUTER** by double clicking on it. This will open all available **DRIVES**.
- Double click on the **T:** drive.

<u>To print:</u>

- Double click on the **OCFS Datawarehouse** folder. Then double click on the report that you want to open.
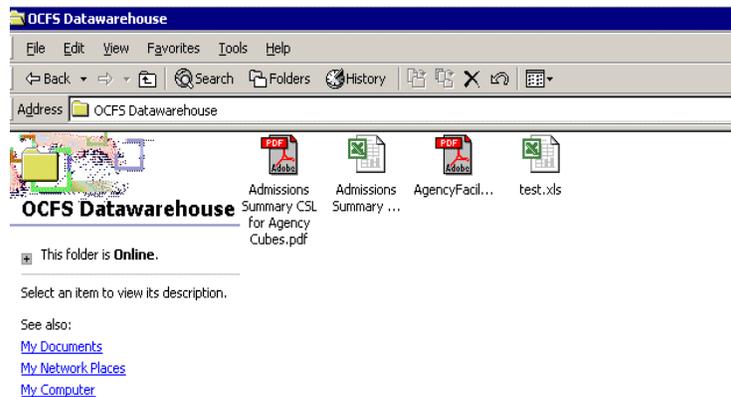
- The report may take a few minutes to open depending on the **SIZE** of the **FILE.** On the bottom of the .**PDF** file is the **Number of Pages** for that report. If you print the entire report, this is the number of pages that will be printed. Please note that a large report may tie up the printer.
- To help alleviate this problem, you can print only selected pages. From the Menu bar, click on **File** ➔ **Print**.
- The next screen will ask you the pages to be printed starting at page number ? and ending at page number ?. You need to put in the page numbers that you want to print and you can change the printer that you want to print to. Otherwise, it will go to your default printer. When complete, click **OK** to print.
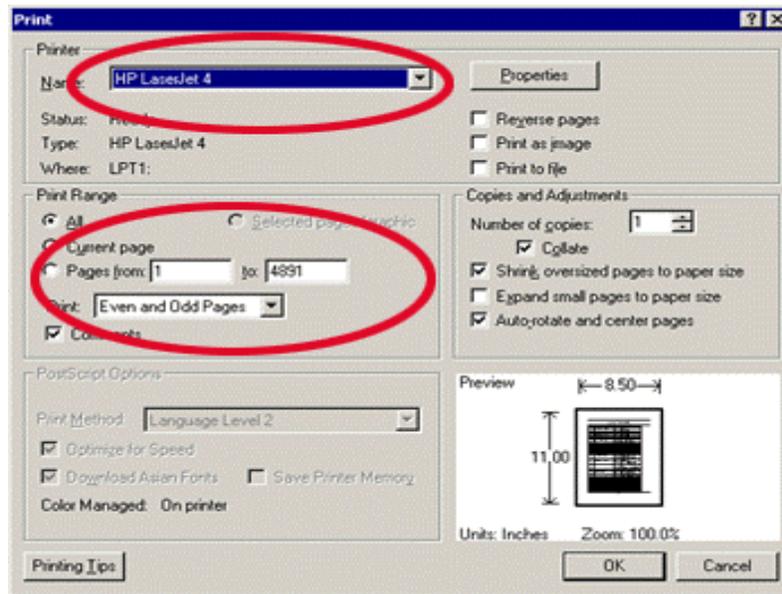
- You can preview the pages before deciding which ones to print by clicking on the Arrows located at the bottom left hand side of the window.
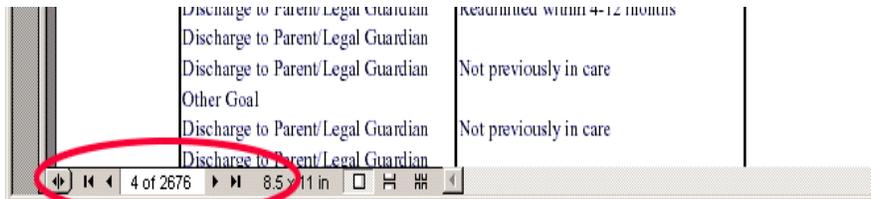
- The same procedure, in terms of choosing specific pages to print, is also followed when printing an Excel document.
- This will open the same print window as when printing a document with Adobe Acrobat. When the Printer and Print Range have been selected, click on **OK** to print.
- Close report by clicking on **File → Exit.**

VI. To Copy and Paste Reports to the Local Machine

In order to copy reports from the T: drive to your C: drive, you must first provide a location on the C: drive for these reports. Create a new folder on the C: drive and name it **OCFS Datawarehouse Reports.** If you are uncertain how to do this, refer to Section I of this document on how to create a folder.
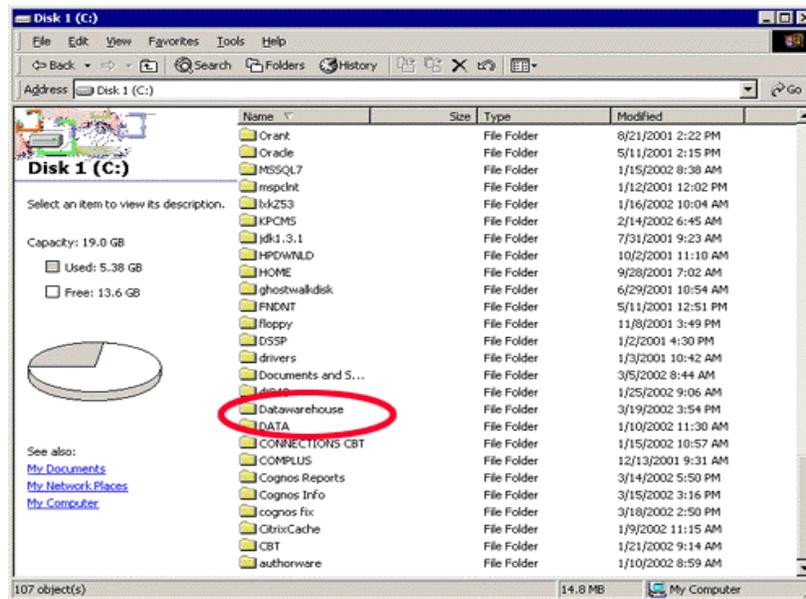
You will then need to access the T: drive to get the report(s) you will be copying **FROM**. Open the OCFS Datawarehouse Folder to display the reports.

Highlight the report that you want to copy and click on the Edit Menu bar and then choose Copy.

Once COPY has been selected, access your C: Drive and open the OCFS Datawarehouse Reports folder. Place your cursor anywhere within the blank space of this folder and then select the Edit Menu bar and choose Paste.

When the copying is complete, double click on the document to open. You will then be able to print using your normal print functions.

COGNOS Training:

Training is available for Cognos users that includes more advanced used of the Data Warehouse data including how to create ad hoc reports Security reports using the security data in the Data Warehouse. Contact Joe Delucia via email through Outlook or Exchange.