



Chapter 9

Hyperion Enterprise

Processes & Responsibilities

A. System Configuration and Administration

1. System Configuration

The departmental system for preparing financial statements is the Consolidated Financial Statement (CFS) System. This system includes the following components: Hyperion Enterprise, Citrix, the XA Server, and the Financial Statement Trail Head. We use a more sophisticated and robust environment to provide user access to the Hyperion Enterprise suite of programs, Hyperion Enterprise databases, and project files via the Citrix Metaframe XP thin-client operating environment. This section of the document describes the CFS System, the purpose of each component, and how users connect to the environment.

The CFS System consists of seven servers and they are:

- Citrix Server 1 (Primary communications server)
- Citrix Server 2 (Load balancing communications server)
- Citrix Server 3 (Load balancing communications server)
- Nfuse Web Server 1 (Provides the single point of log on from the Internet)
- Nfuse Web Server 2 (Provides fail over backup for Nfuse Web Server 1)
- HYPNT Server (Database server)
- XA Server (File server)

The Figure 9.1 depicts the current operating environment logical layout. Each of the servers listed above has a different role in the processing environment. The role of Citrix Server 1 is to allow users to connect to the Hyperion Enterprise programs (Enterprise, Reporting, Retrieve, etc.) and project files from a remote location. This has two advantages: one is that it is an easier and more efficient way to provide new users with access to the programs, and the second advantage is that the Hyperion software response time is improved because of the thin-client technology. Citrix Server 2 and Citrix Server 3 act as load balancers with the primary communications server, Citrix Server 1. Users will still log on to the primary Citrix server, but as the load on the primary server increases, processing will shift to the load balancers. In the event that the primary Citrix server becomes unavailable, the load balancers will assume the role as the primary.

The Nfuse Web Server 1 is the first point of contact for all CFS System users. This web server sits in the NBC “demilitarization zone” (DMZ) which is surrounded by firewalls. Once users authenticate to the NBC domain, they are



presented the list of published applications. The Nfuse Web Server 2, also in the DMZ, acts as a fail over server for the Nfuse Web Server 1. If the main web server were to become unavailable, the backup web server would assume the load.

The HYPNT server's primary role is to store the Hyperion Enterprise applications. These applications consist of each bureau financial statement application, the departmental consolidated financial statement application, and any other application, as developed. All users run the Hyperion programs from the Citrix servers and the Citrix servers communicate directly with the HYPNT server to update and query the Enterprise applications.

The XA server's primary role is to act as a file server and store all project files. The XA server's role has not changed much from the previous years.

2. *Process for Gaining Access to the System*

When a new user needs access to the Citrix Server and a Hyperion Enterprise application, the following procedures apply:

A. The new user request will come in to Manisha Tuli and Mike Sciortino (The NBC Hyperion administrators) via the online web form available from the DOI Financial Statement Trail Hear (financial.nbc.gov). The form is only available to authorized Hyperion contacts within each bureau/office (see the current list below). On occasion, we will accommodate phone requests if the circumstances are warranted. The request must provide the following information:

- Employee name
- Employee's phone number
- Employee's email address
- Bureau/Organization
- Position type
- Approving official
- User type (the level of access)

B. To control the process, the NBC will only consider new user requests from the authorized people below. The current list is as follows:

- | | |
|---------------|-------------------------------|
| • PFM | Debra Carey or Donna McKethan |
| • BIA | Rusty Hargrave |
| • BLM | Brad Walbruck |
| • BOR | Doug Denardo |
| • FWS | Edna Romero |
| • MMS Herndon | Teresa Weaver |



- MMS Denver Linda McKinney
- NPS Cindy Robinson or Gary DeBusk
- OS Julie Ehrlichman
- OSM Greg Muehl
- USGS Maurice Roberts
- OIG Steven Jones
- KPMG Julie Lau

- C. Once the request is validated, the NBC Hyperion administrators will forward the approval to the NBC Citrix help desk requesting a new user be set up on the NBC domain. The NBC administrators will forward the new user information to the help desk.
- D. The NBC Hyperion administrator will also copy all other Hyperion administrators on the message to ensure against duplication of effort.
- E. The NBC Citrix help desk will add the user to the domain using the first initial/last name format. The help desk will set up the user access with the default password (#1NBCdoi) and ensure that the user will be required to change their password at first logon. The help desk will then respond back to the Hyperion administrators notifying that the user has access to Citrix.
- F. The help desk will contact the user and walk them through the process of installing the Citrix client software, logging on for the first time, and changing their password. The help desk will notify the Hyperion administrators when this process is completed.
- G. Once confirmation is received from the help desk that the new user has been added to the NBC domain, the Hyperion administrators will add the new user to the appropriate Hyperion Enterprise application, if the user needs Enterprise access. Note: depending on the new bureau user's role on the project we may or may not add them to Enterprise. If a user only needs access to the XA server, then an ID in Enterprise will not be required. When a user does need access to the Enterprise application different circumstances exist depending on the user's organization. Table 9-1 summarizes this treatment.



Organization	Treatment
Bureau User	Receive Citrix access and named access to the bureau Enterprise application.
PFM/NBC Reston User	Receive Citrix access and named access to all applications.
OIG/KPMG User	Receive Citrix access and readonly access to all Enterprise applications.

Table 9.1 - New User Access Treatment

- H. Once the user ID and password are set up in the Hyperion Enterprise application, the Hyperion administrator will contact the user and provide the Hyperion user ID and password. If needed, the administrator will also provide assistance on accessing Enterprise.
- I. After the user has been given access, the Hyperion administrator will add the new user to the Citrix User Access Database stored on the XA server. This database is used to track the access list and provide the mean to audit the list on a periodic basis.
- J. In addition to the Citrix User Access Database, the Hyperion administrator will add the new user to the Lotus Notes contact list and capture the user's name, phone number, email address, and organization. This contact list is also the basis for the Hyperion User email list for use in communicating with system users.
- K. The last step in the process is to add the user's Lotus Notes name to the Hyperion User email list in Notes.

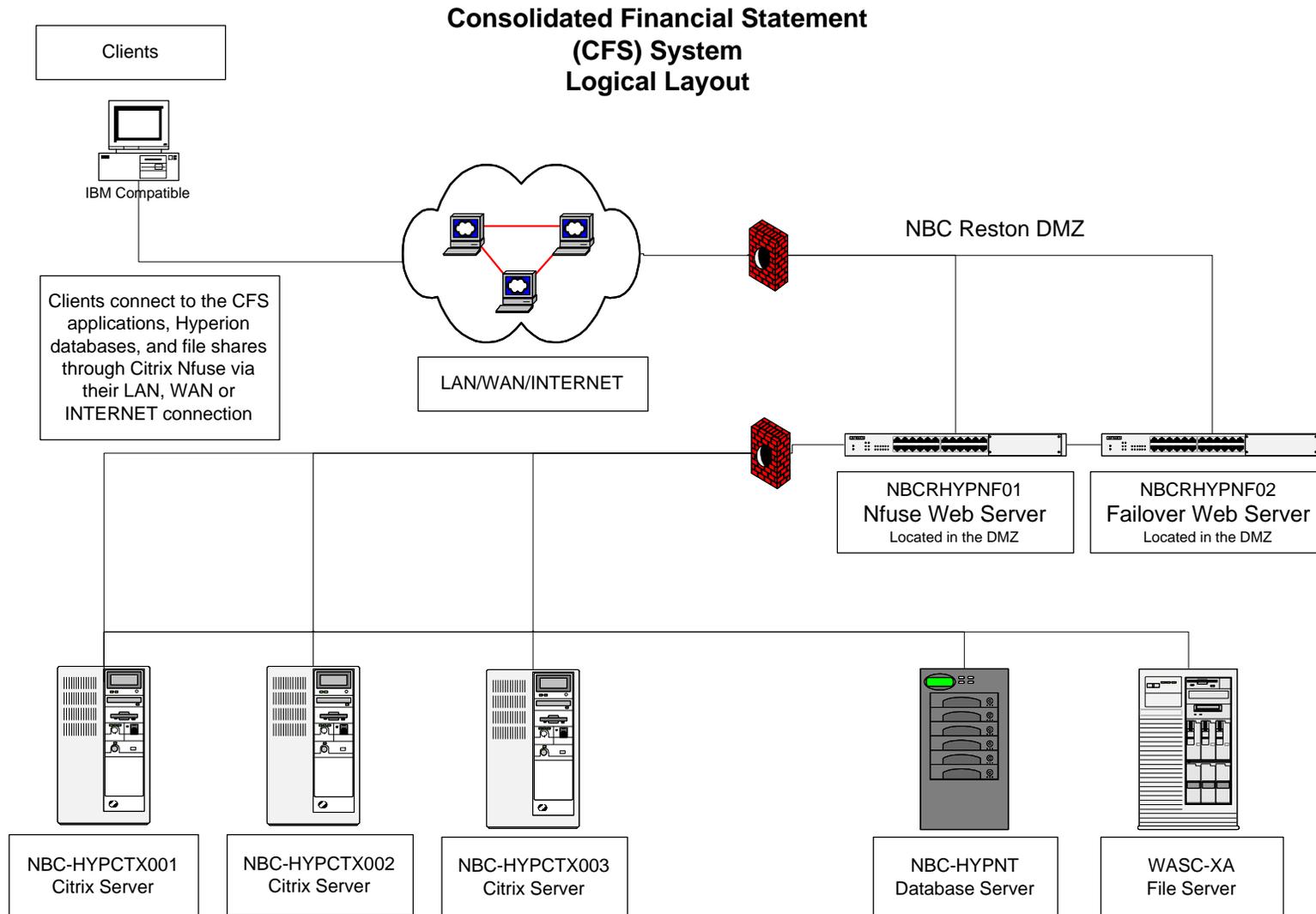


Figure 9.1 - CFS System Logical Layout



B. Logging onto the Citrix Server

1. *The Citrix Nfuse Log In Web Page*

The single point of entry for all financial statement applications and project files is the Citrix Nfuse log-in web page (Figure 9.2). The address for this page is <http://financial.nbc.gov>. This page provides secure access to the CFS System and available financial statement applications and files on the XA server.

To access the CFS System, users launch their Internet browser (Internet Explorer is the preferred browser). In the address bar, users enter <http://financial.nbc.gov> and are brought to the log-in page. Note: if users access the Citrix Nfuse web site routinely, they can add the page to their list of favorites. To start the logon process, users enter their Citrix credentials and click on the “Log In” button.

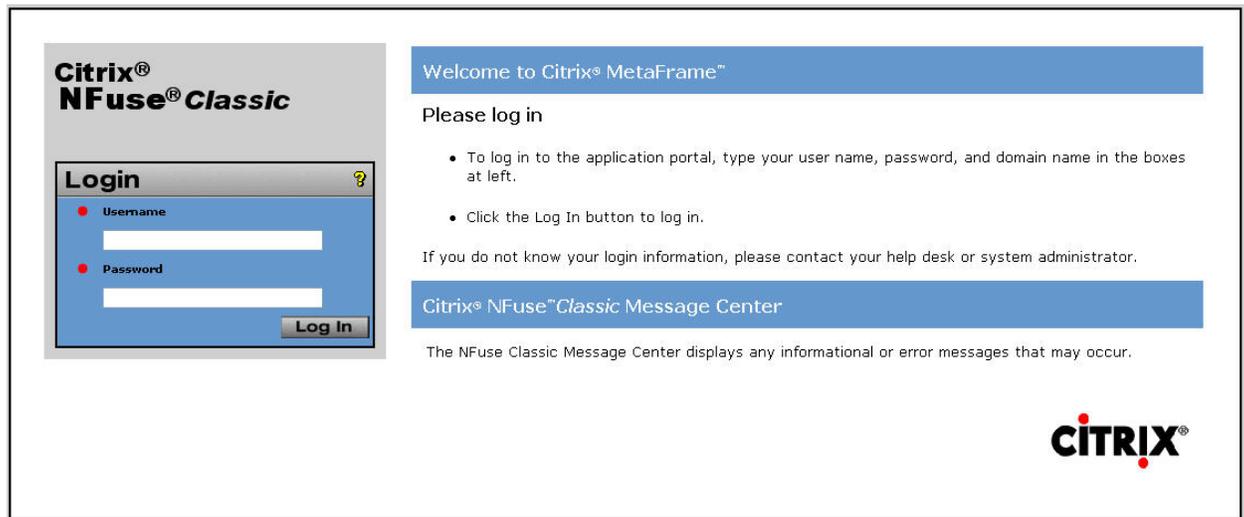


Figure 9.2 - The Citrix Nfuse Log-In Web Page

2. *The Citrix Application Portal*

After users successfully enter their Citrix credentials and are authenticated on the NBC domain, they are presented with a menu of applications available based on their user profile. This list is presented via the Citrix Application Portal (Figure 9.3). The paragraphs that follow highlight the steps for accessing each of the major applications available from the Citrix Application Portal. Also from this portal are two links: 1) the Financial Statement Trail Head Web Site, and 2) the Citrix Help Desk Web Site.

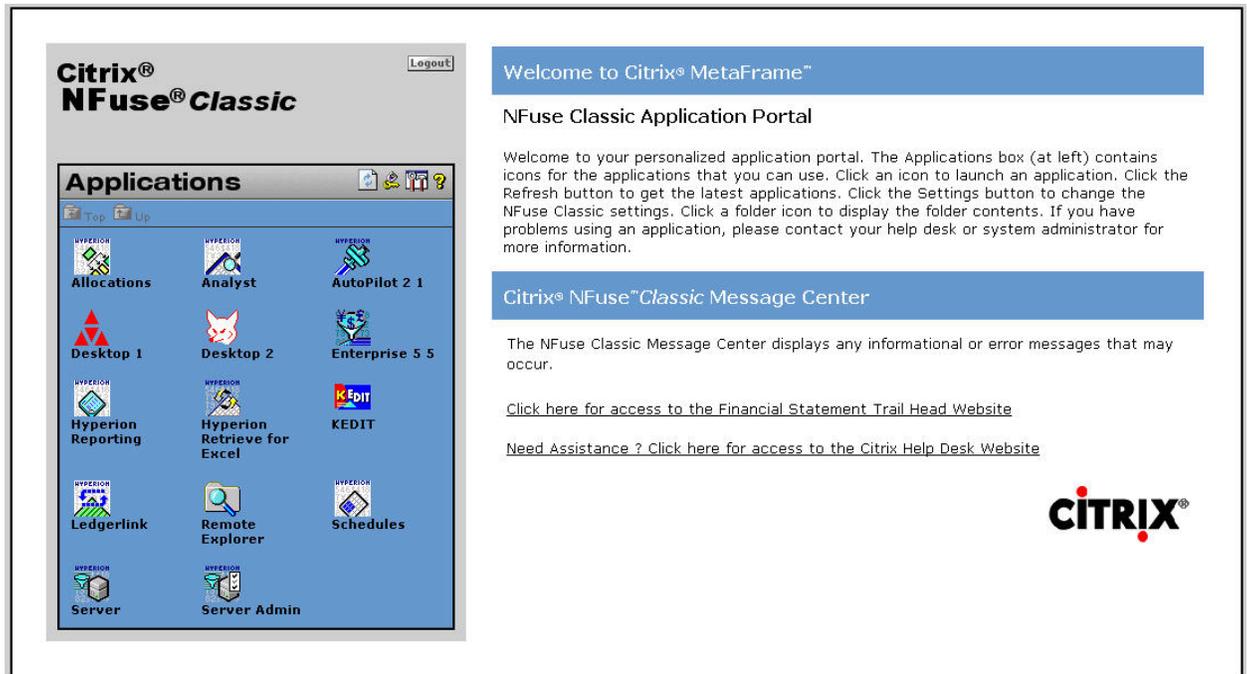


Figure 9.3 - The Citrix Application Portal

The Financial Statement Trail Head (Figure 9.4) is where we store useful information related to the system, DOI's financial statement preparation project, and links to other relevant Internet resources. Since the trail head is behind the Citrix log in, it is only accessible to users with rights to access the system—this site is not accessible to the public. The types of information available on the trail head include guidance documents, links to training material, support for the use of Hyperion software, project contact information, and links to other useful websites. The NBC Reston office maintains the trail head.

The other link is to the Citrix Help Desk Web Site where users can find information and resources related to the Citrix technology.



Figure 9.4 - The Financial Statement Trail Head

3. ***Opening Hyperion Enterprise***

To open Hyperion Enterprise, users click once on the Hyperion Enterprise 5.5 icon. The system will begin to connect and users will receive the standard DOI notification message. The system will then prompt users for their Hyperion Enterprise application, user ID, and password. Note: the Hyperion Enterprise user ID and password are separate and distinct from the Citrix credentials even though they may be synchronized. From the drop down box users select the application they would like to access. Users then enter their Hyperion Enterprise user ID and password. Note: users must make sure that their “caps lock” key on their keyboard is deselected. Users then click the “Okay” button and are brought to the Hyperion Enterprise desktop (Figure 9.5).

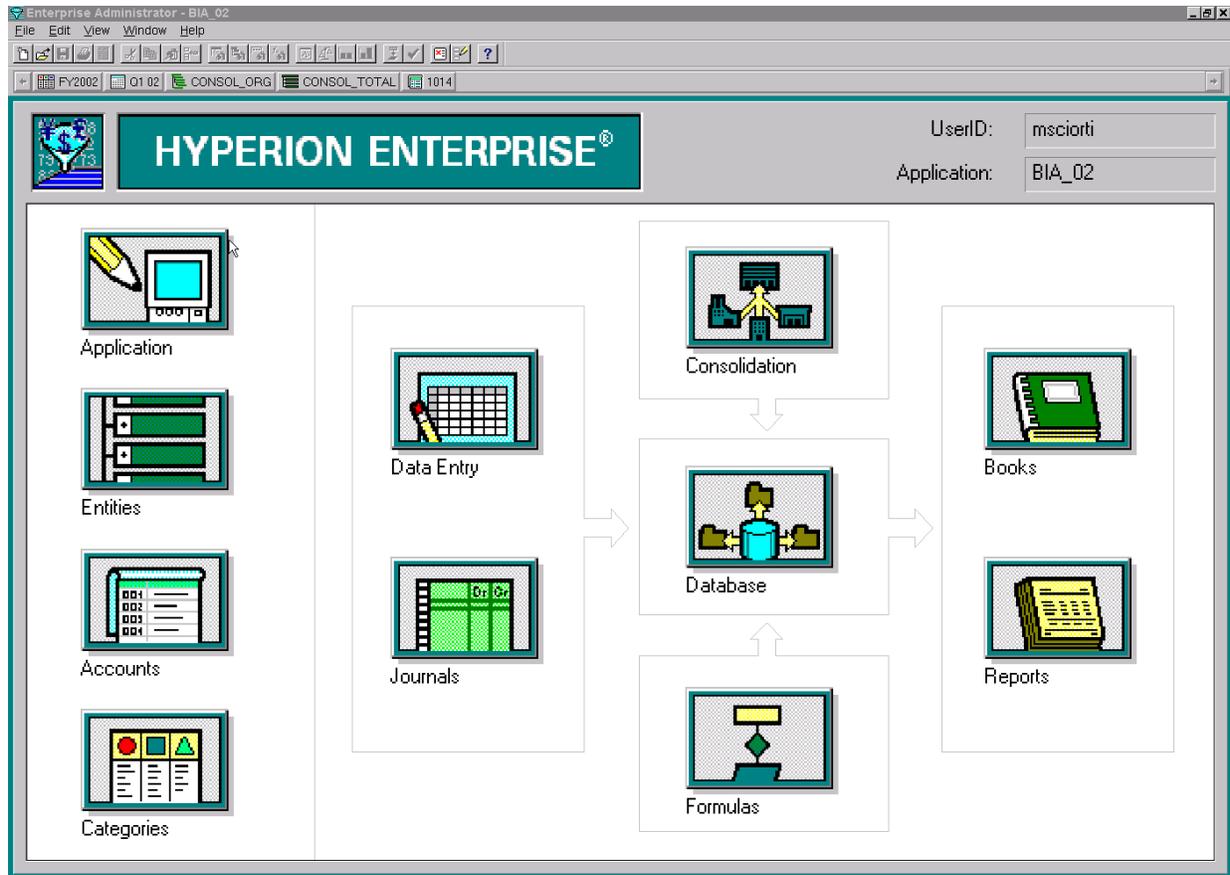


Figure 9.5 - The Hyperion Enterprise Desktop

4. ***Opening Hyperion Reporting***

To open Hyperion Reporting, users click once on the Hyperion Reporting icon. The system will begin to connect and users will receive the standard DOI notification message. Users Click “OK” at this message. Users then enter their Hyperion Enterprise user ID and password and click the Connect button and select the application they wish to access. Users are then brought into the Hyperion Reporting module.

5. ***Opening Hyperion Retrieve for Excel***

To access Hyperion Retrieve, users click once on the Hyperion Retrieve icon. The system will begin to connect and users receive the standard DOI notification message. Users click “OK” at this message. Excel will launch and prompt the users for their Hyperion Enterprise user ID and password. **THIS IS IMPORTANT:** Users must leave the user ID and password blank and click ‘OK’ for each application that pops up. User access to all applications provides the ability to pull data from each application using Excel. This user access is read only and no data



can be changed in the individual applications. Users must remember that this version of Excel is running on the Citrix server and its purpose is to run Hyperion Retrieve only. This is not a local workstation copy of Excel.

6. ***Opening K-Edit***

K-Edit is an extremely useful text editor and it provides an easy-to-use tool for looking at Hyperion Enterprise application extracts, data files, journal entries, and any other text-formatted file. To access K-Edit, users click once on the K-Edit icon. The system will begin to connect and users will receive the standard DOI notification message. Users click “OK” at this message. From within K-Edit users will have the ability to access files on the NT server, the XA server, and files in the user’s personal folder on the CFS System.

7. ***Opening Remote Explorer***

Remote Explorer is the CFS System’s version of Windows Explorer. It provides the ability to access the inbox and outbox directories of the Hyperion Enterprise applications, access XA server files, provide access to the user’s personal file space, and provide a link to the user’s local workstation for copying files. To access the Remote Explorer, users click once on the Remote Explorer icon. The system will begin to connect users will receive the standard DOI notification message. Users click “OK” at this message. Users will then be brought to the default directory, which is the XA server. Users can access the Hyperion Enterprise application directories by drilling into the “Finstate01” folder or other directories as needed.

C. Financial Statement Applications

1. ***Overview of the Hyperion Enterprise Modules***

After logging in to Hyperion Enterprise, the Enterprise desktop appears (Figure 9.5). The desktop buttons and their major functions are outlined in the Table 9.2 below:



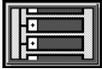
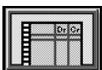
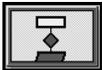
	Application	Edit application's label, description, currency, default translation rate, consolidation methods and percentages, locking accounts and other options.
	Entities	Create, modify, view or print organizations, entities, substructures and subentities, currencies, entity conversion tables and entity lists.
	Accounts	Create, modify, view or print the chart of accounts, subaccount tables, account conversion tables and account lists.
	Categories	Create, modify, view or print categories. DOI has defined categories as fiscal year.
	Data Entry	Create and modify schedules, define schedule preferences, enter and edit data. Print schedules.
	Journals	Enter, load, extract, edit, post, unpost, reverse and print journals.
	Consolidation	Perform consolidations. Consolidations must be performed when modifications are made in the following modules: entities, accounts, categories, data entry, journals, database and formulas.
	Database	View, edit, load, and extract data. Show and calculate formulas.
	Formulas	Create and modify method files. Compile methods and print formula script files.
	Books	Create, modify and compile books using scripts.
	Reports	Manage report sets, print and preview reports. Create, modify and compile reports using scripts.

Table 9.2 - Overview of Hyperion Enterprise Modules

2. *The Point of View Bar*

The importance of the Hyperion Enterprise point of view bar cannot be overstated. The point of view is where users set the parameters for viewing data and other information in Enterprise. Without the correct point of view, users will not see what they expect. The point of view bar is composed of the following elements:



- Category
- Period
- Organization
- Entity
- Account

These data elements define all of the criteria for a specific set of data. The point of view in Figure 9.6 is an example of the point of view bar in a standard DOI application. DOI has defined the data elements as follows:

- Category - Fiscal year
- Period - Quarters (1 through 4)
- Organization - Various views of data defined as needed for reporting
- Entity – Various fund symbols and grouping thereof
- Account = Defined in chart of accounts



Figure 9.6 - Sample Point of View Bar

All Hyperion Enterprise applications contain fiscal year data dating back to FY1998. The data used to produce financial statements for FY2003 will be in the following categories and periods.

<u>Category</u>	<u>Periods</u>	<u>Description</u>
FY2003	1-4	FY 2003 pre-closing balances
BB2003	4	FY 2002 post-closing balances
FY2002	1-4	FY 2002 pre-closing balances

The point of view needs to be set correctly to run reports, extract, review, enter, and consolidate data properly.

3. *Opening Periods in the Journals Module*

In journals module, the quarterly periods must be opened before making journal entries. They must be opened in sequential order. Periods are opened in the journals module using the “Task” menu and selecting “Open Period”.

4. *The “Run Users in Application Report”*

With more users accessing the applications, it has become more important to monitor who is in the application, and what module they are in. For certain



processes, namely consolidations, there must not be any users in any Enterprise module that can affect data. Hyperion Enterprise uses the first-come-first-served basis for rights in the application modules. This means that the first user into a specific module has the control over the module. Any subsequent users can access, but are locked out. This is a safeguard to ensure that users don't conflict with each other while in the same application. When users start consolidations the user should check the "Run Users in Application Report" to determine which users are logged into the application and which module is in use. If any other users are in any of the following modules, the consolidation will stop:

- Entities Module
- Accounts Module
- Database Module
- Journals Module
- Formulas Module

Users in any other module will not affect the consolidation. The report displays user information such as the user description, computer name, module, and task information.

To run the report, follow these steps:

1. Open the applications module.
2. Select "Task".
3. Select "Run Users in Application Report".
4. The "Users in Application Report" dialog box will display. See Figure 9.7 below.

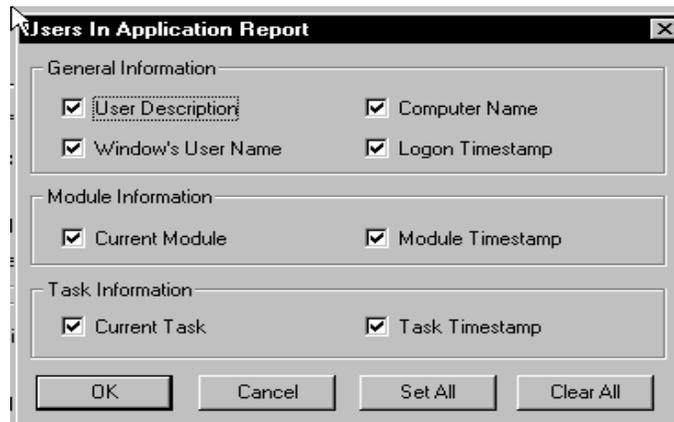


Figure 9.7 - Users in Application Report Dialog Box

5. Select the options that you want to display on the report, then select “Ok”. The report will display.
6. Use the options in the preview window to view or print the report. When using the preview option, the entire page of the report is displayed in several screens. Use the “Next” selection to view all screens.

5. ***The Application Log (a.k.a. the Error Log)***

Each Hyperion Enterprise application has an application log associated with the application. The log can be accessed from the desktop and from each module by selecting the “View” menu and selecting “Error Log”. The title “Error Log” is a bit of a misnomer, because the log serves as more than an error log. It also documents vital information about the application. In addition to providing detail on errors encountered, the error log provides start and completion times for consolidations, data loads, and report generation. Periodically, the Hyperion Administrators clear the log and save the historical record for reference. The Hyperion Administrators are the only users that can clear the log. The following procedure applies if a user wants the error log cleared.

In order to preserve the historical error log record, users are not able to clear the error log. The Hyperion Administrators are the only users authorized to clear the log at this time. If the error log becomes too large and a user would like it cleared, users are directed to the Hyperion administrators. The administrators will copy the current log text into a file, save the text file in the application directory, and clear the log in the error log dialog box. This preserves the application history.



6. *Application Sub-Directories*

On the NT Server there are directories for all of the Hyperion Enterprise applications. Within each of these directories there are individual files and folders specific to the Hyperion Enterprise applications. Bureau personnel have access to their bureau sub-directory only (for example, FWS cannot access BLM's directory, and so on). All auditors have read only access to all directories. Headquarters personnel have full access to all sub-directories.

Each bureau directory has the same sub-directory structure and is as follows:

<u>Sub-Directory</u>	<u>Purpose</u>
Data	Stores the actual Hyperion Enterprise data by category
Inbox	Used as a file folder for files to be loaded into Enterprise applications
Outbox	Used as a file folder for files extracted out of Enterprise applications
Reports	Used as a directory to store all reports run out of Enterprise



7. *Loading and Extracting Information Out of Hyperion Enterprise*

a. Application Information

At anytime users can extract any portion of the Hyperion Enterprise applications for use outside of Enterprise. For example, if a user would like to see the entire list of entities for a particular application, the user can extract this to an external file and use it in Microsoft Excel or K-Edit. Likewise a user could extract information on entity ownership, accounts, account lists, entity lists, etc. To extract application elements, follow these steps:

1. Open the Hyperion Enterprise application.
2. Open the application module.
3. Click on the “Task” menu.
4. Select “Extract Application”.
5. The default is to extract the entire application. If you only want portions, select the tabs and set the flags for those portions you want.
6. Give the extract a file name and click “Ok”.
7. The file will be extracted to the applications outbox.

a. Data

Some of the most critical information in the Hyperion Enterprise application is the data. Hyperion Enterprise stores bureau trial balance data by fiscal year and quarter. Bureau personnel are responsible for loading their quarterly trial balances by the dues dates set forth by PFM. The NBC is responsible for maintaining the data integrity.

To load data to a Hyperion Enterprise application, bureau personnel follow these steps:

1. Open the Hyperion Enterprise application.
2. Open the database module.
3. Click on the “Task” menu.
4. Select “Load Data”.
5. Click on the “Add” button and navigate to the location of the load file (the default is to the application inbox).
6. Select the “Report Calc Account” option.
7. Select “Replace”.
8. Ensure that in the “Default” setting, the appropriate delimiter is set to match the load file delimiter.
9. Click “Load” and the file will be read into Enterprise.
10. A successful load will result in no errors. If errors occur, the user will have to research the error using the application log, make the necessary



corrections, and reload.

On occasion, users may have the need to extract data out of an application for use outside of Hyperion Enterprise (e.g., for use with K-Edit, Microsoft Excel, Microsoft Access, etc.). To extract data from an application, users must follow these steps:

1. Open the appropriate Hyperion Enterprise application.
2. Open the database module.
3. Under the “View” menu select “Entity List”.
4. Select the “ALL_BASE” entity list.
5. Select the column for the data you are trying to extract
6. Under the “Task” menu, select “Extract Data”
7. Assign a name to the extract file
8. Click “Okay”
9. The file will be extracted to the application outbox.

b. Adjusting Journal Entries

Users can extract journals from Hyperion Enterprise to a local drive and view the journal information using a text editor (K-Edit, Notepad, etc.) or Microsoft Excel providing the capability to do further analysis. To extract journal information follow these steps:

1. On the Hyperion Enterprise desktop open the journals module.
2. Make sure the point of view is set to the proper category you wish to extract from (FY2003, BB2003, FY2002, BB2002, etc.)
3. Make sure the proper period is selected in the point of view (Q2 03, etc.)
4. Under the “Task” menu select “Extract Journals” for a single period.
5. In the selection window, select all journal entries by using the shift key and the down arrow (leave all the attribute boxes checked) or just select a single entry.
6. Click “Okay”.
7. In the “Extract Journals – Single Period” window, check the “Extract Posted Journals as Unposted” box.
8. Give the extract file a name and click save.
9. Back at the “Extract Journals – Single Period” window, click “Okay”.
10. The extract will be written to the application outbox with a “jaf” extension.



D. System Security

1. Location Security

All of the project servers (Citrix Servers, NT Server, and XA Server) are located in the west wing of the USGS Data Center in Reston, Virginia. Any additional servers added to this project will likewise be placed in the USGS Data Center.

The USGS property in Reston, Virginia is protected 24 hours a day 7 days a week, 365 days a year by a security staff. Access to any building on the Reston property is only obtained by either a USGS issued ID/security card or by way of guest access, granted by security. Security measures also include sign-in and pass-through of a metal detector for all guests, security monitored and recorded cameras at all entry and exit point of the buildings, and security access swipe cards at all entrances and exits.

The USGS Data Center requires special access cards be issued to cleared personal that have completed a security background investigation and have a legitimate need to have access to the data center. The data center is staffed only during regular USGS business hours. Any person requiring access during off-hours is issued a key code combination for the data center door.

To enter the data center during normal business hours an individual must first gain access to the data center building by way of a security badge swipe card. Once in the building the individual will need to use their card on another swipe card point at the actual server room door.

2. Hardware Security

All of the project servers have unique key locks on the front of each server door. A key is required to access any of the media drives. Also each server's BIOS is set to boot off the primary SCSI hard drive only, allowing the main operating system to boot. Each server's BIOS is locked down with an administrative password.

3. Operating System Security

All project servers run on either Windows Server 2000 or Windows Terminal Server 2000. Each server has been loaded with the most current service pack. As new service packs are released they will be reviewed/tested and then place into service once determined satisfactory.

Second, all servers have had their registries modified to only allow a minimum of six mixed alpha and numeric characters for each user password. Each user must



change their password after a set amount of time. Currently that time length is set for three months.

Also, no previous passwords or deleted user names can be reused. Third, the Windows NT resource kit has been installed on all of the servers. This resource kit contains a feature that audits the system for C2 compliance. Due to the nature of our applications, we are not able to mean all of the criteria to be fully C2 compliant. The following are a list of changes that have been made to increase security on all underlying subsystems of NT.

- Only native Windows applications and DOS subsystem applications can be run. Both POSIX and OS/2 subsystems have been removed from all of the NT servers.
- The security log has been set to not overwrite events.
- The guest user account is disabled.
- Only the administrator may assign drive letters.
- The last user name entered to login will not be displayed.
- The shut down button is no longer displayed to any users except the administrator.
- The registry is locked down with only system and administrative rights able to modify.
- Users are only given read rights to main operating system files.
- File level security is enforced on all drives.
- Each of the ICA clients has 128-bit encryption enforced for log on and 40-bit encryption for communication between the client and the server. If someone were able to crack the 40-bit encryption, the only data they would see would be screen shots from the client. No system data is actually passed to the client in a screen shot.

4. *Hyperion Enterprise Application Security*

In addition to the NT security and credentials required to access the Citrix server, we have an additional level of security established within the individual Hyperion Enterprise applications (the security structure is maintained by the Hyperion Enterprise systems administrators). This security level is mainly forced through the use of security classes. The purpose of this level of security is to limit user access to only specific areas in the Enterprise applications that are deemed necessary by the system owner (PFM). With this security in place we can control access to the database in all respects.

The Hyperion Enterprise security allows the project managers to control access to Hyperion Enterprise tasks and application elements for all department and bureau applications. We use security to protect data and to prevent unauthorized users from viewing, accessing, or changing critical data. In our applications, we apply



security to specific tasks or application elements. For example, we restrict access to tasks such as posting journals, or to specific application elements such as entities, reports, and accounts. Each security class, user group, and user that we establish must also be secured by assigning the element to a security class. Securable items can be arranged into security classes by function, department, entity, or some other criteria. Users can also be classified into user groups by similar criteria. Once we set up security classes, users, and user groups, we assigned access rights to these security classes for individual users and user groups.

5. *The Elements of Hyperion Enterprise Security*

Hyperion Enterprise security elements consist of users, user groups, security classes, and access rights. Users are people who have been granted access to the Hyperion Enterprise applications. User groups are sets of users. A security class is a collection of securable Hyperion Enterprise tasks and application elements that we have defined. Once we defined security classes, users, and user groups, we assigned one of four levels of access rights to security classes for user groups and users. This enables us to set security for many users to many tasks with minimal effort.

6. *Security Classes*

A security class is a collection of items in the application to which administrators can restrict access. The security administrator is responsible for creating security classes. The items that we include in a security class can include tasks, such as posting journals, or application elements, such as access to entities and accounts. When we set up security, we assigned security classes to items and then assigned users and user groups access rights to these classes. For example, we defined a security class called “admin_hi” and assigned it to the task “run rollovers.” We then assigned users and user groups such as “HQ_Admin”, access rights to this “admin_hi” security class.

Table 9.3 contains the current security classes in the current applications:



Security Class	Purpose
Maximum	This is Enterprise's default security class and it provides maximum access. This security level is used for low-risk, read-only type access.
ADMIN_X	No tasks assigned at this time.
ADMIN_HI	High level tasks that are limited to systems administrators at all times.
ADMIN_LO	These tasks are generally performed by administrators, but may be released to bureau level users on a limited and supervised basis.
DATA_EDIT	Routine tasks that users can perform in their day-to-day use of the system.
DATA_EXTRACT	Tasks revolving around extracting data from applications. Note that by design, the ability to extract and view data is available to all users.
BUR_FWS	Security class to limit access to FWS personnel only.
BUR_USGS	Security class to limit access to USGS personnel only.
BUR_BIA	Security class to limit access to BIA personnel only.
BUR_BLM	Security class to limit access to BLM personnel only.
BUR_MMS	Security class to limit access to MMS personnel only.
BUR_NPS	Security class to limit access to NPS personnel only
BUR_BOR	Security class to limit access to BOR personnel only
BUR_OSM	Security class to limit access to OSM personnel only
BUR_DO	Security class to limit access to DO personnel only
BUR_USBM	Security class to limit access for USBM purposes only

Table 9.3 - Security Classes



7. *Users and User Groups*

Users are people who have been granted access to the Hyperion Enterprise application, tasks, or application elements. We defined users in the security setup window in the applications module. We also defined user groups, which are sets of users with similar security requirements. For example, the “read-only” group was established to contain all of the auditor users who require read-only access to all applications.

When a new user needs access to an Enterprise application, the project manager at the reporting site will send a request to the Hyperion Enterprise system administrator asking for the addition. In the Enterprise application, the systems administrator will set up a user ID and password for the new user and add the user to the appropriate user group. With these credentials users are able to access the Enterprise applications and perform tasks according to the security profile in the group to which they belong.

Users and user groups can belong to multiple user groups. When conflicting rights result from a user or user group belonging to multiple user groups, the least restrictive rights apply.

8. *Access Rights*

Access rights determine whether a user can perform tasks or access specific application elements. For example, access rights determine the tasks users can perform, the accounts and entities they can view, data they can edit, and the schedules and methods they can view or change. After defining security classes, users, and user groups, administrators assign users and user groups one of four access rights to each security class in an application. The available access rights are modify, view, limited, and none. The Table 9.4 summarizes these access rights.

Assign...	To...
Modify	<ul style="list-style-type: none">• Allow users to perform tasks.• Allow users to change data.• Allow users to define or change application elements.• Allow users to create, change, and print reports and books.
View	<ul style="list-style-type: none">• Allow users to see, but not change data.• Allow users to see, but not change application elements.• Allow users to print reports and books.



Limited	<ul style="list-style-type: none">• Allow users to see, but not change application elements.• Prevent users from viewing or changing data.• Provide no access to data except in intercompany matching and consolidations.• Allow users to view or modify data for entities without providing access to the parent entity.• Prevent users from printing reports and books.
None	<ul style="list-style-type: none">• Prevent users from performing tasks by disabling menu commands• Prevent users from seeing the data or an application element exists. The secured element or data does not appear on the screen or in reports.• Prevent users from printing reports and books.

Table 9.4. Access Rights

When a conflict results between individual rights and user group rights, the individual rights are retained. When conflicting rights result from a user or user group belonging to multiple user groups, the least restrictive rights apply.

9. *Anti-virus Protection*

Anti-virus software has been installed and configured to scan each server's hard drive at least once in a 24-hour period. Also, each instance of the anti-virus software has been set to update their virus files once a week. Anti password grabbing software has been installed to guard against malicious software such as Back Orifice, Slint and 10pth Crack (commonly used password grabbing software).

E. Online Help

From within Hyperion Enterprise or Hyperion Reporting users can access on-line help guides in PDF format. To access these guides users click on the "Help" menu (the help menu is the last selection on the menu bar) and select "Online Guides (PDF)" Adobe Acrobat Reader will launch and the file can be printed to the user's local printer. Keep in mind that some of the guides are hundreds of pages long. Users can also select F1 or click on the question mark in the toolbar to access Hyperion Enterprise's integrated online help. The online help contains the following types of information:

§ Procedural information needed to complete tasks within Hyperion Enterprise.

§ Window and dialog box explanations.



- § Links to access the online guides, which are in PDF format. The online guides are portable document format (PDF) files that are electronic versions of the printed manuals. They contain conceptual and procedural information, as well as examples, to assist in using Hyperion Enterprise and Reporting.
- § Users can navigate through the online help by using its contents, index, search, back, and desktop buttons. Users can also print any help topic.

F. Trial Balance Review

Several reports are available to assist in reviewing and analyzing trial balance data. Bureaus are expected to review selected reports on a weekly basis to ensure data and system integrity. **See Appendix J for a List of Hyperion Reports.**

G. Procedure for Updating Hyperion Enterprise Entities

If a bureau has a new entity or a change to an existing entity affecting their Hyperion Enterprise application, the designated bureau representative will send the request to the Hyperion systems administrators (Mike Sciortino and Manisha Tuli). Only certain bureau personnel have been designated with the responsibility for maintaining their bureau's entity structure and submitting change requests. These project members are listed below. The requests must be in the form of an email or fax to the Hyperion systems administrators.

- BIA Joe Murphy/Rusty Hargrave
- BLM Brad Walbruck
- BOR Doug Denardo/Bridget Beins
- FWS Bill Burns
- MMS Denver Linda McKinney/Teresa Weaver
- NPS Cindy Robinson/Ed Morris
- OS Mary Ellen Sargent
- OSM Greg Muehl/Terry Carollo
- USGS Maurice Roberts

Once the administrators receive the request, the administrator will evaluate the nature of the change, and work with the bureau representative to ensure the change is made in the proper fashion. Depending on the nature of the change, the entity addition/change needs to be reflected in all of the organizations within the bureau application. Also, depending on the nature of the change, the addition/change must be made to all of the categories and periods effected by the change (see the checklist below for the specific information needed). Any change to the bureau applications will also be made to the Department's consolidated application.



After all changes are made (to both the bureau application and the consolidated application), a database consolidation is performed on all categories and periods impacted by the change.

Following the consolidation the administrator will run the bureau application "Tots" reports to ensure that all organizations total each other and that there are no unintended side-effects as a result of the change. The "Tots" report, short for "totals" report, is a balance sheet report that compares total assets/total liabilities by organization for each of the categories in the application.

Once the totals are verified as correct, the systems administrator will then send a confirmation email back to the bureau representative noting that the change has been made. The bureau representative will then verify that the change was made to their satisfaction and notify the Hyperion administrators if there are any problems.

For documentation purposes, the administrator will print the email, note the date of the change and place the email in the bureau application file.

The following is a checklist of the information required to update the entity structure:

- Entity label
- Entity substructure (One Year, X-Year, Multi-Year, etc.)
- Entity description
- Entity's relationship in the FACTS organization (to which parent does the new entity belong?)
- Entity's relationship in the BUR_SEGMENT organization (to which bureau segment does the entity belong?)
- Also provide any percentage split between multiple segments, if required.
- Entity's relationship in the SOF organization.
- Entity's relationship in the SBR organization.
- Entity's relationship in the DOI Appor Cat organization.
- Category affected by the change (FY2002 only, all categories, etc.)

H. Adjusting Journal Entries

Journal entries are used to record changes in account values and maintain an audit trail of those changes. Post-closing adjusting journal entries **must** be used in order to maintain the integrity and accuracy of the consolidated financial statements and ensure consistency between bureau reports, Department-wide reports and FACTS data.

1. *Journal Entry ID Numbers*



- a. Journal numbers are used as an identifier for each journal entered. They are also used as a filter when selecting journal entries to include in reports. Therefore, it is imperative that journal entry ID numbers are standardized. The following is a sample of a journal entry ID number: 01_Q203_0001

01 = Bureau Code
Q? = Quarter designator (or BB for Beginning Balance)
FY* = Fiscal Year designator
0001 = Serial counter number (Include leading zeros so that journal entries remain in numerical order - trust us on this one!)

***Note:** Prior year adjustment entries will have "PY" in place of "Q?" and "00" in place of "03" in the label and must be posted to the FY2002 Category.

- b. In order to ensure the verifiability of the Department's FACTS I & II submissions, any entries made after the Department's FACTS I & II cutoff dates, will be coded.

FACTS I cutoff is scheduled for November 29, 2003 when the Hyperion Enterprise applications are scheduled for a data lock down.

FACTS II cutoff is scheduled for November 8, 2003. Any journal entries posted ***after*** this date will include an "F" after the serial counter number, e.g.: 01_Q403_0001F.



- c. Table 9.5 presents bureau assigned codes to be used in creating journal entry ID numbers:

Bureau Code	Bureau
01	Office of the Secretary
02	Office of the Inspector General
03	Office of the Solicitor
04	Office of Insular Affairs
05	National Indian Gaming Commission
06	Bureau of Reclamation
07	National Park Service
08	U.S. Geological Survey
09	U.S. Bureau of Mines
11	Bureau of Land Management
16	Fish and Wildlife Service
17	Minerals Management Service
18	Office of Surface Mining
20	Bureau of Indian Affairs
21	Office of Trust Fund Management

Table 9.5 – Bureau Codes for Journal Entry Labels

Use of these journal entry label formats is required.

2. ***Journal Entry Descriptions***

The journal entry descriptions provide information regarding the purpose for the entry being posted and are a necessary part of the audit trail of a journal entry. The description should be detailed enough so that someone unfamiliar with the transaction will understand the reason for the adjustment and the source of the data.

3. ***Journal Codes***

Every journal entry must have a journal code. For FY2003 reporting purposes, new journal entry codes have been added to assist in identifying the cause of post yearend adjustments. Table 9.6 summarizes these codes.



Hyperion Code	Description/Purpose
J_Accruals	Accrual Activity
J_Alloc_Trans	Allocation Transfers
J_Corr_Bud	Budget Corrections
J_Corr_Gen	General Corrections
J_Corr_Prop	Property Corrections
J_IntraBur_Elim	Intra-Bureau/Dept Elimination Activity
J_PY_Adj	Adjusts prior year data
J_Reclass	Presentation Reclass – not posted to GL

Table 9.6 – Journal Codes

4. *Balanced and Unbalanced Adjustments*

Each journal entry created must be in balance prior to posting in Hyperion Enterprise. A balanced journal entry is one in which the total debits are equal to the total credits for each entity (fund/subfund) and for proprietary and budgetary accounts within each entity. The default security in Hyperion Enterprise prohibits unbalanced journal entries.

There are two known occasions when unbalanced entries may need to be posted to Hyperion Enterprise:

- a. Due to a Microsoft Windows bug, when a journal entry contains a large number of lines with multi-million dollar amounts, a digit will be added several places after the decimal (e.g. millionths of a penny: \$100,000,000.000000003.). These added digits can cause the entry to be “out of balance” according to Hyperion Enterprise.
- b. In certain cases, bureaus may inadvertently load out of balance data. The out-of-balance condition can only be corrected with an unbalanced journal entry.

Bureau personnel with rights to modify data do have the ability to post unbalanced journal entries to the current fiscal year only to correct the conditions specified above. To mitigate the risk of creating out of balance conditions, the NBC, the department, and the bureaus rely on a battery of data integrity reports to highlight any out of balance trial balances. When these out of balances are identified, they are immediately brought to the attention of bureau personnel and corrected.

5. *Changes to Existing Hyperion Adjusted Journal Entries*

To cut down on the number of entries in the financial statement application and to



provide for a better audit trail, bureaus are able to correct previously recorded erroneous journal entries as needed. If a bureau decides that a correction is needed, the journal entry must first be unposted, corrected, and then posted again. This can be done up to the appointed cutoff dates in which new journal entries are required and must be labeled as described in Section C.1.b. above.

The bureaus are able to make changes to their journal entries for the current year only (the prior year data cannot be changed) until the cut off date. After the cutoff date, the data is locked down and the bureaus cannot change data without PFM's approval. There are several security options the bureaus can choose from to further safe guard their data. For example, some bureaus have grouped users into two categories: bureau admins and bureau users. The bureau admins are the only people who can post journal entries at the bureau level. The bureau users can only prepare entries. This security stratification varies by bureau.

It is **imperative** the bureaus notify the Hyperion administrators (Mike Sciortino, Manisha Tuli, Patricia Bushrod, Debra Carey and Donna McKethan) by email so that we can ensure the consolidated application is updated with any changes to journal entries.