

4/12/2006

CONNECTIONS

Step-by-Step Guide:

Security



**CONNECTIONS Training Project
SUNY Training Strategies Group**

This material was produced under a contractual agreement with:
*CONNECTIONS Training Project
Training Strategies Group
Office of the Provost and Vice Chancellor for Academic Affairs
State University of New York*

**CONNECTIONS Step-by-Step Guide:
Security
TABLE OF CONTENTS**

Welcome and Participant Information	1
The Content of this Guide	1
Features of this Guide.....	2
Module 1: Introduction to CONNECTIONS Security.....	3
What Is CONNECTIONS Security?	4
Security Access Flow.....	4
The Security Coordinator’s Role in the Security Function	5
Security Questions.....	7
Module 2: System and Application Access	8
System Security vs. CONNECTIONS Security	9
How WEBSTAR Is Used to Manage NT Access	9
Module 3: The Organizational Structure of CONNECTIONS.....	13
Definitions and Descriptions of Organizational Concepts	14
Module 4: Principles of Access Within CONNECTIONS	16
Definition/Description of Access	17
Main Routes of Stage Access.....	18
Restrictions to Routes of Stage Access.....	20
Dialog Access	20
Module 5: Building Blocks of Security in CONNECTIONS	21
Introduction to Terms	22
Security Attribute (SA)	23
Business Functions (BF).....	23
Business Function Profile (BFP)	25
Security Profile (SP).....	29
Module 6: Adding Staff in CONNECTIONS.....	30
Job Types	33
Selected Job Types Only Check Box.....	33
Selected Business Functions Only Check Box	34
Attributes Button	34
System Edits on the Staff Security Window.....	34
Notifying Workers of Newly Assigned Business Functions.....	36
Making a Worker Case Assignable	36

Module 7: Maintaining Staff in CONNECTIONS	37
In/Out-Assigning	38
Assigning Additional Business Functions	39
Removing Business Functions from a BFP	40
Designees	41
Changing the Unit Approver.....	45
Transferring Workers	46
Moving Workers Between Agencies	47
End-Dating Staff.....	47
<i>Removing Inactive Staff from a Unit.....</i>	<i>48</i>
Removing Assignments from a Workload.....	50
Reinstating Staff.....	51
Security Coordinator Responsibilities When a System Build Includes New Business Functions.....	52
Transferring Security Coordinator Responsibilities.....	52
Updating Staff Names.....	54
Module 8: Unit Maintenance in CONNECTIONS	55
Creating a Unit.....	56
Changing a Unit's Specialization	58
Deleting a Unit	59
Unit Organization Housekeeping	60
The Agency Access Window	62
Organizational Hierarchy Window.....	75
Module 9: Security Reports.....	79
Requesting Security Reports	80
Staff Security Report.....	81
Business Function Report.....	82
Assignee/Designee Report.....	83
Unit Approver Report	84
Organizational Hierarchy Report.....	85
Appendix A: Security Coordinator Roles and Responsibilities	86
Appendix B: Glossary of Terms Used in Security.....	88
Appendix C: Codes Used in CONNECTIONS Security.....	92
Appendix D: CONNECTIONS Security Profiles.....	97
Appendix E: Job Types.....	107
Appendix F: Business Functions Guidelines	112

Appendix G: Security Report Samples.....	119
Appendix H: Information Resources	123
Appendix I: Frequently Asked Questions	125
Appendix J: OCFS Security Guidelines	127
Appendix K: The WEBSTAR Agency Users Report	131

Welcome and Participant Information

As your agency's CONNECTIONS Security Coordinator, you play an important role in facilitating workers' use of the CONNECTIONS system in their casework.

Workers' ability to access, record and update casework information depends on the proper assignment and maintenance of security permissions and functionalities. The assignment and maintenance of those permissions and functionalities is the job of the CONNECTIONS Security Coordinator.

The Content of this Guide

This guide leads you through the functions in CONNECTIONS that you'll use in your role as Security Coordinator. It contains step-by-step instructions for accomplishing Security maintenance tasks in CONNECTIONS, introductory remarks that provide a work context for these tasks, and hints on how to carry out these tasks efficiently and effectively.

Updates have been made to this guide to reflect enhancements for future builds. Security architecture was added to the new Case and Financial Management functionality that will be implemented with Build 18. Working in conjunction with current system security, the security architecture will accommodate the needed flexibility and functionality for Family Services Intake and Family Services Stages.

Although the additional security structure affects *only* Build 18 (and future) functionality, Security Coordinators will be able to use a single interface. Please note that these changes will not affect Child Protective Services or Foster Adoptive Home Development (FAD) functionality. Access to information will not be limited if a worker has a role in a stage.



Note:

Any visible identifying data in this guide is simulated.

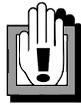
Features of this Guide

Two features of this guide help you quickly identify the information you need:

- **Tips**, set apart in margin boxes, provide information to help you carry out CONNECTIONS tasks efficiently and effectively. Icons in the boxes help focus your attention on the following kinds of tips:



Helpful hints



Things to watch out for

- **Subdivided Instructions:** The step-by-step instructions for each procedure are subdivided into major sub-steps to make it easier to jump ahead to the correct step if you're already on the window you need to access. Step-by-step instructions assume you have accessed the CONNECTIONS Toolbar.

We hope you find this to be a useful aid in your work as Security Coordinator!

Module 1:

Introduction to CONNECTIONS Security

An understanding of the function served by CONNECTIONS Security provides a foundation for learning how to manage CONNECTIONS Security for your agency. This module will provide you with a basic understanding of why CONNECTIONS includes a security component and the role Security Coordinators play in managing that component.

By the end of this module, you'll be able to:

- define the function of security in CONNECTIONS;
- describe how CONNECTIONS determines a worker's access;
- describe the Security Coordinator's role in the security function; and
- determine whom a worker should talk to regarding a security issue.

What Is CONNECTIONS Security?

CONNECTIONS' effectiveness as a casework tool depends in large part on data integrity. The information in the CONNECTIONS database needs to be as accurate as possible. Another underlying factor in CONNECTIONS' effectiveness is data confidentiality. Only those workers who meet certain guidelines of involvement in a stage should be able to view or modify data for that stage.

Workers must understand their role and responsibilities regarding the security of CONNECTIONS information. They have an obligation to protect and preserve all information in a consistent and reliable manner. CONNECTIONS users are responsible for ensuring that appropriate physical, logical and procedural controls are in place to preserve the confidentiality, integrity, availability and privacy of CONNECTIONS information.

CONNECTIONS security protects information about cases and people from being viewed or modified by workers who should not have access to that information. It provides caseworkers with access to all the necessary information to make informed casework decisions, while preventing navigation into areas they are not authorized to view or modify.

Access to information in CONNECTIONS must be restricted to what is necessary for the worker's normal performance of job responsibilities; this is accomplished by assigning each worker a unique User ID. The User ID and Password are the "keys" to access certain agency information. A worker's User ID and password are also a form of identification; they link a worker to actions in the system. Workers are responsible for actions taken with their User ID and password; it is up to each worker to protect his/her password to prevent unauthorized access or misuse of information.

CONNECTIONS security also categorizes workers into role types within the system. You can also classify workers by Job Types.

CONNECTIONS security operates independently of other system functions, but it affects every part of the system. For example, the Security Coordinator may only have access to Security functions, but using those functions allows a determination of whether or not workers can access any other part of CONNECTIONS.

Security Access Flow

When a worker logs on to CONNECTIONS, the system checks security information attached to that worker's logon ID to determine which windows and functionalities the worker will be able to access. If a worker's security information does not include access to certain areas or functions of the system, menu commands or buttons that access those areas or functions will be disabled.

CONNECTIONS users are not allowed to prove a suspected weakness; in other words workers should not attempt to find work-arounds or bugs in the system. All CONNECTIONS users should be aware of the procedure for reporting security incidents that may have an impact on the security of information. Workers must report any incidents to their appropriate supervisor and the Security Coordinator.

If a worker's security information limits that worker's access within a particular CONNECTIONS *dialog* (see page 20), the system will check the security information as the worker attempts to enter individual windows to determine whether the worker is allowed to access those windows.

CONNECTIONS information needs to be maintained in a secure, accurate and reliable manner but also be readily available for use by workers needing information. (Refer the OCFS Security Guidelines in Appendix J for further details.)

The Security Coordinator's Role in the Security Function

CONNECTIONS security uses a decentralized approach in which each agency controls the security assignments for its own staff. The Security Coordinator is the person responsible for managing an agency's security assignments. Each agency should have a designated Security Coordinator and a backup Security Coordinator. It is the Security Coordinator's responsibility to ensure that all security processes and procedures are followed.



If no one is available to perform the Security Coordinator's role, OCFS CONNECTIONS staff will assist in the assigning of security maintenance abilities to a new Security Coordinator.

The Security Coordinator is also responsible for ensuring the security of the CONNECTIONS system by controlling access to information.

An agency may find it necessary to allow workers to complete their job functions outside of the office. When working from a remote location, the following security controls need to be considered and are not limited to:

- the existing physical security of the remote location;
- the communication security requirements;
- the sensitivity of the information that will be accessed and transmitted; and
- the threat of unauthorized access.

If workers must store or transmit confidential information on portable computer devices, protective measures must be implemented. When using mobile computing devices such as laptop computers, Personal Digital Assistants (PDAs) and cellular phones, special care should be taken to ensure that information is not compromised.

When traveling CONNECTIONS staff using portable computers should not check these items in airline luggage systems. Confidential information should be removed prior to traveling; removing confidential information from portable computers should be done on a regular basis.

Dial-up modems should not be connected to computer systems that are on a LAN or another internal communication system, unless approved by the OCFS Information Security Officer. Also, no wireless network or wireless access point should be installed without performing a risk assessment and obtaining appropriate *written* approval from the OCFS Information Security Officer.

Software should never be installed without the approval of the OCFS Information Security Officer. Software security patches are installed by OFT. Computers should be left logged off so

that security patches can be installed when users are not using their computer. (Refer to the OCFS Security Guidelines in Appendix J for instructions on logging off the system.)

Anti-virus software will protect against the vast majority of viruses and other vulnerabilities, but it's *not* fool-proof. Everyone has a responsibility to ensure proper precautions are taken to protect the network and ensure viruses don't get in or get spread.

As Security Coordinator, you may need to advise workers of their security responsibilities in guarding information. Workers should avoid using Internet, third-party or wireless fax services to send or receive faxes containing confidential information. If it is necessary to send confidential information via fax, workers need to verify the phone number prior to sending the fax and contact the fax recipient to ensure the fax is picked up immediately. Workers should also avoid sending teleconference call-in numbers and passwords to a pager, if sensitive information will be discussed in the conference; confirm that *all* participants are authorized to participate prior to starting any discussion.

Staff using CONNECTIONS should only connect to the Internet for purposes authorized by your agency's management. CONNECTIONS staff should not use the Internet for any reason that could breach security. This includes not accessing external e-mail accounts (e.g., Hotmail or Yahoo).

Precautions need to be taken when exchanging information over the telephone. All employees should take care that they are not overheard when discussing confidential matters on the telephone. Workers should also avoid leaving sensitive or confidential messages on voicemail systems. Workers must be sure to take extra precautions when using mobile devices in public areas outside of the workplace. Any use of wireless or cellular phones should be avoided, whenever possible, when discussing sensitive or confidential information.

Confidential information should not be exchanged over a messaging system unless authorized by the OCFS Information Security Officer, after a formal risk assessment of the situation is performed. No external public Instant Messaging, Team rooms or Conferencing services should be used to conduct business unless authorized *in writing* from the OCFS Information Security Officer.

In your role as Security Coordinator, you may need to monitor workers' activity on the OCFS network, including email. Workers should not have any expectation of privacy in the information stored in or sent through CONNECTIONS, as you reserve the right to monitor or search any system at all times. Workers are notified of this each time they log onto the network (a privacy message displays). You may find it necessary to monitor network traffic.

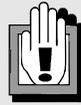
In the broadest terms, the role and responsibilities of the Security Coordinator can be summarized as follows:

- When new staff join the agency, make sure they receive appropriate system access. (See Module 6: Adding Staff in CONNECTIONS.)
- As worker responsibilities, staff makeup, and system functionality change, maintain staff security to ensure that workers' access to CONNECTIONS accurately reflect those changes. (See Module 7: Maintaining Staff in CONNECTIONS.)

For a more detailed list of local Security Coordinator roles and responsibilities, see Appendix A.

Security Questions

When workers in an agency have questions or problems concerning CONNECTIONS security, the Security Coordinator serves as the first point of contact in getting those questions answered. The Security Coordinator determines if the question or problem is a System or Application issue



An exception occurs when a worker requests expanded security access to CONNECTIONS. In this instance, the worker must request the new access from the supervisor. If the supervisor determines the change to be appropriate, the supervisor will request that the Security Coordinator make the change in CONNECTIONS.

and assists the worker in getting the issue addressed. (See Module 2: System and Application Access.)

Most application access issues are handled locally. If the problem can't be addressed locally, a call should be made to the NYS OFT Enterprise Help Desk (1-800-697-1323). A good starting point for system access issues is the local LAN administrator.



The Implementation Coordinator is another source for information and answers, especially for information about changes to CONNECTIONS and how those changes affect system security.

Module 2: System and Application Access

Access to CONNECTIONS can be broken down into two related types of access: access to the computer system and access to the CONNECTIONS application itself. This module will introduce you to these two types of access, who maintains them, and some of the processes involved.

By the end of this module, you'll be able to:

- differentiate between *system* and *application* security;
- recognize who is responsible for maintaining each type of security; and
- describe how WEBSTAR is used to manage access to the Windows NT system.

System Security vs. CONNECTIONS Security

Security for CONNECTIONS consists of two components: System security and Application security.

- *System security* focuses on granting access to the OCFS computer system based on a worker's NT logon ID. Most aspects of system security are handled through an application called WEBSTAR (Web Enhanced Basic Security to Authorize Resources). An agency's local LAN (Local Area Network) Administrator is given the ability to access and use WEBSTAR by the Office for Technology (OFT). The local LAN Administrator uses WEBSTAR to request NT logon IDs for workers in that agency and to reset NT logon passwords when necessary. The NT logon ID allows a worker to logon to the computer system.
- *Application security* focuses on granting access to the CONNECTIONS application itself. After assigning an NT logon to a worker, the agency's local LAN Administrator gives the worker "standard" access to CONNECTIONS using WEBSTAR. (See "How WEBSTAR is used to Manage NT Access" on page 9.) Standard CONNECTIONS access does not allow a worker to access any parts of the CONNECTIONS Toolbar that involve CONNECTIONS client data. Any CONNECTIONS access beyond standard access is granted by the local CONNECTIONS Security Coordinator, who also maintains workers' access, including making any needed changes.



All users in your agency must follow established OFT/OCFS password standards. Automated system controls support the password standards as outlined in the OCFS Security Guidelines in Appendix J. As Security Coordinator, you need to ensure they are regularly practiced.

How WEBSTAR Is Used to Manage NT Access

WEBSTAR allows LAN administrators to have real-time control of Windows NT accounts and Exchange mailboxes. WEBSTAR can be used to add, modify, and delete accounts to accommodate system and user needs, with most changes taking effect immediately. As a dynamic system, WEBSTAR returns error messages that can be acted on immediately, resulting in quick, efficient account management.



For more information on WEBSTAR, refer to the nyseWebstar User Manual.

From the OCFS intranet home page, click on the **nyseWebstar-NYSeMail/HSEN** link under the Employee Resources section (on the left side of the page), then click on **MANUAL** at the top of the nyseWebstar page. The User Manual displays in PDF format.

WEBSTAR will display information and options based on the user, so regular workers will only see features that affect them directly (such as “Update My Mailbox”), while the LAN Administrator will have access to the full complement of features and procedures.

WEBSTAR is accessed through a link on the New York State Human Services intranet site. The WEBSTAR interface is a series of Web pages. The first of these includes a table of available options, which will vary depending on the person accessing WEBSTAR.

Depending on a particular worker’s system access, this list might also include other options such as:

Browser Settings	Get instructions for Internet Explorer settings and login.
Beginner’s Help	New Administrator help page.
Inquiry	Inquire about users, computers and group.
Update Yourself	Update your address and phone number(s).
Your Administrator	Find administrator(s) of your account/computer.
Reset Password	Reset your password.

In addition to the options listed above, WEBSTAR allows a full administrator to perform additional functions, including the following:

RESET User Password	Resets the user account password by identifying the user by means of either his/her first <i>and</i> last name or user ID. You can verify either option by displaying the list of users you can administer (by clicking on the available button on this page), then entering the correct user. This process will also unlock the user account if it is locked. It is not necessary to know if the account is locked. The application will automatically unlock the account if needed.
UNLOCK HSEN User Account	Unlocks an account. In performing this function, if the user ID is locked it will be unlocked; if it is not locked, a message will display.
DISABLE HSEN User Account	Disables the User Account and adds the user to the Disabled-Users Group.
REENABLE HSEN User Account	Reenables an account and removes the user from the Disabled-Users group.
CREATE HSEN User & NYSeMail Account	Creates a new user ID, or creates a new account using a previously assigned user ID, with or without a mailbox. If a mailbox is required, you will need to wait up to 24 hours before Associating a mailbox after completing the application. To Associate a mailbox, go to the User Administration Menu and enter the user ID in the textbox. If a mailbox is required, the Create process will <i>not</i> be complete until a mailbox is associated with the user.
MANAGE User &	Generates the Agency Users Report, which is a listing of

NYSeMail Account	all existing NT accounts for an agency. For an example of the Agency Users Report, see Appendix G in the <i>Security Step-By-Step Guide</i> .
DELETE User & NYSeMail Account	Adds the account to the To Be Deleted group and moves it to a temporary storage location until deletion.
ASSOCIATE NYSeMail Object to HSEN User	Associates a mailbox. The Create Account/Mailbox process is not complete until you Associate a mailbox, since the user will not be able to use his/her account until this step is completed. You will need to wait <i>up to 24</i> hours to allow time for replication before attempting to Associate the mailbox.
ADMINISTER NYSeMail Objects	Provides access to the following options: <ul style="list-style-type: none"> ▪ SHARE a Mailbox ▪ DELETE Mail Object ▪ UPDATE 'Custom Recipient' ▪ CREATE NYSeMail Object for Existing Account ▪ CREATE NEW Distribution List ▪ MANAGE Existing Distribution List ▪ DELETE Existing Distribution List
UPDATE Specific Attribute	Updates specific user attributes, such as Account Expiration Date.
TRANSFER State Employee	Transfers a user account to another agency on the HSEN network (e.g. OFT, OCFS, OTDA, DOL, and DOH). This function is only available for employees from a designated state agency and <i>not</i> for employees from a county or voluntary organization. This process is completed in two steps. First, the user account is transferred to a temporary container "User Transfer" and all previous membership in any security groups is deleted. Next, the user account is transferred from the "User Transfer" container to the target agency OU. If you do not want to keep same home directory and mailbox then you need to create a new user account.
MOVE an Account	Allows movement for a user from one location to another and updates group memberships appropriately.
RESTRICT Account Access to Specific Workstations	Restricts workstation access by allowing you to specify the workstations that the user will be allowed access to.
CONVERT to Custom Recipient	Deletes the user's mailbox and points to another e-mail address known as a Custom Recipient.
Administer Application Access	Adds, updates and removes access to CONNECTIONS. This option permits standard CONNECTIONS access for a worker, which gives access only to the CONNECTIONS toolbar.

When a worker's NT account is disabled through WEBSTAR, WEBSTAR also removes the NT ID in the *Staff Security* window, even if the worker has not been end-dated. This removes the worker's access to CONNECTIONS, so it's important to end-date a worker *before* disabling or deleting him/her from the system through WEBSTAR. (See "End-Dating Staff" on page 47.)



A newly created NT account and mailbox appear in the address book on the same day they are created, but will not be available in CONNECTIONS until the following day, after an overnight batch run.

If a worker needs to be reinstated in NT, OCFS CONNECTIONS staff use WEBSTAR to re-enable the NT logon for that worker. (See "Reinstating Staff" on page 51.)

Module 3:

The Organizational Structure of CONNECTIONS

An understanding of CONNECTIONS security depends in part on familiarity with the way in which staff information is organized within the system. This module introduces the terms and concepts used in organizing staff information in CONNECTIONS.

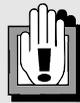
By the end of this module, you will be able to:

- define *staff*, *unit* and *agency* as they are used in CONNECTIONS;
- describe the different staff designations used in CONNECTIONS; and
- explain how to organize agency, unit and staff information for inclusion in CONNECTIONS.

Definitions and Descriptions of Organizational Concepts

Worker information within CONNECTIONS is organized around the concepts of Staff, Unit and Agency.

- An **agency** is a local district, voluntary agency, or other jurisdictional entity made up of one or more units.
- A **unit** is a grouping of staff. A unit generally consists of a group of workers performing similar types of work and a supervisor managing the unit.
- A **staff** person is an employee, contractor, or consultant of OCFS, a Regional Office, a local DSS district, a voluntary agency, or one of the following state agencies: DFY, CCF, OMH, OMRDD, or CQC.



It is the agency's responsibility to make sure that any third party contractor or consultant has access appropriate to complete tasks and that a confidentiality agreement has been signed before working with CONNECTIONS.

Within a unit, staff are categorized in the following hierarchy (from lowest to highest): Workers, Supervisors, Maintainers and Managers. This can allow some individuals within the unit increased access based on their role within the unit.

A separate category within the unit is the **Unit Approver**. This role should be assigned to a unit supervisor. When any worker in a unit saves and submits work for approval, it is automatically sent to the Unit Approver for review and approval. In addition, the Unit Approver receives certain additional types of access to aid in the supervision of a unit's work. Specifically, the assignment of the UNIT SUM ACCESS Business Function (see "Business Functions" on page 23) provides Unit Approvers with view access to stages within the *Assigned Workload* of any staff person in their unit and the same maintain access as the workers in the Unit.

Each unit has one and only one approver.

Creating the Organizational Structure

The organizational structure of CONNECTIONS was introduced as part of Release 1 in 1996. At that time, Security Coordinators were required to gather information about their agencies, organize that information to conform to CONNECTIONS' organizational structure, and enter the information in the system.

While the organizational structure is still in place and there is no need to go through the process of creating it, it is helpful to understand the steps involved and the information required.

Data gathering – Security Coordinators were required to gather information about the staff in their agencies using organizational charts and directories.

Organizing unit structure – A worksheet was completed listing the following information for each unit in the agency: agency code, site code, zone (NYC only), unit number, unit supervisor, and names of unit members.

Completing staff lists for each unit – Worksheets included the following information for each unit: agency code, site code, zone (NYC only), unit number, unit specialization, unit supervisor information (name, role, category, in/out assignment, case assignable Y/N, and CPS worker Y/N), and unit staff information (name, role, category, in/out assignment case assignable Y/N, and CPS worker Y/N).

Completing staff information – A worksheet was completed for each staff member listed in the staff list worksheets with the following information: name, unit number (for the unit to which the respective worker is In Assigned), SCR ID, CCRS ID, WMS ID, business address, and business phone.

Recording data – Information from the completed worksheets was recorded into CONNECTIONS and staff members were placed into the newly created units.

Module 8 details how to establish an organization hierarchy in CONNECTIONS that best represents your own organizational structure.

Module 4: Principles of Access Within CONNECTIONS

Access to data in CONNECTIONS is founded on a set of rules and concepts having to do with a worker's involvement with a stage, the access permissions given to that worker, and the type of case or stage in question. This module will examine the interrelationship of these factors and the role they play in the use of CONNECTIONS.

By the end of this module, you will be able to:

- define *access* and explain the basic principles and issues to be considered when dealing with access in CONNECTIONS;
- list the main routes of Stage Access in CONNECTIONS, some restrictions to those routes, and how exemptions to those restrictions are granted; and
- define *dialog security* and describe how it works.

Definition/Description of Access

Access in CONNECTIONS is defined as a worker's ability to view or maintain information. *View Access* is the ability to see the information without having the ability to modify it in any way. *Maintain Access* is the ability to add, modify, update, delete, or otherwise manage information.

Access to information in CONNECTIONS is controlled through a variety of methods, such as denying access to a window (or dialog – see “Dialog Access on page 20), disabling particular navigational paths from a window (by disabling buttons, which appear grayed out), or filtering out and not displaying certain information returned from a search.

The first type of access a worker must receive is *standard* access, which is assigned when a worker is first given access to CONNECTIONS by the local LAN administrator. This allows the worker to see the CONNECTIONS Toolbar, but does not allow the worker to access all of its functions. All buttons having to do with access to CONNECTIONS client data (the **UNIT**, **PERS** and **CASE** buttons) are disabled (grayed out).

It is the Security Coordinator's responsibility to grant the worker the permissions that provide the additional access the worker needs in order to complete tasks in CONNECTIONS. This access needs to be broad enough to allow the worker to get the job done without being too broad (and therefore granting inappropriate access).

In any particular instance, a worker's ability to use CONNECTIONS to complete tasks is the result of a combination of factors:

- The worker's role in the stage
- The worker's role in the unit
- The worker's job responsibilities (reflected in CONNECTIONS as Business Functions) and
- Specialized job responsibilities (reflected in CONNECTIONS as additional, more restrictive Business Functions.)

Business Functions (BF) will be examined in detail in Module 5. Stage Roles and specialized job responsibilities are discussed in the next section.

Agencies that use CONNECTIONS are categorized into one of nine *office types* (DSS, Regional Office, District, Voluntary Agency, DFY, CCF, OMH, OMRDD, and CQC). An agency's Security Coordinator assigns Business Functions to workers from a list available based on the office type. An office type's list of available Business Functions is known as its Security Profile. The Security Profile and, therefore, types of access available to workers in an office, will vary according to office type. (More details about Security Profiles are available in Module 5 and in Appendix D.)

Workers can access information for stages that are the primary responsibility of other units and agencies. Such access is granted through out-assignments (see “In/Out Assigning” on page 38), assignments as a Secondary worker, and the use of particular Business Functions (see “Main Routes of Stage Access” on page 18). The type of access (View or Maintain) and particular information available will depend on the way access is granted.

Main Routes of Stage Access

As mentioned in the previous section, a worker's access to a stage in CONNECTIONS is the result of a combination of factors: the worker's role in the stage, the worker's role in the unit, and access permissions given to the worker.

Stage Roles

CPS and FAD Roles – There are two possible roles a worker can have in a CPS or FAD stage:

- ▶ **Primary Worker** – The Primary worker has primary responsibility for a stage. There can be only one Primary worker for a stage.
- ▶ **Secondary Worker** – The Secondary worker has been assigned some supporting tasks in a stage. There can be any number of Secondary workers assigned to a stage.

An assignment to a stage as the Primary worker allows navigation to that stage through the *Assigned Workload* or through the *Case Summary* window with Maintain access. Primary workers can also view information for other stages in the same case. Secondary workers have View and Maintain access to information relevant to assigned task(s) in stages to which they are assigned.

Implied Role – Workers have an implied role in a stage if a person in a stage on their workload is also involved in that other stage. An implied role gives the worker view access (but no maintenance abilities) to other stages with which that person is associated. (Access is through *Task List > Person List > Case List*.)

Historical Role – Workers with a Primary or Secondary role at the time a stage was closed will have View access to information for that stage. In addition, an historical Primary worker can modify some stage information using Local Data Maintenance.

Build 18 Family Services Stage (FSS) Roles

Each worker is assigned one of the following four roles, which govern what workers do and their ability to record data in various system components. Basically current work roles remain the same, but in some areas CONNECTIONS will necessitate changes to how staff do their work.

Case Manager

Every Family Services Stage (FSS) has a single Case Manager, who *must* be local district staff. The Case Manager provides oversight for the case and must approve the Family Assessment and Service Plan (FASP). When the Case Manager also acts as the Case Planner, the Case Manager's supervisor must approve the FASP.

Case Planner

The Case Planner, who may be either local district or voluntary agency staff, is responsible for the coordination of work with a family. The Case Planner is also the author of the FASP and is responsible for the entirety of its contents and the timeliness of its submission for approval. This means the Case Planner must coordinate the documentation of all work in the FASP and either accept it as contributed by the worker(s) or revise it accordingly. The Case Planner sends the FASP to the Case Manager for approval. There may be only one Case Planner in the FSS.

CPS Worker/Monitor

The CPS Worker/Monitor *must* be local district staff and may complete the CPS Risk and Safety Assessments. The system supports, but does not require, a review of the FASP by a CPS Worker/Monitor. The Case Planner needs to alert the CPS Worker/Monitor in circumstances where s/he needs to complete work in, or review, the FASP.

Caseworker

Caseworkers may be either local district or voluntary agency staff. These workers may be Associated to a specific child(ren) in the FSS and can complete specific work within the FASP, such as the Child Scales and Foster Care Issues regarding the child(ren) to whom they are Associated. There may be multiple Caseworkers assigned to the FSS.

Role in Unit/Unit Hierarchy

Staff are categorized within a unit into a hierarchy of Workers, Supervisors, Maintainers and Managers; each unit also contains one Unit Approver. Unit members other than the Unit Approver may need to access workloads of other unit members in order to assign stages or record case information, such as fingerprint results. Having a role in the unit hierarchy as (or above that of) the Unit Approver, combined with certain Business Functions, will grant that access. For example, if a worker is the Unit Approver (in addition to being assigned the UNIT SUM ACCESS Business Function), the worker will have access to the *Assigned Workloads* of all workers in the unit and, therefore, can access all stages in the unit. This role will also allow workers to perform certain functions above and beyond the security rights provided by their own role in a stage or the assigned Business Functions (other than UNIT SUM ACCESS).

CONNECTIONS will check when a worker attempts to access or perform specific functions on certain windows to make sure the worker has a particular role in the Unit Hierarchy. Examples of this type of window are the *Assign* window, the *Case List* and the *Assigned Workload*.

Assignment of Appropriate Business Functions

The Security Coordinator uses the assignment of Business Functions to expand a worker's access in CONNECTIONS beyond "standard" access to the Toolbar. Business Functions increase the worker's access beyond that resulting from a Stage Role or Unit Role.

Combinations of Business Functions are used to tailor a worker's access to complete casework duties. Such expansions of access are assigned on a person-by-person basis.

Business Functions (BFs) will be examined in detail in Module 5, but here are some examples of their use:

- Workers in a unit with a role above the Unit Approver can be assigned the UNIT SUM ACCESS Business Function. Those workers will then have Maintain access to every stage in the Unit.
- Workers with the ACCESS ALL DIST Business Function can view all stages in their district through Case Search, unless the associated cases require further security as described in the next section.

Restrictions to Routes of Stage Access

There are certain types of cases or situations that require additional security beyond that provided by normal routes of stage access. These special situations all require specific CONNECTIONS Business Functions, which are assigned by the Security Coordinator.

When access to a restricted case is required, the Security Coordinator can assign a particular BF that grants the worker an exception to the restriction.

The following table displays some of these restricted types of cases, the nature of the restriction, the corresponding BF that allows a worker to access the associated stage despite the restriction, and the result of that access. (In each instance, it is assumed that the worker has the required role in the stage or unit or the ACCESS ALL DIST Business Function.)

Type of Case	Nature of Restriction	Business Function that Allows Access	Result
Sensitive*	Case details of sensitive cases are not available from the <i>Case Summary</i> window.	VIEW SENSITIVE	Worker is able to access case details from <i>Case Summary</i> window.
Administrative Review	Administrative Review cannot be opened from the <i>Case Summary</i> window.	VIEW ADMIN REV	Worker is able to open <i>Admin Review</i> window from <i>Case Summary</i> window.

*A Sensitive Case is one in which an allegation of abuse or maltreatment has been made against an employee of the SCR or a local district.

Dialog Access

In CONNECTIONS, a dialog is a series of windows that work together to capture information or perform a function. For example: the Intake Dialog consists of all of the windows accessed while recording an Intake.

Certain dialogs require specific Business Functions (see Module 5) in order to modify information within the dialog. Some examples of this type of dialog are Clearance and Request for Information, Contracts, FAD, Intake and Resource. CONNECTIONS verifies a worker's security access on individual windows within such a dialog.

Module 5: Building Blocks of Security in CONNECTIONS

Preceding modules have provided the conceptual framework for CONNECTIONS Security functions. This module presents the basic tools used by Security Coordinators as they maintain security for their agencies.

By the end of this module, you'll be able to:

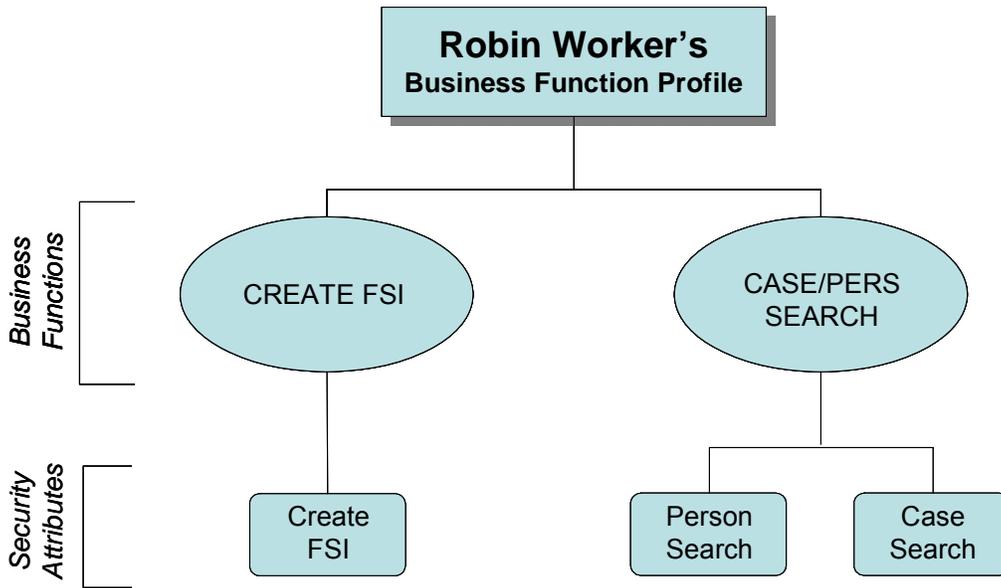
- define *security attribute* and explain how it is used in CONNECTIONS;
- define *Business Function* and explain how it is used in CONNECTIONS;
- define *Business Function Profile* and explain how it is used in CONNECTIONS; and
- define *security profile* and explain how it is used in CONNECTIONS.

Introduction to Terms

The “building blocks” of CONNECTIONS security maintenance are Security Attributes (SAs), Business Functions (BFs), Business Function Profiles (BFPs), and Security Profiles (SPs).

OCFS CONNECTIONS staff create Security Attributes and Business Functions to reflect system functionality and to meet casework requirements. A local Security Coordinator uses Business Functions to create Business Function Profiles that enable individual workers to do their jobs. Different types of workers will need different BFPs based on their work and responsibilities. For instance, a CPS worker might need the ability to view a child protective case that is currently under investigation, while a FAD worker needs the ability to maintain a foster or adoptive home.

Security Attributes, Business Functions and Business Function Profiles—and the relationship between them—are described in detail in the sections that follow. That relationship is summarized in the following diagram.



Security Attribute (SA)

Security Attributes (SAs) are the primary manner in which access to CONNECTIONS is given. Each security attribute allows access to a particular window, dialog or functionality in CONNECTIONS.

Security Attributes are created by OCFS CONNECTIONS staff. They are not used directly by local Security Coordinators, but they function “behind the scenes” as the foundation for the Security Coordinator’s primary security maintenance tool: the Business Function (BF).

The following are examples of Security Attributes currently used in CONNECTIONS:

- Case Merge/Split (allows access to the *Case Merge/Split* window in modify mode)
- Maintain Security (allows a Security Coordinator to maintain Business Function Profiles for workers in the agency)

Business Functions (BF)

Business Functions (BFs) are used by the local Security Coordinator to maintain security and grant CONNECTIONS access to workers (beyond the “standard” access granted by the local LAN administrator through WEBSTAR). Business Functions are made up of Security Attributes. Like Security Attributes, Business Functions are created by OCFS CONNECTIONS staff.

A Business Function is designed to allow a worker to perform a particular function or group of functions. For example, supervisors need to be able to review and approve (or reject) the work of workers in their unit. The assignment of the UNIT SUM ACCESS Business Function provides the Unit Approver with View access to stages on the *Assigned Workload* of each staff person in the Unit and the same Maintain access as the workers in the Unit.

In some instances there is a one-to-one relationship between a Business Function and a Security Attribute. In other instances, a Business Function is made up of more than one Security Attribute. For example, the Business Function VIEW UNDER INV contains only the “View Under Investigation” Security Attribute, while the MAINT SECURITY Business Function for State workers contains three Security Attributes: “Maintain Security,” “Maintain Login,” and “View Business Functions.”

For a list of all Business Functions available for your office type, see Appendix D.

Business Functions for Security Coordinators

In order to perform security maintenance functions, Security Coordinators must have the following Business Functions in addition to “standard” CONNECTIONS access:

Business Function	Description
MAINT SECURITY	Allows Security Coordinators to view and assign Business Functions for workers in their agencies and to assign designees to other workers
MAINTAIN STAFF	Allows Security Coordinators to add, modify and delete staff information for workers in their agencies, including end-dating and reinstating workers
MAINTAIN UNIT	Allows Security Coordinators to add, modify and delete unit information for their agencies
MAINTAIN OFFICE	Allows Security Coordinators to add, modify and delete office information for their agencies
MAINT ORG HIER	Granted by State Staff for locally designated workers to maintain the <i>Organizational Hierarchy</i> window
MAINT AGY ACC	Granted by State Staff for locally designated workers to maintain the <i>Agency Access</i> window



Prior to the implementation of Build 17, each district/agency specified which individual(s) should receive these Business Functions.

Business Functions Requiring Special Handling

Certain Business Functions allow a worker to change data in a case. In some instances, these changes will alter the results of a search. These Business Functions are known as “Business Functions Requiring Special Handling” and they must be assigned with extra care.

One example of such a Business Function is the MAINT CLSD INV (“Maintain Closed Investigation”) Business Function, which allows the worker to correct errors in information in closed cases (such as adding a missing allegation).

Such Business Functions are designed to be given to specific types of workers (e.g., “Supervisor or above” or “only workers who are knowledgeable about the Person Unrelate process and its impacts”).

Business Function Profile (BFP)

A Business Function Profile (BFP) can be thought of as an outline of the parameters of a worker's CONNECTIONS access. The BFP is attached to the worker's logon ID and it is this profile that the system checks to determine which windows and functionalities the worker is permitted to access.

The Business Function Profile is the collection of all Business Functions assigned to the worker. The makeup of the BFP is tailored to the access a worker needs to perform casework responsibilities, rather than being based on a job title. For instance, a CPS worker's responsibilities require the ability to perform case and person searches and to view investigation stages. The Security Coordinator assigns the CASE/PERS SEARCH and VIEW UNDER INV Business Functions, which allow the worker to carry out those tasks. This system allows agencies to design BFPs to accommodate local practices and assignments of responsibilities. Any number of workers can have the same BFP. Similarly, a particular BFP can be unique to a single worker.

Some unit members (such as supervisors and Unit Approvers) have work responsibilities that involve more than the servicing of individual stages. Additional Business Functions are included in their respective BFPs to reflect this. Business Functions can be added to or removed from a worker's BFP as job responsibilities change. (See Module 7.) The BFP should be re-examined and adjusted (if necessary) when a worker moves to a new unit or is assigned new job responsibilities.



The Business Function Report is a valuable tool in managing Business Functions and their assignments. The report identifies all workers in an agency who have been assigned a particular Business Function. For more information about the Business Function Report, see page 82.

CONNECTIONS access is determined by the relationship between a worker's role in a stage (Primary, Secondary, Case Manager, Implied or Historical), the worker's role in the Unit and the worker's BFP. The View and/or Maintain access abilities granted by a particular Business Function will vary depending on whether the worker has a role in a particular stage and what that role is.

For example, the Business Function of VIEW UNDER INV will provide different types of access to a stage depending on a worker's role in that stage.

Differences in access provided by VIEW UNDER INV depending on worker role in stage	
Worker Role	Access to Case
Primary	View and Maintain access to entire case through <i>Assigned Workload</i> .
Secondary	Limited Maintain access. For example, cannot Save and Submit Investigation Conclusions and Fatality Reports.
None	Cannot access case at all.



The example on the previous page assumes the worker has *not* been assigned the ACCESS ALL DIST (“Access All in District”) Business Function. If the worker without a stage role in the above example was assigned the ACCESS ALL DIST Business Function, this would provide view access to the case through a case search.

Access to CPS stages in CONNECTIONS is based on a combination of various factors. In order to view CPS stages:

- the worker must have a role or implied role in the CPS stage; AND
- the worker must *not* be in a voluntary agency (only local district workers can access CPS Intake and Investigation stages).

In order to *print* information related to CPS stages, workers must have the appropriate Business Function(s): VIEW UNFOUNDED, VIEW INDICATED and VIEW UNDER INV.

Bundled Security Attributes

While CONNECTIONS security is designed to allow local Security Coordinators a great deal of flexibility in tailoring access to the needs of workers, there are certain Business Functions that any worker of a particular type will need. The table on the next page presents Bundled Security Attributes, one for each of four job types.

Bundled Security Attributes allow a Security Coordinator to assign a single Business Function that grants a particular type of worker the CONNECTIONS access needed to perform that job.

For example, a CPS worker needs to be able to conduct case and person searches and view investigation stages. The CPS WORKER Business Function includes the “Case Search,” “Person Search” and “View Under Investigation” Security Attributes.

Bundled Security Attributes are available for local districts *only*.

It is important to understand that what you are assigning is a single Business Function containing many Security Attributes. Think of bundled Security Attributes as a “package deal.” When you assign the CPS WORKER Business Function, the worker will automatically have all of the access abilities listed in the table. **If you do *not* wish the worker to have one or more of those abilities, do *not* assign the Business Function (since it is comprised of the bundled Security Attributes).** Instead, assign individual Business Functions until you have created the appropriate set for the worker.

Bundled Security Attributes Contained in Specific Business Functions			
CPS WORKER	FAD WORKER	CPS SUPERVISOR	FAD SUPERVISOR
Access All in District	Access All in District	Access All in District	Access All in District
Case Search	Case Search	Case Search	Case Search
Person Search	Person Search	Person Search	Person Search
View Admin Review	Maintain Closed Person Demographics	Maintain Designees	Maintain Closed Person Demographics
View Call Log	Maintain Home	Maintain Staff	Maintain Home
View Indicated	Maintain Resources	Maintain Unit	Maintain Home History
View Reporter/Source	View Contracts	Mark Sensitive Case	Maintain Resources
View Under Investigation		Case Merge/Split	Case Merge/Split
View Unfounded		Person Merge/Split	Person Merge/Split
		Unit Summary Access	Remove Person—Added in Error
		View Admin Review	Unit Summary Access
		View Call Log	View Contracts
		View Indicated	View Security
		View Reporter/Source	
		View Security	
		View Sensitive Case	
		View Under Investigation	
		View Unfounded	

Additional Business Functions can be added to these bundled Security Attributes to reflect a worker's responsibilities within your agency. The ways in which your agency is organized will determine who performs certain duties. For example, one district might have one or two designated workers who are authorized to perform Local Data Maintenance on closed cases and will assign the MAINT CLSD INV and/or MAINT CLSD PERS Business Functions accordingly. Another district may decide that any caseworker can perform Local Data Maintenance and assign those Business Functions as part of each worker's BFP.



Listings of all available Business Functions (organized as Security Profiles for each office type) are available in Appendix D.

Viewing Business Function Profiles

The VIEW SECURITY Business Function allows a worker to review BFPs in CONNECTIONS.



Step-by-Step: Viewing Business Function Profiles

- 1 Click on the **Options** menu on the CONNECTIONS Toolbar and select the **Security** command.
The Security sub-menu displays.
- 2 Click on the **View Staff Security** command.
The Staff Search Criteria window displays.
- 3 Type the worker's first and last names or Person ID into the appropriate fields.
- 4 Click on the **Search** button.
The Staff List displays.
- 5 Click on a name to select it from the *Staff List*.
- 6 Click on the **OK** button.
*The Staff Security window displays. The **Business Function** field on this window contains the Business Functions that have been assigned to the worker.*
- 7 The assigned Business Functions are identified with red check marks. Use the vertical scroll bar inside the **Business Function** list box to view the entire list.
- 8 To close the *Staff Security* window, click on the **Cancel** button.

Security Profile (SP)

Agencies that use CONNECTIONS are categorized into one of nine *office types* (State, Regional Office, District, Voluntary Agency, DFY, CCF, OMH, OMRDD, and CQC). Each office type has a set of Business Functions that are available for its workers. The list of all available Business Functions for a particular office type is its Security Profile. The Security Profile will vary for each office type.

For example, because local districts perform CPS Investigations, the Security Profile for that office type includes investigation-oriented Business Functions, such as VIEW UNDER INV and MAINT CLSD INV. These Business Functions do not appear in the security profile of office types that do not conduct CPS investigations, such as voluntary agencies.

See Appendix D for a complete listing of the Security Profiles for each office type.

Module 6: Adding Staff in CONNECTIONS

When a new worker joins an agency, it is the Security Coordinator's responsibility to ensure that the worker is provided with the security credentials that will allow the worker to fulfill casework responsibilities. This module provides instructions for accomplishing this task using the *Staff Security* window.

By the end of this module, you will be able to:

- assign a new worker to the appropriate unit within an agency;
- set up or modify Job Types for a worker;
- assign the appropriate Business Functions to that worker;
- see what attributes are associated with a Business Function; and
- make the worker "case assignable."

Overview

A Security Coordinator's responsibilities when a new worker joins an agency's staff can be broken down into three parts (each of these tasks is examined in detail in the sections that follow):

- The worker must be reassigned from the "default" unit to the unit appropriate for the worker's position.
- The appropriate Business Functions must be assigned to the worker.
- The worker must be informed of his/her Business Function Profile.

Assignment to New Unit

When a worker who is new to CONNECTIONS is first entered into the system by the LAN Administrator (through WEBSTAR), the worker is placed in a default unit; the numbered designation of all default units starts with "N." The creation of default units has implications for unit maintenance. (See page 60.) The default unit is a holding place until the Security Coordinator In-Assigns the worker to the required unit. (For more information on In/Out-assigning, see page 38.) Once the worker is assigned to the designated unit, s/he can be made Case Assignable; a worker cannot be Case Assignable in "N" units.



Step-by-Step: Assigning a New Worker to a Unit

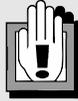
- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Maintain Unit window displays.
- 2 Click on the **Search** button.
Search results listing all units in your agency appear in the list.
- 3 Click to select the unit into which you want to move the worker, then click on the **Detail** button.
The Unit Detail window displays.
- 4 Click on the **Staff** button.
The Staff Search Criteria window displays.
- 5 Enter the name or Person ID of the worker you wish to add to the unit, then click on the **Search** button.
The Staff List displays with the search results.
- 6 Select the worker's name from the *Staff List*, then click on the **OK** button.
The Unit Detail window displays.
- 7 Click on the drop-down arrow for the **Role** field and select the worker's role from the resulting list.
- 8 Click on the drop-down arrow for the **In/Out** field and select **In** for In-Assigned. (For more information on In/Out-assigning, see page 38.)
- 9 Click on the **Modify** button.
- 10 Click on the **Save** button.



If you know the unit code for the unit to which you are assigning the worker, entering it in the **Unit** field will return search results for only that unit.



Supervisors should be In-Assigned to the unit they supervise.



When a worker receives an In-Assignment to a unit, CONNECTIONS automatically deletes the In-Assignment to the default unit (or whatever unit to which the worker was previously assigned) because a worker can only be In-Assigned to one unit at a time.

Staff Security Window

Security Coordinators use the *Staff Security* window to set up or modify an employee's Job Type, Assignees and Business Functions. A Security Coordinator must have the MAINT SECURITY Business Function assigned in order to *modify* the window; the VIEW SECURITY Business Function must be assigned in order to *view* the window.

The screenshot shows the 'Staff Security - Ballou, Wally' window. It has a menu bar with 'File', 'Edit', 'Options', and 'Help'. The 'Type' is set to 'District' and the 'Logon ID' is 'XX1234'. Under 'Organizational Hierarchy Access', there are two lists: 'Job Types' and 'Business Functions'. The 'Job Types' list includes ACCOUNTING CLERK, ACCOUNTING SUPERVISOR, ADMINISTRATIVE STAFF, ADOPTION CASEWORKER, and ADOPTION DIRECTOR. The 'Business Functions' list includes ACCESS ALL DIST (checked), APPROVE HP INV, CASE/PERS SRCH (checked), CPS CASEWORKER, CPS SUPERVISOR, and ENTER PROG NOTE. There are checkboxes for 'Selected Job Types Only' and 'Selected Business Funcs Only', and an 'Attributes...' button. The 'Assignees' section has a table with columns 'Employee Name' and 'Expiration Date'. Below the table are input fields for 'Employee Name' and 'Expiration Date' (with '11' entered), and buttons for 'Add', 'Delete', 'Modify', 'Clear', 'Staff...', 'Save', and 'Cancel'.

The existing CONNECTIONS security structure allows access to another worker's *Assigned Workload* based on unit hierarchy, rather than organizational hierarchy. Currently, a staff person who has a role in a unit as the Unit Approver (or has a role above the Unit Approver) who also has been assigned the UNIT SUM ACCESS Business Function can access (and update) all data for any case in that unit (subject to specialized access, such as sensitive cases). However, the roles currently available (Worker, Supervisor, Maintainer and Manager) do not correspond to the way most districts or agencies are organized, nor do they provide sufficient flexibility. In addition, Unit Summary Access security is not specific to a function, which can result in allowing an individual to have greater system access than may be necessary.

Three main factors currently determine a user's access to information in CONNECTIONS:

- Assignment of a Business Function Profile (BFP), which is composed of all Business Functions assigned to a particular worker
- Role in the case
- Role in the unit in conjunction with Unit Summary Access

Job Types

By assigning Job Types to the workers in a district/agency, the Security Coordinator can provide access that more closely mirrors the practical application of work in the field. A worker can be assigned one, several or no Job Types.

There are Job Types for each Office Type; these Job Types fall into two main categories: Clerical and Non-Clerical. (See Appendix E for a list of all Job Types and their corresponding categories.) Staff designated as Non-Clerical will have access to all units below their own, if this option is selected by their district/agency. If no Job Type is specified for a worker, the worker is classified by default with a Clerical Job Type.

Job Types should not be confused with Business Functions. While Security Coordinators use Job Types to determine Agency Access, Business Functions determine the access to windows available to a worker (i.e., which windows can be viewed/maintained for which stages). Assigning a Job Type to a worker does *not* affect that worker's BFP in any way.

For example, if caseworkers Jane Baker, Tom Cook and Sara Miller are all assigned the Job Type of "Child Preventive Caseworker," each worker can access the Family Services Stages (FSS) on the other's *Assigned Workload*. This requires all of them to have the same Job Type and the same option selected on the *Agency Access* window. Let's look at the ability of these three workers to view a Sensitive Case:

1. Jane has the VIEW SENSITIVE Business Function; however, even though she is not currently assigned to a Sensitive Case, she can view the details of another worker's Sensitive Case.
2. Tom is not assigned the VIEW SENSITIVE Business Function, so he cannot view the details of another worker's Sensitive Case.
3. Sara is assigned to a Sensitive Case; even though she is not assigned the VIEW SENSITIVE Business Function, she can view and access the case because she has a role in that case.

A Security Coordinator's BFP must include the MAINT SECURITY Business Function in order to assign Job Types to workers.

When a Security Coordinator opens the *Staff Security* window for a particular worker, only the Job Types *available* for that worker's Office Type will display on the list in the **Job Types** field. To select a Job Type, simply double-click it; a check mark will display to the left of the Job Type to indicate that it has been selected. Multiple Job Types may be selected for an individual employee. To deselect a Job Type, double-click it again to remove its corresponding check mark. Remember, it is not required that a worker be assigned a Job Type.

Selected Job Types Only Check Box

The **Selected Job Types Only** check box displays below the **Job Types** field. Click on this check box to display only the Job Types that have been selected for a worker, rather than having to scroll through the entire list of available Job Types. A check mark will display in the check box to indicate that it has been selected. To deselect this check box, click on it again; all available Job Types will display on the list.

Assignment of Appropriate Business Functions

When a new worker is first added to the CONNECTIONS system, the agency LAN Administrator gives the worker “standard” access, allowing access to only some of the functions on the CONNECTIONS Toolbar. All buttons on the Toolbar granting access to CONNECTIONS client data are disabled. It is the Security Coordinator’s responsibility to assign the additional Business Functions that will allow workers to complete their responsibilities in CONNECTIONS.

Consult with the worker’s supervisor to determine what Business Functions the worker will need. (See Appendix F for details regarding the Business Functions introduced in Build 17.)

In the **Business Functions** field, the list displays only the Business Functions *available* for that worker’s Office Type. Double-click a Business Function to select it; a check mark will display to the left of the Business Function to indicate that it has been selected. Multiple Business Functions may be selected for an individual employee. To deselect a Business Function, double-click it again to remove its corresponding check mark.

Selected Business Functions Only Check Box

The **Selected Business Functions Only** check box displays below the **Business Functions** field. Click on this check box to display only the Business Functions that have been selected for a worker, rather than having to scroll through the entire list of available Business Functions. A check mark will display in the check box to indicate that it has been selected. To deselect this check box, click on it again; all available Business Functions for that worker’s Office Type will then display on the list.

Attributes Button

Business Functions are comprised of one or more Security Attributes, which are created (and connected to specific Business Functions) by state staff. To see the Security Attribute(s) contained in a particular Business Function, select the Business Function from the list and click on the **Attributes...** button to open the *Security Attributes* window.

System Edits on the Staff Security Window

The following rules apply when viewing the **Business Functions** field on the *Staff Security* window:

- The VIEW ORG HIER and VIEW AGY ACC Business Functions will work the same as any other Business Function; therefore, they can be viewed and assigned by anyone with the MAINT SECURITY Business Function, or viewed by anyone with the VIEW SECURITY Business Function for anyone in that person’s agency.
- Only OCFS CONNECTIONS staff can be assigned the ASSIGN ACC/HIER Business Function.
- Only OCFS CONNECTIONS staff who have the ASSIGN ACC/HIER Business Function can assign the MAINT ORG HIER or MAINT AGY ACC Business Functions.
- Only staff persons who have the MAINT ORG HIER Business Function *and* have access to the *Staff Security* window will see MAINT ORG HIER in the list of Business Functions for themselves and others who have been assigned that Business Function.

Only staff persons who have the MAINT AGY ACC Business Function *and* have access to the *Staff Security* window will see MAINT AGY ACC on the list of Business Functions for themselves and others who have been assigned that Business Function.



Step-by-Step: Viewing Job Types and Business Functions for a Worker

- 1 On the CONNECTIONS Toolbar, click on the **Options** menu and select **Security**.
The Security sub-menu displays.
- 2 Click on the **View Staff Security...** command.
The Staff Search Criteria window displays.
- 3 Enter the staff person's name or Person ID, then click on the **Search** button.
The Staff List displays with the search results.
- 4 Select the correct staff person from the *Staff List*, then click on the **OK** button.
The Staff Security window displays in view only mode.
- 5 Click the **Selected Job Types Only** check box.
The Job Types field displays only the Job Types assigned to the worker.
- 6 Click the **Selected Business Functions Only** check box.
The Business Functions field displays only the Business Functions assigned to the worker.



If a check mark displays next to a Business Function in the **Business Functions** list box on the *Staff Security* window, that Business Function has been assigned to the worker.



Step-by-Step: Modifying Job Types and Business Functions for a Worker

- 1 On the CONNECTIONS Toolbar, click on the **Maintain** menu and select the **Staff Security...** command.
The Staff Search Criteria window displays.
- 2 Enter the staff person's name, then click on the **Search** button.
The Staff List displays with the search results.
- 3 Select the correct staff person from the *Staff List*, then click on the **OK** button.
The Staff Security window displays in modify mode.
- 4 Double-click the **Job Types** and/or **Business Functions** you need to add or delete.
- 5 Click on the **Save** button.

Notifying Workers of Newly Assigned Business Functions

Workers need to be notified when new Business Functions have been assigned to them, what those Business Functions are, what tasks they can accomplish in CONNECTIONS, and what viewing and maintaining rights these Business Functions grant to them. Your agency can determine the most effective way to do this: via e-mail, memo, or face-to-face meeting.

Making a Worker Case Assignable

When first entered into CONNECTIONS, a worker is not “case assignable.” In other words, no stages can be assigned to that worker. Marking a worker as case assignable can be performed by any worker with the MAINTAIN STAFF Business Function (usually the Security Coordinator). The point at which the Security Coordinator is asked to make a worker case assignable may vary depending on the worker’s training and job responsibilities. Avoid leaving sensitive or confidential messages on voicemail systems, to notify the worker that s/he is now Case Assignable. Additionally, CONNECTIONS workers should not use the Internet or e-mail for any reason that could compromise security.



Step-by-Step: Making a Worker Case Assignable

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the new worker and click on the **Search** button.
The Staff List displays.
- 3 Select the worker from the *Staff List* and click on the **Detail** button.
The Staff Detail window displays.
- 4 Click on the **Case Assignable** check box.
A check mark displays in the check box.
- 5 Click on the **Save** button.
The Staff Detail window closes.
- 6 Click on the **Close** button.
The Staff List closes.
- 7 Click on the **Close** button.
The Staff Search Criteria window closes.

Module 7: Maintaining Staff in CONNECTIONS

As worker responsibilities, staff makeup and system functionality change, the Security Coordinator must perform various functions to ensure that all workers have appropriate access to CONNECTIONS. This module provides instructions for accomplishing these tasks.

By the end of this module, you will be able to:

- use the In/Out-Assignment function to assign workers correctly;
- assign additional Business Functions to a worker;
- remove Business Functions from a worker's Business Function Profile;
- explain the concept of *designees* and how to assign and remove them;
- change a unit's Unit Approver;
- transfer workers between units;
- move workers between agencies;
- end-date and reinstate staff in CONNECTIONS;
- list the tasks required of a Security Coordinator when a CONNECTIONS system build includes new Business Functions; and
- transfer Security Coordinator responsibilities.



The Staff Security Report is a valuable tool in tracking workers' security characteristics while performing any of the tasks listed in this module. The report allows you to see which agency staff members are in CONNECTIONS, what Business Functions have been assigned to each staff member, whether a staff member is a Unit Approver, and whether a staff member is an Assignee or Designee. For more information about the Staff Security Report, see page 80.

In/Out-Assigning

When a worker is assigned to a unit, the assignment must take the form of an In-Assignment or an Out-Assignment.

- An *In-Assignment* is the formal placement of a worker into the primary unit where that person works.
- An *Out-Assignment* is the assignment of a worker to a unit *in addition* to the unit into which that worker has been in-assigned. An out-assigned worker does work for the out-assigned unit, but this unit is not the primary unit to which the worker is assigned. There is no time limit on an Out-Assignment, nor is there any limit to the number of Out-Assignments a worker can have.



Each worker is In-assigned to only one unit. Supervisors should be In-Assigned to the unit they supervise.

Possible uses of out-assigning are:

- To allow a worker to receive assignments more easily from a unit other than the in-assigned unit. (An out-assigned worker can be assigned a stage from the unit list without the necessity of conducting a staff search from the *Assign* window.)
- To allow a supervisor to serve as a back-up for another supervisor (when also given a role in that unit higher than the Unit Approver).
- To allow someone who is not officially part of the unit (e.g., Director of Services) to review or approve work for the unit.

An In-Assignment is made as part of adding a new worker to a unit (see Module 6) or transferring a worker to a new unit (see page 46). Therefore, the steps for in-assigning are listed as part of the step-by-step descriptions for those processes.

You cannot add staff to Conversion Units with the Conversion Person (PID 18012) as the Unit Approver, the **Staff** button is disabled.



Step-by-Step: Out-Assigning a Worker

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Maintain Unit window displays.
- 2 Click on the **Search** button.
Search results listing all units appear in the list box.
- 3 Select the unit **to which you want to out-assign the worker** and click on the **Detail** button.
The Unit Detail window displays.
- 4 Click on the **Staff** button.
The Staff Search Criteria window displays.
- 5 Enter the name or Person ID of the worker you wish to out-assign to the unit and click on the **Search** button.
The Staff List displays with the results of the search.



If you know the unit code for the unit **to which you are assigning the worker**, entering it in the **Unit** field will return search results for only that unit.

- 6 Select the worker's name from the *Staff List*, then click on the **OK** button.
The Unit Detail window displays.
- 7 Click on the drop-down arrow for the **Role** field and select the worker's role from the resulting list.
- 8 Click on the drop-down arrow for the **In/Out** field and select **Out** for Out-Assigned.
- 9 Click on the **Modify** button.
- 10 Click on the **Save** button.



Be sure to select **Out-Assign**.
If you select In-Assign, the worker will be removed from the Primary unit.

Assigning Additional Business Functions

Workers' BFPs need to be adjusted as new Business Functions are added to the CONNECTIONS system or as workers' responsibilities change. For example, if a caseworker was assigned to perform Local Data Maintenance for a unit, the Security Coordinator would add the MAINT CLSD INV and/or MAINT CLSD PERS Business Functions to the worker's BFP.

Business Functions are added to a worker's BFP on the *Staff Security* window.



When a worker's Business Function Profile is altered, changes do not take effect until the next time the worker logs onto CONNECTIONS.

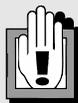


Step-by-Step: Assigning Additional Business Functions

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff Security** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the worker and click on the **Search** button.
The Staff List displays with the search results.
- 3 Select the worker's name from the *Staff List*, then click on the **OK** button.
The Staff Security window displays in modify mode.
- 4 Scroll through the **Business Functions** field, double-clicking the Business Functions you wish to assign to the worker.
A check mark displays to the left of each Business Function you select.
- 5 Click on the **Save** button.



If a check mark displays to the left of a Business Function in the **Business Functions** field on the *Staff Security* window, that Business Function has already been assigned to the worker.



Remember to notify the worker of the Business Function Profile change and how the BFP affects access in CONNECTIONS.

Removing Business Functions from a BFP

Another way in which Business Function Profiles need to be adjusted is the removal of Business Functions that are no longer relevant to the worker's responsibilities. Business Functions are removed from a worker's Business Function Profile on the *Staff Security* window.



When a worker's Business Function Profile is altered, changes do not take effect until the next time the worker logs into CONNECTIONS.



Step-by-Step: Removing Business Functions from a BFP

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff Security** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the worker and click on the **Search** button.
The Staff List displays with the search results.
- 3 Select the worker's name from the *Staff List*, then click on the **OK** button.
The Staff Security window displays.
- 4 Scroll through the **Business Functions** field and double-clicking the Business Functions you wish to *remove* from the worker's BFP.
Check marks are removed from the Business Functions as you double-click them.
- 5 Click on the **Save** button.



If no check mark displays next to a Business Function in the **Business Functions** field, that Business Function has not been assigned to the worker.



Remember to notify the worker of the Business Function Profile change and how the BFP affects access in CONNECTIONS.

Designees

There are situations, such as during vacations, in which a worker needs to have another worker cover his/her responsibilities. CONNECTIONS allows workers to assign their own security rights, including Business Functions, to another worker for a specified amount of time.

Workers who temporarily assign their own security rights to another worker are called Assignees. A worker who is temporarily assigned the security rights of another worker is known as that worker's Designee.



There are three ways to verify designee assignments:

- Workers with the MAINT DESIGNEES Business Function can check the *Maintain Designee* window.
- Security Coordinators (or any staff with the MAINT SECURITY or VIEW SECURITY Business Functions) can check the *Staff Security* window.
- The Assignee/Designee Report identifies which workers are assignees or designees of another worker. For more information about the Assignee/Designee Report, see page 83.

A Designee assumes all access rights of the Assignee. A Designee assigned the Business Function UNIT SUM ACCESS (whether assigned to themselves or through being a designee) gains the ability to access the Assignee's *Assigned Workload* and can perform work as s/he were the Assignee. In essence, the Designee becomes the Assignee (from an access standpoint).

When the Designee is a worker in the same district as the Assignee *and* has the UNIT SUM ACCESS Business Function, the Designee can access the same workloads as the Assignee and has the same approval authority on tasks. If the Assignee is a Unit Approver, the Designee gains access to all workloads within the Assignee's unit.

There are two ways to create a designee assignment:

- Workers who have been assigned the MAINT DESIGNEES Business Function can make their own designee assignments on the *Maintain Designees* window. The Security Coordinator (or any staff with the MAINT SECURITY Business Function) can assign the MAINT DESIGNEES Business Function to any worker who needs it.
- Workers with the MAINT SECURITY Business Function (often the Security Coordinator) can assign an assignee to a worker (making that worker a designee) on the *Staff Security* window.



Step-by-Step: Assigning a Designee via the *Maintain Designees* Window

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Maintain Designees** command.
The Maintain Designees window displays.
- 2 Click on the **Staff** button.
The Staff Search Criteria window displays.
- 3 Enter the name or Person ID of the worker to be made a designee and click on the **Search** button.
The Staff List displays with the search results.
- 4 Select the name of the worker to be made a designee from the *Staff List*, then click on the **OK** button.
The Staff Security window displays for the selected worker.
- 5 Enter the expiration date of the assignment in the **Expiration Date** field, then click on the **Add** button.
The designee's name displays in the list section.
- 6 Click on the **Save** button.



Step-by-Step: Assigning a Designee via the *Staff Security* Window

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff Security** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the worker **to be made a designee**, then click on the **Search** button.
The Staff List displays with the search results.
- 3 Select the name of the worker **to be made a designee** from the *Staff List*, then click on the **OK** button.
The Staff Security window displays for the selected worker.
- 4 Click on the **Staff** button in the Assignees section of the *Staff Security* window.
The Staff Search Criteria window displays.
- 5 Enter the name or Person ID of the worker who is going to be the Assignee for the worker for whom you previously searched. Click on the **Search** button.
The Staff List displays with the search results.
- 6 On the *Staff List*, select the name of the worker to be made an assignee, then click on the **OK** button.
*The Staff Security window displays for the designee, with the Assignee's name displayed in the **Employee Name** field.*
- 7 Enter the expiration date of the assignment in the **Expiration Date** field, then click on the **Add** button.
The designee's name displays in the list.
- 8 Click on the **Save** button.

One common use of assigning a Designee is to add the ability to perform approvals. When a Designee has been assigned, Approval To-Do's are still sent to the Assignee. If the Designee is in the unit hierarchy of the Assignee's unit and is either the Unit Approver or above *and* assigned the UNIT SUM ACCESS Business Function, the Designee can access the Assignee's To-Do list. The designee must check the Assignee's *Staff To-Do List* for these To-Dos. A worker can submit the approval to the Designee, who can then approve it themselves and an alert is sent to the approver that this was completed. The Designee will not be able to approve the closing of a FSS stage if the Assignee is the Unit Approver UNLESS that Designee is the Unit Approver's supervisor.

Please keep in mind that all information that is created, acquired or used in the support of CONNECTIONS business activities should only be used for those specific purposes.



Step-by-Step: Performing Approvals as a Designee

- 1 Click on the **UNIT** button on the CONNECTIONS Toolbar.
The Unit Summary window displays.
- 2 Enter the **Site** and **Unit** of the assignee.
- 3 Click on the **Search** button.
Search results appear in the list section of the Unit Summary window.
- 4 Click on the name of the assignee to select it from the results list.
*The **To-Do** button enables.*
- 5 Click on the **To-Do** button on the *Unit Summary* window.
The assignee's Staff To-Do List displays.
- 6 Click to select the approval task.
*The task highlights and the **Navigate** button enables.*
- 7 Click on the **Navigate** button.
*The appropriate window displays for review of the submission.
The specific window(s) that displays for review will vary depending on the type of approval.*
- 8 After reviewing the submission, close all review windows.
The Approval Status window displays with the assignee listed as approver in the list section.
- 9 Select the assignee in the list section.
The assignee's name highlights and the designee's name displays in the Approval Information section of the window as the person performing the approval.
- 10 Click on the **Approve** button.
*The following message displays:
"Approval completion will freeze Events. Do you wish to add another approver?"*
- 11 Click on **Yes** the button to assign another approver.
—OR—
Click on the **No** button if you do *not* want to assign another approver.
- 12 Click on the **Save** button on the *Approval Status* window.

Both the *Maintain Designees* and *Staff Security* window can be used to remove a designee. The *Maintain Designees* window is used by an assignee to cancel a designee assignment previously made.



Step-by-Step: Canceling a Designee Assignment via the *Maintain Designees* Window

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Designees** command.
The Maintain Designees window displays.
- 2 In the list section, select the name of the designee to be removed, then click on the **Delete** button.
The following message displays: "Are you sure you want to delete this record?"
- 3 Click on the **Yes** button.
The designee's name is removed from the list section.
- 4 Click on the **Save** button.

The *Staff Security* window can be used by the Security Coordinator (or anyone with the MAINT SECURITY Business Function) to cancel a designee assignment.



Step-by-Step: Canceling a Designee Assignment via the *Staff Security* Window

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff Security** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the **designee**, then click on the **Search** button.
The Staff List displays.
- 3 Select the name of the **designee** from the *Staff List*, then click on the **OK** button.
The Staff Security window displays for the selected worker. The name of the assignee displays in the Assignees list section.
- 4 Select the assignee.
The worker's name highlights.
- 5 Click on the **Delete** button.
The following message displays: "Are you sure you want to delete this record?"
- 6 Click on the **Yes** button.
The Assignee is removed, thereby canceling the designee's assignment.
- 7 Click on the **Save** button.

Changing the Unit Approver

The Unit Approver (usually the unit supervisor) reviews and approves (or rejects) all work completed and submitted by workers in the unit.

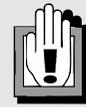
Each unit has one and only one approver. If this worker leaves the unit (e.g., transfers or retires), the Security Coordinator must assign a new Unit Approver *before* the previous Unit Approver is end-dated or removed from the unit.

There are actually two phases to this process: removing the previous Unit Approver and assigning the new Unit Approver.



Step-by-Step: Changing the Unit Approver

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Unit List displays.
- 2 Enter the Unit number in the **Unit** field, then click on the **Search** button.
Search results appear in the list box.
- 3 Select the unit from the list and click on the **Detail** button.
The Unit Detail window displays. The list contains the names of all unit members. There is a check mark to the left of the Unit Approver's name.
- 4 Select the current Unit Approver and deselect the **Unit Approver** check box.
*The check mark in the **Unit Approver** check box is removed.*
- 5 Click on the **Modify** button.
The check mark next to the current Unit Approver's name is removed.
- 6 Select the unit member to be assigned as the new Unit Approver and click on the **Unit Approver** check box.
*A check mark displays in the **Unit Approver** check box.*
- 7 If the worker's role needs to be modified, click on the drop-down arrow for the **Role** field and select the appropriate role from the resulting list.
- 8 Click on the **Modify** button.
A check mark displays next to the new Unit Approver's name. If a new role was selected, the worker's role changes.
- 9 Click on the **Save** button.
The Unit List displays.
- 10 Click on the **Close** button.



Workers with an assignment of Unit Approver must be removed as Unit Approver before they can be end-dated.



The Unit Approver Report identifies the Unit Approver for any unit in your agency. For more information about the Unit Approver Report, see page 84.

Transferring Workers

On occasion, workers will move into a position with a new unit in their current agency. In these situations, the worker must be transferred from the old unit to the new unit. A worker's *Assigned Workload* transfers with the worker to the new unit.



Step-by-Step: Transferring a Worker Within an Agency

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Maintain Unit window displays.
- 2 Click on the **Search** button.
The Unit List displays with the search results.
- 3 Select the unit into which you want to transfer the worker, then click on the **Detail** button.
The Unit Detail window displays.
- 4 Click the **Staff** button.
The Staff Search Criteria window displays.
- 5 Enter the name or Person ID of the worker you wish to transfer into the unit, then click on the **Search** button.
The Staff List displays with the search results.
- 6 Select the worker's name from the search results list and click **OK**.
The Unit Detail window displays.
- 7 Click on the drop-down arrow for the **Role** field and select the worker's role from the resulting list.
- 8 Click on the drop-down arrow for the **In/Out** field and select **In** for In-Assigned. (For more information on In/Out-assigning, see page 38.)
- 9 Click on the **Modify** button.
- 10 Click on the **Save** button.



When a worker receives an In-Assignment to a unit as a result of a transfer, CONNECTIONS automatically deletes the In-Assignment in the previous unit because a worker can only be In-Assigned to one unit at a time.

Moving Workers Between Agencies

Moving a worker between agencies is a three-step process.

In the agency the worker is leaving:

1. It is the responsibility of the Security Coordinator in the moving worker's old agency to end-date the worker in that unit (see "End-Dating Staff" on page 47.)

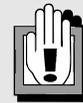
In the agency the worker is joining:

1. The new agency's local LAN administrator must request through WEBSTAR that the worker be given a new NT logon ID. The LAN administrator then assigns the worker "standard" CONNECTIONS access.
2. The Security Coordinator in the moving worker's new agency adds the worker to the new unit.

This process includes:

- assigning the worker to the new unit;
- assigning appropriate Business Functions; and
- notifying the worker of the new BFP.

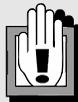
For detailed instructions on these steps, see Module 6: Adding Staff in CONNECTIONS.



When a worker receives an In-Assignment to a unit CONNECTIONS automatically deletes the In-Assignment to the temporary unit because a worker can only be In-Assigned to one unit at a time.

End-Dating Staff

When a worker leaves an agency (either temporarily or permanently), it is the Security Coordinator's responsibility to remove that worker's CONNECTIONS access by disabling the CONNECTIONS Person ID. This is accomplished by end-dating the Person ID on the *Maintain Staff* window.



A worker with an assignment of Unit Approver must be removed as Unit Approver before that worker can be end-dated.

- A worker's *Assigned Workload* and *Staff To-Do List* must be empty before the worker can be end-dated.
- It is important that workers are end-dated **before** their Person ID is disabled or before they are deleted from the system through WEBSTAR, since disabling the Person ID through WEBSTAR eliminates access to the *Assigned Workload*.



Step-by-Step: End-Dating Staff

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Enter the name or Person ID of the worker to be end-dated, then click on the **Search** button.
The Staff List displays with the search results.
- 3 Select the worker to be end-dated, then click on the **Detail** button.
The Staff Detail window displays.
- 4 Enter the current date in the **End Date** field, then click the **Save** button.
- 5 You can see that the worker has been end-dated if you conduct a staff search on the worker's name. The worker's name will not appear.

Removing Inactive Staff from a Unit

Sometimes when workers have been end-dated, their names still display on the *Unit List*. This can lead to confusion while maintaining security later on. The following instructions describe how to check whether an inactive worker has actually been removed from the unit and, if not, how to remove the worker.



Step-by-Step: Verifying that End-Dated Staff Have Been Removed from the Unit

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Click on the **Inactive** check box.
*A check displays in the **Inactive** check box and the **Last Name** field highlights in yellow, indicating that it is required.*
- 3 Enter the last name or Person ID of the worker in question, then click on the **Search** button.
The Staff List displays the search results.
- 4 Look for the worker on the *Staff List*.
*If there are entries in the **Unit** and **Unit Site** columns, the worker has **not** been removed from the unit.*



You can also see if a worker has been removed from the unit by checking the worker's old unit through the **Maintain Unit** function.



Step-by-Step: Removing an Inactive Worker from the Unit

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Click on the **Inactive** check box.
*A check mark displays in the **Inactive** check box and the **Last Name** field highlights in yellow, indicating that it is required.*
- 3 Enter the last name or Person ID of the worker in question, then click on the **Search** button.
The Staff List displays with the search results.
- 4 Select the worker in question on the *Staff List*, then click on the **Detail** button.
The Staff Detail window displays.
- 5 Click on either of the arrows next to the **End-Date** field to change the date.
The date displays in red.
- 6 Click on the opposite arrow to return the **End-Date** field to its original date.
*The **Save** button enables.*
- 7 Click on the **Save** button.
- 8 If you conduct another “inactive” search for the end-dated worker, you will find that the worker no longer has entries for **Unit** or **Unit Site** in the search results list.

Removing Assignments from a Workload

Since it is not possible to end-date a worker until his/her *Assigned Workload* has been cleared, it is important to be familiar with the process of re-assigning stages from one worker to another. Even though it is not strictly a security issue, it sometimes falls to the Security Coordinator to clear an *Assigned Workload* by re-assigning stages.



Step-by-Step: Reassigning Stages from the *Assigned Workload*

- 1 Click on the **UNIT** button on the CONNECTIONS Toolbar.
*The Unit Summary window displays. The **Unit** field pre-fills with your unit number. If the worker whose Assigned Workload you are clearing works in a different unit, enter that unit's number in the **Unit** field.*
- 2 Click on the **Search** button.
The Unit List displays with the search results.
- 3 Select the name of the worker whose *Assigned Workload* you want to access.
*The **Workload** button enables.*
- 4 Click on the **Workload** button.
The Assigned Workload displays for the selected worker.
- 5 Select the stage you wish to re-assign.
*The **Assign** button enables.*
- 6 Click on the **Assign** button.
The Assign window displays.
- 7 Select the name of the worker to whom you wish to re-assign the stage.
*The worker's name highlights and the **Primary** and **Secondary** button are enabled.*
- 8 Click on the appropriate assignment button.
*If you click on the **Primary** button, a confirmation message displays; click on the **Yes** button to confirm the reassignment.*
- 9 Click on the **Save** button on the Assign window.
The Unit Detail window displays.
- 10 Click on the **Close** button.
The Unit Summary window displays.
- 11 Click on the **Close** button.
The Unit Summary window closes.



You can assign a stage to a worker whose name does not display on the *Unit List* by using the *Assign* window. Conduct a staff search from the *Assign* window by clicking on the **Options** menu and selecting the **Staff Search Criteria** command. Searching for the worker and selecting the worker's name from the *Staff List* will display the worker's name in the *Assign* window's Available Staff section.

Reinstating Staff

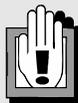
There are instances in which a worker whose Person ID was end-dated returns to work in the unit or agency. In such an instance, it is the responsibility of the Security Coordinator to reinstate the worker by removing the end-date on the *Maintain Staff* window, which restores the worker in CONNECTIONS.

A worker's Business Functions, Case Assignability and Job Type(s) are removed when s/he is end-dated. There should be a conscious decision on the part of the Security Coordinator regarding the Business Functions and Job Type(s) that should be assigned to the worker, as well as whether case assignability should be granted.



Step-by-Step: Reinstating Staff

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Click on the **Inactive** check box.
*A check displays in the **Inactive** check box and the **Last Name** field highlights, indicating that it is required.*
- 3 Enter the last name or Person ID of the worker in question and click on the **Search** button.
The Staff List displays with the search results.
- 4 Select the worker in question on the *Staff List*, then click on the **Detail** button.
The Staff Detail window displays.
- 5 Clear the end-date from the **End-Date** field.
*The **Unit Site**, **Unit**, **Role** and **Office Site** fields highlight to indicate that they are required.*
- 6 Enter the required information: **Unit Site**, **Unit**, **Role** and **Office Site**.
*The **Validate** button enables.*
- 7 Click on the **Validate** button.
Unit information (Supervisor's Name, Office Name and Unit Specialization) displays on the window.
- 8 Click on the **Save** button.
The Staff List displays.
- 9 Click on the **Close** button.
The Staff Search Criteria window displays.
- 10 Click on the **Close** button.



Once the end-date has been removed, the Security Coordinator must notify OCFS CONNECTIONS staff that the reinstated worker's NT logon must be re-entered in CONNECTIONS.

Security Coordinator Responsibilities When a System Build Includes New Business Functions

OCFS CONNECTIONS staff are continually working to improve and update the functionality and features of the CONNECTIONS system. Rather than release these changes one at a time, they are bundled together and released at intervals as “system builds.” Often, new or modified functionality introduces new security considerations requiring new Business Functions. The Security Coordinator’s responsibility in this case is four-fold:

1. Reference the security update information for the build. This information is made available in various forms. If the build includes additions or changes to Business Functions, OCFS staff will send a set of Business Function Guidelines to Implementation Coordinators and Security Coordinators. Release Notes outlining the changes included in the build are also sent. Both of these documents are also made available on the OCFS CONNECTIONS intranet site.
2. Determine who in the agency requires the new Business Functions. After reviewing the new Business Functions and their purposes, review agency information to determine which workers need the new Business Functions. The various security reports and meetings with unit supervisors are both good starting points for gathering this information.
3. Assign new Business Functions to appropriate staff. (See “Assigning Additional Business Functions” on page 39.)
4. Be sure to notify affected staff of their new Business Functions, the tasks the new Business Functions enable them to accomplish, and their new viewing and maintaining rights.

Transferring Security Coordinator Responsibilities

If an agency’s Security Coordinator leaves the agency, Security Coordinator responsibilities must be transferred to a new Security Coordinator. This is a two-step process:

1. Establish the new Security Coordinator.
2. Remove the old Security Coordinator.

Establishing the New Security Coordinator

The unit’s outgoing Security Coordinator establishes the new Security Coordinator using the processes with which you’re already familiar.

- If the new Security Coordinator is transferring from another *unit* within the agency, the new Security Coordinator can be treated as a transferring worker. (See “Transferring a Worker Within an Agency” on page 46.)
- If the new Security Coordinator is *moving from another agency*, the Security Coordinator must be added to the new agency as a new worker through WEBSTAR. This gives the worker an NT logon ID and “standard” CONNECTIONS (Toolbar) access. The Security Coordinator can then be assigned the appropriate Business Functions. (See “When a Worker Moves Between Agencies” on page 47.)

Once the new Security Coordinator has been established, the CONNECTIONS Communications Team must be notified. (See the OCFS CONNECTIONS intranet site's Security page for details.)

If there is no existing Security Coordinator or backup Security Coordinator who can establish a new Security Coordinator, OCFS CONNECTIONS staff will assist in assigning security maintenance abilities to a new Security Coordinator. To avoid such a situation, the new Security Coordinator should assign a backup Security Coordinator as soon as possible.

Removing the Old Security Coordinator

Once the new Security Coordinator has been established, the old Security Coordinator can be removed. There are three possible scenarios in this situation, all of which use the processes with which you're already familiar.

For the purposes of these examples, assume the following:

Jerry = Old Security Coordinator in Agency X

Phil = New Security Coordinator in Agency X

Donna = Security Coordinator in Agency Z (Jerry's new agency)

- A. In the first scenario, Jerry is staying in his present unit but is no longer the agency's Security Coordinator:
 - 1) Phil simply removes the Security Coordinator Business Functions from Jerry's BFP. (See "Removing Business Functions from a Business Function Profile" on page 40.)
 - 2) Phil assigns Jerry the Business Functions he'll need in his new position. (See "Assigning Additional Business Functions" on page 39.)
- B. In the second scenario, Jerry is transferring to a new unit within the same agency and is no longer the agency's Security Coordinator:
 - 1) Phil removes the Security Coordinator Business Functions from Jerry's BFP. (See "Removing Business Functions from a Business Function Profile" on page 40.)
 - 2) Phil then moves Jerry into the new unit and assigns him the Business Functions he'll need in his new position. (See "Transferring a Worker Within an Agency" on page 46.)
- C. In the last scenario, Jerry is moving to a new agency:
 - 1) Phil end-dates Jerry. (See "End-Dating Staff" on page 47.)
 - 2) Phil disables Jerry's NT account (or notifies the unit's LAN administrator of the need to do so).
 - 3) After Jerry has received a new NT logon ID for Agency Z and standard CONNECTIONS access, Donna moves Jerry into his new unit and assigns him the Business Functions he'll need in his new position. (See "When a Worker Moves Between Agencies" on page 47.)

Updating Staff Names

There will be situations in which a worker's name needs to be updated in CONNECTIONS. Perhaps the worker got married and took her spouse's name. The name might have been misspelled or entered as all uppercase letters. If a worker's name was entered using all uppercase letters, this makes subsequent searches on that name more difficult because searching on the worker's full name will return no results for that name. Such names will appear at the *beginning* of the list of names starting with that first letter, rather than in true alphabetical order, but *only* if the search is conducted on only the first letter of the worker's name. (SMITH will appear before Samson in the results of a search – see the example below.)

Results of a search for "S" when a worker's name was entered as all uppercase:

SMITH, ARNOLD

Samson, Delilah

Seaborn, Samuel

Smithers, Waylon



Step-by-Step: Updating Staff Names

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Staff** command.
The Staff Search Criteria window displays.
- 2 Enter the last name of the worker whose name you are updating and click on the **Search** button.
The Staff List displays with the search results.
- 3 On the *Staff List*, select the worker whose name you are updating, then click on the **Detail** button.
The Staff Detail window displays.
- 4 Modify the name as necessary.
- 5 Click on the **Save** button.
The Staff List displays.
- 6 Click on the **Close** button.
The Staff Search Criteria window displays.
- 7 Click on the **Close** button.

Module 8: Unit Maintenance in CONNECTIONS

Many of the forms of security maintenance described in previous modules result in changes being made to the makeup of units within an agency. In some cases, these changes might result in the agency's unit structure in CONNECTIONS no longer accurately reflecting the way work actually gets done in the agency. In order to make it easier to keep track of workers, unit approvers, and the agency's organization, the Security Coordinator performs maintenance on the units themselves. In this module, you will learn how to perform that maintenance.

By the end of this module, you will be able to:

- create a unit in CONNECTIONS;
- change a unit's specialization;
- delete a unit in CONNECTIONS;
- provide access privileges using the *Agency Access* window; and
- create organizational hierarchy.

Creating a Unit

The *Unit Detail* window is used to create new units within an agency/district. The **Supervisory Unit** field on this window is a protected field. This field on the *Unit Detail* window displays the supervisory unit information recorded on the *Organizational Hierarchy* window. The information in this field can only be modified via the *Organizational Hierarchy* window.

To open the *Unit Detail* window in modify mode, click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command. When the window opens, both the **Unit** field and the **Supervisory Unit** field are pre-populated after Organizational Hierarchy has been created. The **Supervisory Unit** field is protected to prevent modifications to Supervisory Unit data. The *Organizational Hierarchy* window uses the information in these fields to display the organizational hierarchy. All modifications to the Supervisory Unit must be done through the *Organizational Hierarchy* window.

Name	Role	In/Out
------	------	--------

There will be instances in which a Security Coordinator needs to create a new unit within the agency. Perhaps a district is adding a second CPS unit or an agency is starting a new Transitional Care unit.



Step-by-Step: Creating a New Unit in CONNECTIONS

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Unit List window displays with Agency information pre-filled.
- 2 Enter the Site information for the new unit in the **Site** field.
- 3 Click on the **New** button.
The New Unit Detail window displays.
- 4 In the **Unit** field, enter the Unit number for the new unit.
- 5 **FOR ACS UNITS ONLY:** Click on the drop-down arrow for the **Zone** field and select the appropriate zone from the resulting list.
- 6 Click on the drop-down arrow for the **Unit Specialization** field and select the appropriate Unit Specialization from the resulting list.

- 7** Click on the **Staff** button.
The Staff Search Criteria window displays.
- 8** Enter the name or person ID of the worker whom you wish to assign to the unit, then click on the **Search** button.
The Staff List displays with the search results.
- 9** Select the worker's name from the *Staff List*, then click on the **OK** button.
The New Unit Detail window displays.
- 10** Click on the drop-down arrow for the **Role** field and select the appropriate role for the worker from the resulting list.
- 11** Click on the drop-down arrow for the **In/Out** field and select the appropriate assignment from the resulting list.
- 12** If the worker is to be the Unit Approver, click on the **Unit Approver** check box.
*A check mark displays in the **Unit Approver** check box.*
- 13** Click on the **Modify** button.
A check mark displays next to the worker's name to indicate the Unit Approver assignment
- 14** Repeat **Steps 7 – 13** for each worker to be assigned to the unit.
- 15** Click on the **Save** button.
The Unit List displays.
- 16** Click on the **Close** button.



Remember that if you select "In" for In/Out Assignment, the worker will be removed from the unit in which currently assigned because a worker can only be In-Assigned to one unit at a time.

Changing a Unit's Specialization

A unit's specialization is a description of the sort of work the unit performs, such as "Data Entry," "Child Protective Services (listed as **Child Prot Services** in the drop-down list)," or "Foster Care." There may be situations in which a unit's specialization needs to be changed due to agency reorganization or an incorrect selection when the unit was first created.



Step-by-Step: Changing a Unit's Specialization

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Unit List displays with the Agency field pre-filled.
- 2 In the **Unit** field, enter the Unit number of the unit whose specialization you wish to change.
- 3 Click on the **Search** button.
The Unit Approver for the unit displays in the list.
- 4 Click to select the Unit Approver, then click on the **Detail** button.
The Unit Detail window displays.
- 5 Click on the drop-down arrow for the **Unit Specialization** field and select a new specialization from the resulting list.
- 6 Click on the **Save** button.
The unit specialization is changed. A unit can only be deleted if it has no subordinate units.
- 7 Click on the **Close** button.

Deleting a Unit

There will be situations in which a Security Coordinator needs to delete a unit from the agency. Perhaps workers from the unit have all been reassigned to other units as part of an agency's reorganization, or a unit was created in CONNECTIONS that now only contains a conversion worker. Such empty units make it more difficult to keep track of workers and unit organization.

Before a unit can be deleted, any in-assigned staff must be moved to other units or end-dated, as appropriate. Out-assigned workers can be deleted using the *Maintain Unit* window, but be sure to leave one out-assigned worker in the unit and make sure that worker is assigned as Unit Approver.



Step-by-Step: Deleting a Unit in CONNECTIONS

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Unit** command.
The Unit List displays with the Agency field pre-filled.
- 2 In the **Unit** field, enter the Unit code for the unit to be deleted.
- 3 Click on the **Search** button.
The Unit Approver for the unit displays in the list.
- 4 Click to select the Unit Approver, then click on the **Detail** button.
The Unit Detail window displays.
- 5 Click to select the worker's name in the **Member Information** field.
- 6 Click on the **Delete** button to remove the worker from the unit.
The worker's name is removed from the list.
—OR—
Click on the **File** menu on the *Unit Detail* window and select **Delete**.
The following message displays: "Are you sure you wish to delete this unit?"
- 7 Click on the **Yes** button to delete the unit.
The Unit List displays.
- 8 Click on the **Close** button.



A unit can only be deleted if it has no subordinate units.

If you attempt to delete a unit that is a Supervisory Unit to one or more other units, the **Delete** command will not enable in the **File** menu on the *Unit Detail* window.

To delete the Supervisory Unit, you must first move all of its subordinate units to other units on the *Organizational Hierarchy* window. (See page 69.) Only then will the **Delete** command enable.



CONNECTIONS will not permit the deletion of a unit if *any* stage was *ever* assigned to a worker in that unit.

CONNECTIONS determines historical jurisdiction through unit numbers, so these numbers must remain in the system.

If all workers are to be transferred out of a unit, but the unit cannot be deleted, be sure to out-assign one of the transferring workers as a Unit Approver for the now "empty" unit.



Any conversion workers remaining in a unit can be removed from the unit using the **Delete** button as described above for an Out-Assigned worker.

Unit Organization Housekeeping

The creation and deletion of units and the moving of workers between units can result in the following types of situations:

- Multiple units end up with the same agency/site/unit code. Each agency/site/unit should be unique. Duplicates should be deleted or consolidated.
- There are many conversion units with no workers, one conversion worker, one conversion worker and one other worker, or just one worker. These units should be deleted and/or consolidated as necessary.



An easy way to see a complete list of all units in an agency is the Staff Security Report. (See Module 9: Security Reports.)

The Creation of Default Units: Background

An understanding of how default units are created and populated provides a basic foundation for unit maintenance.

When a new staff person is added through WEBSTAR, the information is sent to the nightly batch update. When the batch is run, it looks to see if the designated site contains a unit beginning with "N." If there is, the system attempts to add the person to the highest numbered "N" unit. An "N" unit can hold a maximum of 50 workers. If the highest numbered "N" unit already contains 50 workers, a new "N" unit is created using the next highest number. (For example, if N12 is full, unit N13 will be created.)

If the highest numbered N unit is N99 and that unit is full, the next unit created by the batch will be N00. Subsequent N units will all be numbered N00 (since a unit designation can only contain 3 characters).

When a new default unit is created, it is automatically populated with a generic Conversion Person (PID 18012), who serves as the Unit Approver; thus, each N unit can really only accept 49 new workers.

Anyone in the Conversion Unit can continue to work on current assigned cases on his/her *Assigned Workload*, but s/he cannot be assigned any new cases while in any Conversion Unit (defined as any unit with the Conversion worker as the Unit Approver).

When a worker is placed in a default Unit with the Conversion Person as the Unit Approver, the worker cannot be made Case Assignable, and cannot be assigned Business Functions. Once the worker is placed in an actual unit, s/he can then be designated as Case Assignable and assigned Business Functions. Any worker added to CONNECTIONS is initially automatically assigned the single Business Function STANDARD ACCESS, which only allows access to the CONNECTIONS Toolbar.

As the Security Coordinator moves new workers from their default units to their in-assigned units, this leaves N units with only the generic Conversion Person. If these units are not cleared out (by deleting the Conversion Person and then deleting the unit), CONNECTIONS is eventually forced to create multiple N00 units.



The Unit Approver Report can provide you with a view of all the Unit Approvers in your agency. (See Module 9: Security Reports.)

To avoid the creation of duplicate units, the Security Coordinator should delete the Conversion Person from N units that contain no other workers and then delete those units. There are also a large number of units with only one person or only one person and the Conversion Person. A CONNECTIONS system data fix cannot be done for these; as only the district or agency will know if the person in the unit still works for the agency and whether the person should be end-dated or moved, or if the district or agency has a reason for keeping the unit with only one person in it.

If stages are associated with units, they cannot be deleted. CONNECTIONS is working on a solution to the situation where there are units that have stages associated with them that districts and agencies want to delete.

As Security Coordinator, you should either end-date or in-assign staff to a permanent unit. In-assigning the real person to another unit (or end-dating the worker) and subsequently deleting the unit will remove the units with just one person in them. If that one person is out-assigned to the unit, the unit can simply be deleted after deleting the out-assigned person. To maintain the units that have only one person or the Conversion Person, move the real person to another unit or end-date the worker, then delete the Conversion Person from the unit, and finally delete the unit.

A listing is available of the units that have to be deleted by the district or agency, with the name of the staff person in each unit. Contact your CONNECTIONS Regional Office Implementation Representative if you have questions.

Please keep in mind that access should always be granted on a "Need to Know" basis; no staff should be granted access because they "might" need that access in the future.

The Agency Access Window

Security Coordinators can provide access privileges to workers within their own districts/agencies, aside from the assignment of Business Functions. Security Coordinators use the *Agency Access* window to create and maintain access privileges for their own agencies; in order to perform these functions, the Security Coordinator must have the MAINT AGY ACC Business Function. Agency staff can be granted view privileges, maintain privileges or no privileges for each staff grouping (Case Assignable Staff, Unit Approver, Direct Supervisory Line).

Agency Access is only available for system functionality created with Build 18 and beyond. In deciding whether to use Agency Access and how to set up Agency Access, administrative personnel must consider what kind of access they would like their staff to have. Decisions must be made regarding what staff should have view access, maintain access or no access to other workers' cases. For example, a small agency with less than 10 workers where there is overlap between worker responsibilities (e.g., all workers may have both CPS and foster care job roles) may prefer for all staff to have maintain access to all cases in the agency; however, that type of setup may not work for a large agency where there are clear divisions of unit responsibilities and there is no overlap in worker roles. The decision of how to use Agency Access should be based on the size and culture of the agency and whether the agency wants to permit more open access to cases. Each agency must carefully decide who *needs* what type of access. Access should always be granted only on a "*Need to Know*" basis; no staff should be granted access because they might need that access in the future.

Initially, Agency Access needs to be created for each agency. If the *Agency Access* window is opened in either view-only or modify mode *before* Agency Access has been recorded and saved in CONNECTIONS, the default access for all staff groupings is **None** and the following message displays:

"Agency Access Information has not yet been entered."

Once the Security Coordinator has established Agency Access, the most current data will be retrieved each time the *Agency Access* window opens.

In order to view the *Agency Access* window, a worker's BFP must include the VIEW AGY ACC Business Function. To maintain this window, the worker's BFP must include the MAINT AGY ACC Business Function.

The *Agency Access* window works in conjunction with the *Organizational Hierarchy* window. The organizational hierarchy of each district/agency is viewed and maintained on the *Organizational Hierarchy* window.

The **District/Agency** field at the top of the window automatically populates with the worker's own district/agency code. For example, if the worker's Agency ID is A01, "A01" displays in the **District/Agency** field.

The main body of the *Agency Access* window is divided into three sections:

Case Assignable Staff

This section works in conjunction with the **Case Assignable** check box on the *Staff Detail* window, the unit to which the worker is assigned, and the worker's Job Type.

Three staff groupings are included in this section:

- **All Within District** provides access to all cases in the district/agency.
- **All Within Unit** provides access to all cases in the same unit.
- **All Within Same Job Type** provides access to all cases that are of the same Job Type as the staff person.

Unit Approver

This section is used only for staff with Unit Approver status in the district/agency, whether In- or Out-Assigned.

Two staff groupings are included in this section:

- **All Within District** will provide access to all cases in the district/agency for all Unit Approvers.
- **All Within Same Unit Spec** will provide access to all cases within the same unit specialization for all Unit Approvers.

**Direct
Supervisory
Line**

This section works in conjunction with the *Organizational Hierarchy* window.

Two staff groupings are included in this section:

- **All Staff** provides access to all cases within a direct supervisory line for all staff, regardless of Job Type.
- **All Non-Clerical Staff** provides access to all cases within a direct supervisory line for all staff with a Non-Clerical Job Type. (See Appendix E for a list of Job Types.)

The Security Coordinator can assign **View** access, **Maintain** access, or **None** by clicking on the corresponding radio button for each staff grouping within each section, as appropriate.

Two buttons display at the bottom of the *Agency Access* window:

Save

This button saves the information to the database and closes the *Agency Access* window. This button enables only if unsaved changes have been made to the window. Clicking on the **Save** button displays the following message:

“Changes have been saved.”

- Click on the **OK** button in response to this message to close the *Agency Access* window.

Cancel

This button discards any unsaved information and closes the *Agency Access* window.

If the window was opened in view-only mode, clicking on this button closes the window. If the window was opened in modify mode and unsaved changes have been made to the window, clicking on the **Cancel** button displays the following message:

*“Do you want to exit?
Unsaved data and/or narrative(s) will be lost.”*

- Click on the **Yes** button to discard any unsaved information and close the *Agency Access* window.
- Click on the **No** button to keep the window open without discarding unsaved information.



Step-by-Step: Accessing the **Agency Access Window in View-Only Mode**

- 1 Click on the **Options** menu on the CONNECTIONS Toolbar and select the **View Agency Access** command.
The Agency Access window displays in view-only mode.



Step-by-Step: Maintaining Agency Access

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar and select the **Agency Access** command.
*The Agency Access window displays in modify mode. If agency access has not yet been established, the following message displays:
“Agency Access information has not yet been entered.”*
- 2 Click on the **OK** button in response to the message.
*The default setting for all staff groupings on the Agency Access window is **None**.*
- 3 To change the agency access setting for a specific staff grouping, click on its corresponding **View**, **Maintain** or **None** radio button, as appropriate.

If two workers access the *Agency Access* window in modify mode for the same district/agency at the same time, only the first worker who saves the changes will be allowed to do so. If the second worker attempts to save changes after the first worker has done so, the following message displays:

“Save Failed: Data has been modified by another user. Exit and try again.”

Click on the **OK** button to close the message.

The default agency access is established based on the business rules, which are reflected in the Agency Access Options Matrix on the next page.

The following conditions apply to the *Agency Access* window:

- For each of the options, only one (**View**, **Maintain** or **None**) may be selected.
- There are no system edits necessary among the choices for the three sets of options, because each one encompasses a different set of staff.
- If the district/agency has not yet opened the *Agency Access* window in modify mode and saved the information, the default is **None** for all choices.
- The access granted via the *Agency Access* window does *not* remove access granted in other ways. The options on this window only *add* access to that which is granted in other ways, they will never remove access.

Agency Access Options Matrix

(E = Option Enabled D = Option Disabled)
 (Highlighted items indicated what is selected or enabled.)

Case Assignable Staff

	View	Maintain	None
All Within District/Agency	Selected		
All Within Unit	D	E	D
All Within Same Job Type	D	E	D

When **View** is selected for the **All Within District/Agency** staff grouping, only the **Maintain** radio button enables for the **All Within Unit** and **All Within Same Job Type** staff groupings. If no radio button is selected for either of these staff groupings, the default access is **View**, since that was selected for all workers within that district/agency.

	View	Maintain	None
All Within District/Agency		Selected	
All Within Unit	D	D	D
All Within Same Job Type	D	D	D

When **Maintain** is selected for the **All Within District/Agency** staff grouping, *all* radio buttons disable for the **All Within Unit** and **All Within Same Job Type** staff groupings, since the broadest level of agency access has already been established for all workers within that district/agency.

	View	Maintain	None
All Within District			Selected
All Within Unit	E	E	E
All Within Same Job Type	E	E	E

When **None** is selected for the **All Within District** staff grouping, *all* radio buttons enable for the **All Within Unit** and **All Within Same Job Type** staff groupings. If no radio button is selected for either of these staff groupings, the default access is **None**, since that was selected for all workers within that district/agency.

Unit Approver

	View	Maintain	None
All Within District	Selected		
All Within Same Unit Spec.	D	E	D

When **View** is selected for the **All Within District** staff grouping, only the **Maintain** radio button enables for the **All Within Same Unit Spec** staff grouping. If no radio button is selected for this staff grouping, the default access is **View**, since that was selected for all workers within that district/agency.

	View	Maintain	None
All Within District		Selected	
All Within Same Unit Spec.	D	D	D

When **Maintain** is selected for the **All Within District** staff grouping, *all* radio buttons disable for the **All Within Same Unit Spec** staff grouping, since the broadest level of agency access has already been established for all workers within that district/agency.

	View	Maintain	None
All Within District			Selected
All Within Same Unit Spec.	E	E	E

When **None** is selected for the **All Within District** staff grouping, *all* radio buttons enable for the **All Within Same Unit Spec** staff grouping. If no radio button is selected for this staff grouping, the default access is **None**, since that was selected for all workers within that district/agency.

Direct Supervisory Line

	View	Maintain	None
All Staff	Selected		
All Non-Clerical Staff	D	E	D

When **View** is selected for the **All Staff** grouping, only the **Maintain** radio button enables for the **All Non-Clerical Staff** grouping. If no radio button is selected for this staff grouping, the default access is **View**, since that was selected for all workers within that district/agency.

	View	Maintain	None
All Staff		Selected	
All Non-Clerical Staff	D	D	D

When **Maintain** is selected for the **All Staff** grouping, *all* radio buttons disable for the **All Non-Clerical Staff** grouping, since the broadest level of agency access has already been established for all workers within that district/agency.

	View	Maintain	None
All Staff			Selected
All Non-Clerical Staff	E	E	E

When **None** is selected for the **All Staff** grouping, *all* radio buttons enable for the **All Non-Clerical Staff** grouping. If no radio button is selected this staff grouping, the default access is **None**, since that was selected for all workers within that district/agency.

Agency Access Scenarios

Personnel determining Agency Access for their agency must have a clear understanding of the ramifications of setting up certain types of access. The following scenarios have been created to help show what an agency's access will look like, based on certain factors selected while using the Agency Access functionality in CONNECTIONS. These examples may help assist administrative personnel in determining their ideal Agency Access setup.

In all of the following scenarios, when a worker is granted View access, s/he must access the case via a Person/Case Search (not from the *Assigned Workload*). Maintain access is available from the *Assigned Workload* and the worker must be assigned the UNIT SUM ACCESS Business Function. If the worker is not assigned this Business Function, s/he can still view the case through a Case/Person Search.

The following scenarios are based on this information regarding worker Phil:

Phil works for Unit 001 in an agency and is Case Assignable. In Unit 001, he is higher than the Unit Approver. Unit 001 is the Supervisory Unit to Unit 002. Phil's Business Function Profile (BFP) includes UNIT SUM ACCESS, but not ACCESS ALL DIST.

Scenario 1

Agency Access is set to “None” for all categories.

The screenshot shows a software window titled "Agency Access" with a menu bar containing "File", "Options", and "Help". Below the menu bar, there are two input fields: "Agency" with the value "A31" and "Office Type" with a dropdown menu set to "District". The main area of the window is divided into three sections, each with a title and a list of categories with radio buttons for "View", "Maintain", and "None".

Section	Category	View	Maintain	None
Case Assignable Staff	All Within District	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Within Unit	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Within Same Job Type	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Unit Approver	All Within District	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Within Same Unit Spec.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Direct Supervisory Line	All Staff	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Non-Clerical Staff	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

At the bottom of the window, there are three buttons: "Search", "Save", and "Cancel".

Due to his position in the Unit and his BFP, Phil can access and modify the *Assigned Workload* and *Staff To-Do List* of the Unit Approver of Unit 001, as well as the *Assigned Workload* and *Staff To-Do Lists* of all workers in Unit 001. Phil has no access to cases in Unit 002.

Scenario 2

For Case Assignable staff, Agency Access is set to “View” for All Within District; this action automatically selects “None” for All Within Unit and All Within Same Job Type.

For all Unit Approver and Direct Supervisory Line groupings, “None” is selected.

The screenshot shows the 'Agency Access' configuration window. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu bar, there are two input fields: 'Agency' with the value 'A31' and 'Office Type' with a dropdown menu showing 'District'. The main area is divided into three sections, each with a title and a list of options with radio buttons:

- Case Assignable Staff**
 - All Within District: View, Maintain, None
 - All Within Unit: View, Maintain, None
 - All Within Same Job Type: View, Maintain, None
- Unit Approver**
 - All Within District: View, Maintain, None
 - All Within Same Unit Spec.: View, Maintain, None
- Direct Supervisory Line**
 - All Staff: View, Maintain, None
 - All Non-Clerical Staff: View, Maintain, None

At the bottom of the window, there are three buttons: 'Search', 'Save', and 'Cancel'.

Phil has access to all cases within his agency. However, he cannot modify any of the cases outside of his unit.

Scenario 3

For all Case Assignable Staff and Direct Supervisory Line groupings, Agency Access is set to “None.”

For the All Within District Unit Approver grouping, “Maintain” is selected; this action automatically selects “None” for All Within Same Unit Spec.

Section	Grouping	View	Maintain	None
Case Assignable Staff	All Within District	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Within Unit	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Within Same Job Type	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Unit Approver	All Within District	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
	All Within Same Unit Spec.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Direct Supervisory Line	All Staff	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
	All Non-Clerical Staff	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Phil will have access to all stages within his own unit due to his BFP. However, the Agency Access selected does not provide him with any additional access since he is not a Unit Approver.

Scenario 4

For all Case Assignable Staff and Unit Approver groupings, Agency Access is set to “None.”

For Direct Supervisory Line, Agency Access is set to “View” for All Staff; this action automatically selects “None” for All Non-Clerical Staff.

The screenshot shows the 'Agency Access' dialog box. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu bar, there are two input fields: 'Agency' with the value 'A31' and 'Office Type' with a dropdown menu showing 'District'. The dialog is divided into three main sections, each with a title and three radio button options: 'View', 'Maintain', and 'None'.
1. 'Case Assignable Staff' section:
- 'All Within District': View, Maintain, None (None is selected)
- 'All Within Unit': View, Maintain, None (None is selected)
- 'All Within Same Job Type': View, Maintain, None (None is selected)
2. 'Unit Approver' section:
- 'All Within District': View, Maintain, None (None is selected)
- 'All Within Same Unit Spec.': View, Maintain, None (None is selected)
3. 'Direct Supervisory Line' section:
- 'All Staff': View (selected), Maintain, None
- 'All Non-Clerical Staff': View, Maintain, None (None is selected)
At the bottom of the dialog, there are three buttons: 'Search', 'Save', and 'Cancel'.

Phil has view access to all cases in Unit 002 because Unit 002 is in the direct supervisory line of his unit.

Scenario 5

For all Case Assignable Staff and Unit Approver groupings, Agency Access is set to “None.”

For Direct Supervisory Line, Agency Access is set to “Maintain” for All Staff; this action automatically selects “None” for All Non-Clerical Staff.

The screenshot shows the 'Agency Access' configuration window. At the top, there is a menu bar with 'File', 'Options', and 'Help'. Below the menu bar, there are two input fields: 'Agency' with the value 'A31' and 'Office Type' with a dropdown menu showing 'District'. The window is divided into three main sections, each with a title bar and a list of options with radio buttons for 'View', 'Maintain', and 'None':

- Case Assignable Staff:**
 - All Within District: View, Maintain, None
 - All Within Unit: View, Maintain, None
 - All Within Same Job Type: View, Maintain, None
- Unit Approver:**
 - All Within District: View, Maintain, None
 - All Within Same Unit Spec.: View, Maintain, None
- Direct Supervisory Line:**
 - All Staff: View, Maintain, None
 - All Non-Clerical Staff: View, Maintain, None

At the bottom of the window, there are three buttons: 'Search', 'Save', and 'Cancel'.

Phil has maintain access to all cases in Unit 002 because Unit 002 is in the direct supervisory line of his unit.

Organizational Hierarchy Window

Local districts and voluntary agencies can establish an organizational hierarchy in CONNECTIONS that best represents their own organizational structure. The *Organizational Hierarchy* window provides an organizational chart of a district/agency and its corresponding units. Workers with the proper security can view and/or modify access to their own district/agency. Changing a unit's position within the organizational hierarchy of the district/agency can grant implicit security access rights to individuals at higher management levels. Anyone in a direct supervisory line above a worker with a role in the case can be given access to that case, *if the district/agency chooses to authorize such access*. As with Agency Access, organizational hierarchy is only available for system functionality created with Build 18 and beyond.

When the *Organizational Hierarchy* window opens, CONNECTIONS automatically searches for and retrieves the following information to build the organizational hierarchy for the district/agency:

- Unit Number, Unit Specialization, In-/Out-Assignment data, Unit Approver and Supervisory Unit (from the *Unit Detail* window)
- Employee Name and Employee Role (from the *Staff Detail* window)

The *Organizational Hierarchy* window contains a tree-view list that displays the organizational hierarchy for the specified district/agency. This tree-view list has the look and feel of Windows Explorer, providing a familiar environment for maintaining the Organizational Hierarchy of the units within a district/agency. When this window opens, the following information is pre-filled by the system:

- User's **District/Agency**
- User's **Office Type**
- Tree-view list displaying the district/agency and units in a hierarchical display

All units in the district/agency display on the left side of the window. By default, units display directly under the root (district/agency). Once a unit is moved, it displays where it has been inserted. Each unit is listed under its supervisory unit. Each unit is displayed with a name that is composed of the Site ID, Unit number and Unit Specialization.

For example:

If a unit has a Unit Number labeled "VAB" and a Unit Specialization labeled "Administration" in site "1Q2," this unit will display as (1Q2) VAB-Administration.

The *Organizational Hierarchy* window contains two fields at the top of the window:

District/Agency	The code of the worker's own district/agency (e.g., "A15" for Essex County DSS, "A31" for Onondaga County).
Office Type	The district/agency's office type (e.g., "District" for LDSS offices, "Vol Agen" for voluntary agencies).

Below these fields are two lists: the tree-view list on the left side of the window and the detail list on the right side.



Step-by-Step: Accessing the Organizational Hierarchy Window in View-Only Mode

- 1 Click on the **Options** menu on the CONNECTIONS Toolbar.
- 2 Select the **View Org. Hierarchy** command.
The Organizational Hierarchy window opens in view-only mode.



Step-by-Step: Accessing the Organizational Hierarchy Window in Modify Mode

- 1 Click on the **Maintain** menu on the CONNECTIONS Toolbar.
- 2 Select the **Org. Hierarchy** command.
The Organizational Hierarchy window opens in modify-mode.

Drag-and-Drop Feature

Workers with the MAINT ORG HIER Business Function can modify the hierarchy of the units within their district/agency by using a drag-and-drop feature. Click the *right* mouse button to initiate this feature. Highlight a unit within the agency/district, then drag and drop it under a supervisory unit, thereby modifying its organizational position within the district/agency. Each time a drag-and-drop action is performed, the following message displays:

“Are you sure you want to make this change to the Organizational Hierarchy?”

- Click on the **Yes** button to save the change.
- Click on the **No** button to cancel the change.

The message also allows the worker to turn off the confirmation message by selecting the **Do not prompt again in this window session** check box at the bottom of the message box. When the *Organizational Hierarchy* window is closed, the session is ended. The next time the window is opened in modify mode, a new session begins and the confirmation message displays after each drag-and-drop action is performed. Changes are saved when the worker clicks on the **Yes** button in response to the confirmation message; if the worker turns off the confirmation message for that session, the changes are saved immediately as they are made.

If the worker attempts to drag and drop a unit onto itself, or drag and drop a supervisory unit under a subordinate unit, no change displays in the tree-view list. If a unit is listed several pages below in the tree-view list and the worker needs to drag and drop it to the root unit, s/he can drag the unit and drop it on any blank area within the tree-view list. (See the screen graphic on page 76.) This feature eliminates the need to drag a unit and scroll several pages to reach the top of the tree-view list.

System edits will be in place to prevent two workers from modifying the Organizational Hierarchy for the same district/agency at the same time. For example, if Worker A moves the Adoptive unit from the Foster Care unit to the Preventive Services unit, Worker B is prevented from moving the Adoptive unit to any other unit. Worker B is also prevented from moving any other units into the Preventive Services unit. If Worker B attempts to do so, the following message will display:

*“Save Failed: Data has been modified by another user.
Exit and try again.”*

A system edit that currently prevents workers from creating duplicate units within an agency site remains in place.

Module 9: Security Reports

Five Security Reports are available from the CONNECTIONS Data Warehouse. These reports are a valuable tool for the maintenance of CONNECTIONS security. This module describes these reports and how to obtain them.

Depending on the particular report, the information it contains can be useful in specific situations or as an overview of agency security information. In some cases, using two reports together can provide important information that would otherwise be difficult to obtain. We'll look at the contents of each report individually, see where they can be helpful, and learn how to obtain them.

By the end of this module, you will be able to list the reports used in managing CONNECTIONS security and describe their contents.

Requesting Security Reports

The OCFS Data Warehouse is a repository of data retrieved from the CONNECTIONS and Child Care Review Service (CCRS) systems that can be accessed independently of those systems. The data from the two systems is organized and stored in the Data Warehouse and is available as a read-only file in current point-in-time (snapshot), trend and historical views. The Data Warehouse is updated on a weekly basis; thus, every Monday the data reflects the state of the CONNECTIONS system as of the previous week. The Security Reports all include an “As of” date, which indicates when the Data Warehouse was last updated.

Reports are generated from the OCFS Data Warehouse using an application called Cognos. Each agency should have at least one designated Cognos specialist—a staff member trained in the use of Cognos to generate reports from the Data Warehouse.

Check with your supervisor to determine the Cognos specialist for your agency. Depending on which security report you are requesting, you may be asked for certain information.

Report	Required Information
Staff Security	Agency code Site(s) or unit(s) to be reported on
Business Function	Agency code Business Functions to be reported on
Assignee Designee	Agency code
Unit Approver	Agency code
Organizational Hierarchy	Agency code

Reports are available in two formats: Excel spreadsheet and Adobe Acrobat (.pdf file).

Staff Security Report

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 been assigned, which staff member 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 must access three different windows—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 BFP at the same time. Seeing more than one worker's BFP at one time would enable the Security Coordinator to determine the appropriate mix of Business Functions more easily for a particular unit.

The Staff Security Report addresses these issues by allowing local Security Coordinators to see this information in one pre-formatted report. An agency can only generate reports on its own staff. The data from which the report is drawn is updated weekly.

The Staff Security Report includes the following information:

Staff Name	Worker's name as it displays 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 any other worker?
Case Assignable	Yes or No – Can case stages be assigned to the worker?

The report also includes the agency name and code, the site code, the unit code, the date of the report and the date the database was last updated ("As of" date).

The request for the report starts with the Agency code. The requester can then specify the site(s) or unit(s) within the agency to be reported on. The report is sorted by site, then by unit, and then alphabetically by worker last name.

See Appendix G for an example of the Staff Security Report.



The report only displays 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 member has a particular Business Function. Such a listing would enable the Security Coordinator to determine the appropriate mix of Business Functions more easily for a particular unit and to be sure that all workers' BFPs accurately reflect their responsibilities.

There is no automated way for a Security Coordinator to obtain this information within the CONNECTIONS application. A local Security Coordinator must 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 need to check assignees and designees to determine if any worker has given another worker the rights to that Business Function.

The Business Function Report addresses these issues by allowing local Security Coordinators to see this information in one pre-formatted report. This report, together with the Assignee/ Designee Report, provides information about all workers who have a particular Business Function either as part of their own BFP or as a designee of someone who has it.

An agency can only generate reports on its own staff. The data from which the report is drawn is updated weekly.

The Business Function Report includes the following information:

Agency	The name of the agency
Agency Code	The agency's unique 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, the date of the report, and the date the database was last updated ("As of" date).

The request for the report starts with the Agency code. Office Type is automatically filled in for that code. The requester can then specify from a drop-down list of all available Business Functions which Business Functions are to be reported on. (If a Business Function is selected that is not available for the office type being reported on, the results will be blank.) The report will be sorted by site, then by unit, and then alphabetically by worker last name.

For an example of the Business Function report, see Appendix G.

Assignee/Designee Report

For reasons mentioned in the previous two sections, 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 determine more easily which staff person has which Business Functions.

There is no automated way for a Security Coordinator to obtain this information within the CONNECTIONS application. A local Security Coordinator must review the *Maintain Designee* or *Staff Security* window for each worker, one at a time, to see if that worker is any other staff member's designee or assignee.

The Assignee/Designee Report 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 about all workers who have a particular Business Function either as part of their own BFP or as a designee of someone who has it.

An agency can only generate reports on its own staff. The data from which the report is drawn is updated weekly.

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, the date of the report, and the date the database was last updated ("As of" date).

The request for the report starts with the Agency code. The report is sorted by site and then alphabetically by worker last name.

For an example of the Assignee Designee report, see Appendix G.

Unit Approver Report

There are instances in which it is very helpful for a Security Coordinator to be able to see easily who the Unit Approver is for any unit in the agency. Such instances involve changing Unit Approvers or to view the units with the Conversion Person (PID 18012) as the Unit Approver. As was mentioned in Module 7 (“Changing Unit Approver” on page 45), a Unit Approver cannot be end-dated in CONNECTIONS until s/he is removed as a Unit Approver. Such information 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 must 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 Unit Approver Report addresses these issues by allowing local Security Coordinators to see this information in one pre-formatted report.

An agency can only generate reports on its own staff. The data from which the report is drawn is updated weekly.

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, the date of the report, and the date the database was last updated (“As of” date). The request for the report starts with the Agency code. The report is sorted alphabetically by worker last name. For an example of the Unit Approver report, see Appendix G.



Organizational Hierarchy Report

You can be provided a means to view how an agency is organized by accessing the OCFS Data Warehouse to view the Organizational Hierarchy. The Organizational Hierarchy Report allows users to view the organizational hierarchy for their agency in a pre-defined report. The report can be printed as needed.

This prompt defaults to your agency code; you can select multiple agencies. Workers with the proper security can view and/or modify access to their own district/agency. If the worker is in the State Worker user class, more than one agency will be presented by the prompt and all may be selected.

The Organizational Hierarchy Report includes the following information:

Agency Code	The Agency Code from CONNECTIONS.
Agency Name	The Name of the Agency.
Parent Unit	The Site Code, Unit Code and Unit Specialization from Connections for a unit with no units above it in the organizational hierarchy.
Level One and Subsequent Levels	The Site Code, Unit Code and Unit Specialization from Connections for the Level One Unit in the hierarchy. Level one is the unit just below the Parent unit, Level 2 is the next level below level one and this continues to the lowest level of unit in the organizational hierarchy.
Data As Of	The date of the last refresh of the data in the report.
Date of the Report	The date this report was run.

The report is sorted alphabetically by the Parent Unit, then by Levels. The report has dynamic columns that will expand as more levels of the hierarchy are entered into CONNECTIONS. If you have seven or more levels in your agency's hierarchy, the report will expand. If you have not entered an Organizational Hierarchy, the report will only contain a list of Parent Units. The data supporting this report is refreshed weekly.

Appendix A:

Security Coordinator Roles and Responsibilities

When New Staff Join the Agency

- Move staff from Temporary Unit to In-Assigned unit.
- Assign Business Functions to grant appropriate system access.
- Assign a Job Type(s) (Optional)
- Inform the worker of the BFP, related to what tasks can be accomplished and any changes to the viewing and maintaining rights.

Maintain Security for Existing Agency Staff

As worker responsibilities, staff makeup, and system functionality change, agency security will need to be modified to ensure that all workers have appropriate access to CONNECTIONS.

For existing workers:

- Assign additional Business Functions.
- Remove Business Functions from a worker's BFP.
- Assign a Job Type(s) (Optional)
- Create Out-Assignments.
- Change Unit Approvers.
- Update worker name information.

When workers transfer or move:

- A worker transferring within an agency needs to be transferred to the new unit and the BFP must be adjusted to reflect any new duties.
- Assign a Job Type(s) (Optional)
- A worker moving to a new agency must be end-dated in the agency currently employed for by that agency's Security Coordinator. The worker can then be moved into the new unit by the Security Coordinator of the new agency and be assigned new Business Functions.

When workers leave CONNECTIONS:

- End-date staff – This must occur **before** the worker's Person ID is disabled or deleted through WEBSTAR.

When workers return to CONNECTIONS:

- Reinstate staff.
- Assign Business Functions.
- Assign a Job Type(s) (Optional)

When a CONNECTIONS system build includes new Business Functions:

- Reference the security update information for the build.
- Determine who in the agency requires the new Business Functions.
- Assign new Business Functions to appropriate staff.
- Notify affected staff of the new Business Functions.

When Security Coordinator responsibilities need to be transferred:

- The old Security Coordinator must establish a new Security Coordinator.
- The new Security Coordinator must remove the old Security Coordinator.

Maintain Units

- Create Units
- Change Unit Specializations
- Delete Units
- Maintain Agency Access
- Assign a Job Type(s) (Optional)
- Create Organizational Hierarchy

Appendix B: Glossary of Terms Used in Security

Access	A worker's ability to view or maintain information in CONNECTIONS.
Agency	A local district, voluntary agency, or other jurisdictional entity made up of one or more units.
Application Security	Focuses on granting access to the CONNECTIONS application itself as opposed to the computer network as a whole.
Assignee	Workers who temporarily assigns their own security rights to another worker.
Assignee Designee Report	A report available from the CONNECTIONS Data Warehouse that lists which agency workers are assignees or designees and for whom.
Business Function (BF)	Used by the local Security Coordinator to maintain security and grant CONNECTIONS access to workers. BFs are made up of Security Attributes to allow access to a particular window, dialog or functionality. Each BF is designed to allow a worker to perform a particular function or group of functions.
Business Function Profile (BFP)	The list of all Business Functions given to a worker. It is attached to the worker's logon ID and it is this profile that the system checks to determine which windows and functionalities the worker is permitted to access.
Business Function Report	A report available from the CONNECTIONS Data Warehouse that lists all workers in an agency who have been assigned a particular Business Function.
Business Function Requiring Special Handling	A Business Function that allows a worker to change data in a case, including changes that affect the results returned in a search. Designed to be given to specific types of workers.
CCF	Office Type: Council of Children and Families.
CQC	Office Type: Commission of Quality Care.
Current Role in a Stage	Being assigned as the Primary or Secondary in a stage of a case.
Default Unit	A "holding place" for workers until they can be In-Assigned to their proper units. All workers are initially In-Assigned to one of the agency's default units. The Security Coordinator moves workers from default units to their In-Assignments.
Designee	The worker who is temporarily assigned the security rights of another worker.
DFY	Office Type: OCFS Rehabilitative Services.
Dialog	A series of windows that work together to capture information or perform a function.
District	Office Type: Local County Social Services.
DSS	Office Type: State OCFS.

End-Dating Staff	Entering an end date in the <i>Maintain Staff</i> window to disable a worker's Person ID when that person has left an agency (either permanently or temporarily).
Historical Role	The role in a stage accorded a worker if the worker was the Primary or Secondary worker at the time a stage was closed.
Implied Role	The role in a stage accorded a worker if a person in a stage on their workload is also involved in that other stage.
In-Assignment	The formal placement of a worker into a unit. Each worker is In-Assigned to only one unit.
Job Type	A category designation in the <i>Staff Security</i> window that can allow access to the <i>Assigned Workload</i> of other workers with the same Job Type. (For example, someone designated as a Foster Care Caseworker could have view access to all other Foster Care Caseworkers' workloads in the district/agency, if the district/agency chose that option).
Job-Type Business Function	A collection of Security Attributes forming a single Business Function designed to meet the basic access requirements of a particular type of worker: CPS worker, CPS supervisor, FAD worker, or FAD supervisor.
Maintain Access	The ability to add, modify, update, delete, or otherwise manage information in CONNECTIONS.
Maintainer	Staff members with security rights to maintain the staff members, in their own office, in CONNECTIONS.
Manager	A unit member whose level exceeds the Supervisor's.
Office Type	Categorization of agencies that use CONNECTIONS. The nine Office Types are OCFS (State), Regional Office, Local District, Voluntary Agency, DFY (Division for Youth), CCF (Council of Children and Families), CQC (Commission on Quality Care), OMH (Office of Mental Health), OMRDD (Office of Mental Retardation Developmental Disabilities). Each Office Type has its own Security Profile.
OMH	Office Type: Office of Mental Health.
OMRDD	Office Type: Office of Mental Retardation and Developmental Disabilities.
Organizational Hierarchy Report	A report available from the CONNECTIONS Data Warehouse that lists the Organizational Hierarchy set up for an agency or multiple agencies.
Organizational Hierarchy window	Access that is determined by a unit's position within an organization.
Out-Assignment	The assignment of a worker to a unit that is not the unit into which the worker has been formally placed (In-Assigned). The Out-Assigned staff member does work for the unit, but this unit is not the primary unit that the staff member works for.
Primary Worker	The worker who has primary responsibility for a stage. There can be only one Primary worker for a stage.
Regional Office	Office Type: OCFS Regional Office.

Reinstating Staff	Removing an end-date from the <i>Maintain Staff</i> window to enable the worker's Person ID in CONNECTIONS.
Role in a Stage/Case	The role assigned to a staff person to work on a stage/case.
Secondary Worker	A worker who has been assigned some supporting tasks in a stage. There can be any number of Secondary workers assigned to a stage.
Security Attribute (SA)	The primary manner in which access to CONNECTIONS is given. Each SA allows access to a particular window, dialog, or functionality in CONNECTIONS.
Security Coordinator	The person in an agency responsible for maintaining CONNECTIONS security.
Security Profile	The list of all Business Functions available to a particular Office Type.
Sensitive Case	A case involving a person who is an agency, district, or state employee.
Site	A designation given to a particular location. Each site has its own unique code.
Staff Security Report	A report available from the CONNECTIONS Data Warehouse that lists all agency staff in CONNECTIONS, what Business Functions each staff member has, which staff member is a Unit Approver, and whether a staff member is an Assignee or Designee.
Stage Role	Workers with a stage role, if the worker is associated with a stage in some way, such that they are able to access information about that stage. Possible stage roles include having a Current role in a stage, having an Implied role in the stage, or having a Historical role in the stage.
Standard Access	The first level of CONNECTIONS access given to workers. It permits workers to see the CONNECTIONS Toolbar and use only those functions that do not allow access to CONNECTIONS client data.
Super User	A Business Function that gives its recipient state-wide access in CONNECTIONS.
Supervisor	Usually, but not necessarily, the unit member who is responsible for approving the work of all other unit members.
System Build	A group of functionality and feature changes introduced to the CONNECTIONS system.
System Security	Focuses on granting access to the OCFS computer system based on a worker's NT logon ID. Most aspects of system security are handled through an application called WEBSTAR.
Unit	A grouping of staff. A unit generally consists of a group of workers performing similar types of work and a supervisor managing the unit. A unit may be located in one office or it may be located in multiple offices.
Unit Approver	The person responsible for reviewing and approving all work done by workers in the unit. This role is usually assigned to a unit supervisor.
Unit Approver Report	A report available from the CONNECTIONS Data Warehouse that lists all Unit Approvers for an agency.

Unit Hierarchy	Access based on a person's position within a unit.
Unit Specialization	The primary function of a unit, such as Intake or Adoption.
View Access	The ability to see information in CONNECTIONS without having the ability to modify it in any way.
Voluntary Agency	Office Type: Non-Profit Foster Care, Preventive and/or Adoption agency.
WEBSTAR	Web Enhanced Basic Security to Authorize Resources. The application used to maintain system security through the assigning and maintenance of NT logon IDs.
Worker	A staff member in a unit.

Appendix C: Codes Used in CONNECTIONS Security

Job Categories

- Accounting
- Administrator
- Administrative Staff
- Adoption Services
- Assistant Commissioner
- Assistant Program Director
- Associate Commissioner
- Auditor
- Bureau Director/Head
- Case/Program Aide
- Caseworker
- Child Protective Services
- Child Protective Manager-Administration
- Child Protective Manager-CES
- Child Protective Manager-Operations
- Clerical Aide
- Clerical Associate 2
- Clerical Associate 3
- Clerical Support
- Commissioner
- Community Services Worker/Aide
- Custodial
- Deputy Commissioner
- Deputy Director-Administration
- Deputy Director-CES
- Deputy Director-Operations
- Liaison/Coordinator
- Manager
- Mental Health Coordinator
- Mentor Coordinator
- MIS Staff
- Nurse
- Office Manager
- Parent Advocate/Mentor
- Per Diem
- Preventive Services
- Principal Administrative Associate 1
- Principal Administrative Associate 2
- Principal Administrative Associate 3
- Program Director
- Program Manager
- Psychiatrist
- Psychologist
- Quality Control
- Receptionist
- Recreation Coordinator
- Regional Staff
- Secretary/Typist
- Security
- Senior Caseworker
- Senior Youth Counselor
- Site Director

Continued on next page ►

Job Categories (continued)

- District Director
- Doctor
- Eligibility
- Executive Administrative Assistant
- Executive Deputy Commissioner
- Executive Director
- Executive Secretary
- Family and Community Advocate
- First Deputy Director
- Fiscal
- Foster Care Services
- Home Finder
- House Aide
- Interstate Compact
- Legal/Court
- Special Assistant
- Social Worker/Clinician
- Staff Development
- State Adoption Services
- State Central Register
- Stockroom
- Supervisor
- Supervisor I
- Supervisor II
- Support Staff
- Teacher
- Temporary
- Trainee
- Visitation Specialist/Coordinator
- Youth Councilor

Unit Roles

- Maintainer
- Manager
- Supervisor
- Worker

Staff Skills

- Adolescent Issues
- Adoption Subsidy Specialists
- Adoption Worker
- Aftercare
- Case Analyst
- Child Disability
- Child Fatality
- Child Protective Services
- Community Service Coordinator
- Community/School Worker
- Contract Manager
- Creole
- Day Care
- Developmental Disability
- Domestic Violence
- Eligibility Specialist
- Family Preservation
- Family Reunification
- Foster Care
- Foster Care Billing
- Foster Care/Adoption Recruiting
- French
- HIV/AIDS
- Housing Specialist
- Independent Living
- Institutional Placement Coordinator
- Institutional Abuse Investigator
- Intensive Family Preservation
- Legal/Court
- Medical Issues
- Parent Education
- Permanency Plan Specialty
- Placement Coordinator
- Preventive Services
- Residential Care Specialty
- Respite Specialty
- Routing Coordinator
- Resource Maintainer
- Sexual Abuse
- Sign Language
- Spanish
- Staff Development
- Substance Abuse Prevention
- Substance Abuse Specialty
- Therapeutic Crisis Intervention
- Training Specialist
- Unmarried Parents
- Video Interview
- Vietnamese
- Volunteer Coordinator

Unit Specializations

- | | | | |
|--------------------------|--------------------------|---------------------------|---------------------------|
| • Accountability Review | • Dep Dir Operations | • Housing Subsidy | • Rate Setting |
| • Administration | • DepDirAdministration | • Human Resources | • Referral Monitoring |
| • Adopt Subsidy Review | • Deputy Commissioner | • Independent Living | • Regional Director |
| • Adoption | • Deputy Director | • Institutional | • Regional Office |
| • Adoption Review | • Deputy Director CES | • Institutional Abuse | • Residential Licensor |
| • Advocacy Center | • Discharge | • Intake | • Respite |
| • Aftercare | • District Director FPP | • Interstate Compact | • Sanctions |
| • Assistant Commissioner | • Div Director/Head | • Investigation & Reports | • School Based |
| • Assoc Commissioner | • Domestic Violence | • Kinship | • SCR – Intake |
| • Attorney | • Educational Consultant | • Legal | • SCR – Post Intake |
| • Audit | • Eligibility | • Management Services | • SCR – RFI |
| • Auxiliary Services | • Exec Dep Commissioner | • ManagementInfo Liaison | • SCR Clearances |
| • Bookkeeping | • Executive Director | • Medical | • Screening |
| • Bureau Director/ Head | • F/A Recruitment | • Medical Serv Review | • Service Plan Review |
| • Budget | • F/A Training | • Multi Discipline Team | • Sexual Abuse |
| • Case Management Unit | • Fam Assessment Prog | • Nursery | • Site Director Unit |
| • Case Transfer | • Family Outreach | • Office Management | • Spec/Exception Rate |
| • Central Office | • Family Preservation | • Operations Support | • Staff Development |
| • Child Care Licensing | • Family Reunification | • Other | • State Adoption Services |
| • Child Evaluation | • Family Services | • PersonsinNeedof Super | • Substance/Alcohol Abuse |
| • Child Fatality | • Family Violence | • Placement | • Support |

Continued on next page ►

Unit Specializations

(continued from previous page)

- Child Protective Services
- Comm/Facility
- Commissioner
- Community Liaison
- Complaints
- Comptroller
- Contract Manager
- Court Ordered Invest
- CPM-Administration
- Data Entry
- Day Care
- Financial Claims
- First Deputy Director
- Fiscal
- Foster Care
- Foster Care Licensing
- Generic
- Helpline
- Home Finding
- Homemaking
- Hospital
- Hospital & Sex Abuse
- Planning
- Pre-PlacementService
- Preventive
- Program Assessment
- Program Director
- Program Management
- Program Operation Support
- Program/Policy
- Project Confirm
- Protective Diagnostic
- Quality Control
- Teen Pregnancy
- TherapeuticFosCare
- Third Party Review
- TrainBiologicParents
- Training
- Training-Foster Child
- TrainingFosterParent
- Transitional Care
- Transportation
- Unit Clerk
- Youth Development

Appendix D: CONNECTIONS Security Profiles

Each of the nine Office Types in CONNECTIONS has an individualized list of available Business Functions. It is from this list that the Security Coordinator selects Business Functions to create Business Function Profiles.

Detailed Business Function Guidelines are available on the OCFS CONNECTIONS intranet site Security page.

The following tables list the Security Profile for each Office Type.

Security Profile for CCF	
Business Function	Security Attributes
STANDARD ACCESS	Maintain Login, View Security
VIEW AGY ACC	View Agency Access
VIEW ORG HIER	View Organizational Hierarchy

Security Profile for CQC	
Business Function	Security Attributes
ACCESS ALL CQC	Case Search, Access all in District
CASE/PERS SRCH	Person Search, Case Search
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT DESIGNEES	Maintain Designees
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MERGE/SPLIT	Person Merge/Split, Case Merge Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person - Added in Error
STANDARD ACCESS	

Continued on next page ►

Security Profile for CQC	
Business Function	Security Attributes

(Continued from previous page)

UNIT SUM ACCESS	Unit Summary Access
VIEW AGY ACC	View Agency Access
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for DFY	
Business Function	Security Attributes
ACCESS ALL DFY	Case Search, Access all in District
ACC SERPLAN REV	Access Service Plan Review
CASE/PERS SRCH	Person Search, Case Search
CREATE FSI	Create Family Services Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT CONTRACTS	Maintain Contracts
MAINT DESIGNEES	Maintain Designees
MAINT FAD	Maintain Home
MAINT FAD HIST	Maintain Home History
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT RESOURCES	Maintain Resources
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit

Continued on next page ►

Security Profile for DFY	
Business Function	Security Attributes
<i>(Continued from previous page)</i>	
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person – Added in Error
SIGN CONTRACTS	Sign Contracts,
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW AGY ACC	View Agency Access
VIEW CONTRACTS	View Contracts
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for Local District Offices	
Business Function	Security Attributes
ACCESS ALL DIST	Case Search, Access all in District
ACC SEALED ADOP	Access Sealed Adoption
ACC SERPLAN REV	Access Service Plan Review
APPROVE HP INV	Approve High Priority Investigation
CASE/PERS SRCH	Person Search, Case Search
CREATE FSI	Create Family Services Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT CONTRACTS	Maintain Contracts
MAINT DESIGNEES	Maintain Designees

Continued on next page ►

Security Profile for Local District Offices

Business Function	Security Attributes
<i>(Continued from previous page)</i>	
MAINT FAD	Maintain Home
MAINT FAD HIST	Maintain Home History
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT RESOURCES	Maintain Resources
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MARK SENSITIVE	Mark Sensitive Case
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person - Added in Error
SIGN CONTRACTS	Sign Contracts
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VAC AWARD/CLOSE	Maintain Closed To Intake/CD Awards
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW ADMIN REV	View Admin Review
VIEW AGY ACC	View Agency Access
VIEW CALL LOG	View Call Log
VIEW CONTRACTS	View Contracts
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for OMH	
Business Function	Security Attributes
ACCESS ALL OMH	Case Search, Access all in District
APPROVE IAB INV	Approve IAB Investigation
CASE/PERS SRCH	Person Search, Case Search
CREATE FSI	Create Family Services Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT DESIGNEES	Maintain Designees
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person - Added in Error
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW AGY ACC	View Agency Access
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for OMRDD	
Business Function	Security Attributes
ACCESS ALL OMR	Case Search, Access all in District
APPROVE IAB INV	Approve IAB Investigation
CASE/PERS SRCH	Person Search, Case Search
CREATE FSI	Create Family Services Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT DESIGNEES	Maintain Designees
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person - Added in Error
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW AGY ACC	View Agency Access
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for Regional Offices	
Business Function	Security Attributes
ACCESS ALL CASE	Access all Cases
ACC SERPLAN REV	Access Service Plan Review
APPROVE IAB INV	Approve IAB Investigation
CASE/PERS SRCH	Person Search, Case Search
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT CONTRACTS	Maintain Contracts
MAINT DESIGNEES	Maintain Designees
MAINT FAD	Maintain Home
MAINT FAD HIST	Maintain Home History
MAINT ON-CALL	Maintain On-Call
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT REPD ERR	Maintain Person Role
MAINT RESOURCES	Maintain Resources
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MARK SENSITIVE	Mark Sensitive Case
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person - Added in Error
SIGN CONTRACTS	Sign Contracts
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VAC AWARD/CLOSE	Maintain Closed To Intake/CD Awards
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW ADMIN REV	View Admin Review
VIEW AGY ACC	View Agency Access
VIEW CALL LOG	View Call Log
VIEW CONTRACTS	View Contracts

Continued on next page ►

Security Profile for Regional Offices	
Business Function	Security Attributes

(Continued from previous page)

VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded

Security Profile for State DSS	
Business Function	Security Attributes
ACCESS ALL CASE	Access all Cases
ACC SEALED ADOP	Access Sealed Adoption
ACC SERPLAN REV	Access Service Plan Review
ALL ON-CALL	All On-Call
ALL UNIT SUMMAR	All Unit Summary
APPROVE IAB INV	Approve IAB Investigation
ASSIGN ACC/HIER	Assign Agency Access/Hierarchy
CASE/PERS SRCH	Person Search, Case Search
CPS/IAB INTAKE	CPS/IAB Intake, View Call Log
CREATE FSI	Create Family Services Intake
DEL ALLEGATIONS	Delete Allegations
DELETE INTAKE	Delete Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD INV	Maintain Closed Investigation
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT CONTRACTS	Maintain Contracts, View Contracts
MAINT DESIGNEES	Maintain Designees
MAINT FAD	Maintain Home
MAINT FAD HIST	Maintain Home History
MAINT ON-CALL	Maintain On-Call
MAINT PAY IND	Maintain Payment Indicators

Continued on next page ►

Security Profile for State DSS

Business Function	Security Attributes
-------------------	---------------------

(Continued from previous page)

MAINT REPD ERR	Maintain Person Role
MAINT RESOURCES	Maintain Resources
MAINT SECURITY	Maintain Security, Maintain Login, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
MARK INTAKE DEL	Mark Intake for Deletion
MARK SENSITIVE	Mark Sensitive Case
MERGE/SPLIT	Person Merge/Split, Case Merge/Split
OPEN ADMIN REVW	Open Admin Review
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person – Added in Error
SCR CLRNCE/RFI	SCR Clearance, RFI
SCR SUPERVISOR	SCR Supervisor
SECURITY ADMIN	Maintain Business Functions, Maintain Security, Maintain Login
SIGN CONTRACTS	Sign Contracts
STANDARD ACCESS	
SUPER USER	
UNIT SUM ACCESS	Unit Summary Access
VAC AWARD/CLOSE	Maintain Closed To Intake/CD Awards
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW ADMIN REV	View Admin Review
VIEW AGY ACC	View Agency Access
VIEW CALL LOG	View Call Log
VIEW CONTRACTS	View Contracts
VIEW INDICATED	View Indicated
VIEW ORG HIER	View Organizational Hierarchy
VIEW RPTR/SOURC	View Reporter/Source
VIEW SECURITY	View Security
VIEW SENSITIVE	View Sensitive Case
VIEW UNDER INV	View Under Investigation
VIEW UNFOUNDED	View Unfounded
WITHDRAW ALLEGA	Withdraw Allegations

Security Profile for Voluntary Agencies	
Business Function	Security Attributes
ACC SERPLAN REV	Access Service Plan Review
ACCESS ALL AGY	Case Search, Access all in District
ACC SEALED ADOP	Access Sealed Adoption
CASE SEARCH	Case Search
CREATE FSI	Create Family Services Intake
ENTER PROG NOTE	Enter Progress Notes
MAINT AGY ACC	Maintain Agency Access
MAINT CLSD PERS	Maintain Closed Person Demographics
MAINT DESIGNEES	Maintain Designees
MAINT FAD	Maintain Home
MAINT FAD HIST	Maintain Home History
MAINT ORG HIER	Maintain Organizational Hierarchy
MAINT SECURITY	Maintain Security, View Business Functions
MAINTAIN OFFICE	Maintain Office
MAINTAIN STAFF	Maintain Staff
MAINTAIN UNIT	Maintain Unit
PERSON SEARCH	Person Search
PERSON UNRELATE	Person Unrelate
REM PER ADD ERR	Remove Person – Added in Error
STANDARD ACCESS	
UNIT SUM ACCESS	Unit Summary Access
VACANCY MAINT	Bed Maintenance
VACANCY SEARCH	Vacancy Control Search
VIEW AGY ACC	View Agency Access
VIEW ORG HIER	View Organizational Hierarchy
VIEW SECURITY	View Security

Appendix E: Job Types

State Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Administrative Staff Commissioner's Staff Legal Support Staff SCR 6 & 9 SCR Support Staff	Administrator Adoption Services Assoc. Commissioner Attorney Auditor Budget Manager Clerical Support Commissioner Deputy Commissioner Fiscal Staff Interstate Compact Staff Program Director Program Staff Quality Control Rate Setting SCR Admin Review SCR CPS 1 SCR CPS 2 SCR CPS 3 State Adoption Services Technical Support Staff

Regional Office Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Administrative Support	Adoption Specialist BECS Licensing Staff BECS Licensing Supervisor BECS Regional Director Connections Implementation County Lead County Lead Supervisor IAB Investigator IAB Supervisor Regional Office Director VA Lead VA Lead Supervisor

LDSS Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Accounting Clerk	Accounting Supervisor
Clerical Staff	Administrative Staff
Commissioner's Staff	Adoption Caseworker
Legal/Court Support Staff	Adoption Director
Support Staff	Adoption Supervisor
	Assistant Commissioner
	Attorney
	Auditor
	Caseworker
	Child Protective Caseworker
	Child Protective Director
	Child Protective Supervisor
	Commissioner
	Contract Manager
	Director of Services
	Fiscal Staff
	Foster Care Caseworker
	Foster Care Director
	Foster Care Supervisor
	Home Finder
	Home Finding Supervisor
	Interstate Compact
	Preventive Caseworker
	Preventive Services Director
	Preventive Supervisor
	Quality Control Staff
	Senior Caseworker
	Senior Welfare Examiner
	Social Worker/Clinician
	Staff Development
	Welfare Examiner

Voluntary Agency Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Accounting Clerk Clerical Staff Legal/Court Support Staff Support Staff	Accounting Supervisor Administrative Staff Adoption Caseworker Adoption Director Adoption Supervisor Asst. Executive Director Attorney Auditor Bureau Director/Head Case/Program Aide Caseworker Executive Director Executive Director's Staff Fiscal Staff Foster Care Director Foster Care Caseworker Foster Care Supervisor Home Finder Home Finding Supervisor Preventive Caseworker Preventive Services Director Preventive Services Supervisor Program Director Quality Control Staff Senior Caseworker Social Worker/Clinician Staff Development Supervisor Youth Counselor

OMH Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Account Clerk Administrative Support Staff Clerical Staff Staff Development Support Staff	Commissioner's Office Contract Manager CPS Investigator CPS Supervisor Director Fiscal Staff Foster Care Services Home Finder Interstate Compact Legal Quality Control Senior Youth Counselor Social Worker/Clinician Youth Counselor

OMRDD Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Account Clerk Administrative Support Staff Clerical Staff Staff Development	Commissioner's Office Contract Manager CPS Investigator CPS Supervisor Director Foster Care Services Home Finder Interstate Compact Legal Quality Control Senior Youth Counselor Social Worker/Clinician Youth Counselor

CQC Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Administrative Support Staff	Commissioner's Office Director IAB Investigator IAB Supervisor Quality Control

DFY Job Types	
<i>Clerical</i>	<i>Non-Clerical</i>
Account Clerk Administrative Support Staff Clerical Staff Support Staff	Contract Manager CPS Investigator CPS Supervisor Facility Director Fiscal Staff Foster Care Services Home Finder Interstate Compact Legal Quality Control Senior Youth Counselor Social Worker/Clinician Staff Development Youth Counselor

Appendix F: Business Functions Guidelines

BUSINESS FUNCTIONS FOR THE FOLLOWING OFFICE TYPES:

State, Regional, CCF, CQC, District, DFY, Voluntary Agency, OMH, OMRDD

To be assigned at the discretion of the agency.

Business Function	Security Attribute	Description	Recommendation	Comments
MAINT ORG HIER	Maintain Organizational Hierarchy	<p>This Business Function allows a worker to maintain the organizational hierarchy that is displayed for the worker's District/ Agency.</p> <p>Organizational Hierarchy works in conjunction with the <i>Agency Access</i> window.</p> <p>Changing a unit's position within the organizational hierarchy of the District/Agency offers the ability to implicitly grant security access rights to individuals at higher management levels. Anyone in an organization in a direct supervisory line above a worker with a role in a case can have access to that case, if that option is chosen on the <i>Agency Access</i> window.</p> <p>This new functionality will only apply to new Case and Financial Management (FSI/ FSS stages), but all units will be displayed and can be moved.</p> <p>Right clicking on the unit and dragging and dropping it to the subordinate or supervisory position changes a Unit's position.</p> <p>The supervisory unit field on the <i>Unit List</i> window will be blank until supervisory changes are made in the <i>Organization Hierarchy</i> window. Only then will the Supervisory Unit display.</p>	<p>Only State CONNECTIONS staff with the ASSIGN ACC/ HIER BF can assign this Business Function.</p> <p>Locally designated workers in each District/ Agency with this Business Function will be able to maintain the <i>Organizational Hierarchy</i> window for their District/ Agency.</p>	<p>Visible on the <i>Staff Security</i> window only if this Business Function is assigned to a worker.</p>
VIEW ORG HIER	View Organizational Hierarchy	<p>The organizational hierarchy is displayed for the user's District/Agency with all the units for their own District/Agency.</p> <p>Organizational Hierarchy works in conjunction with the <i>Agency Access</i> window.</p> <p>This new functionality will only apply to the new Case and Financial Management (FSI/ FSS) stages but all units will be displayed.</p> <p>The supervisory unit field on the <i>Unit List</i> window will be blank until supervisory changes are made in the <i>Organization Hierarchy</i> window; only then will the Supervisory Unit display.</p>	<p>Locally designated workers in each District/ Agency with this Business Function will be able to view the <i>Organizational Hierarchy</i> window for their District/Agency.</p> <p>Only staff with the MAINT SECURITY BF can assign this Business Function.</p>	

**BUSINESS FUNCTIONS FOR THE FOLLOWING OFFICE TYPES:
 State, Regional, CCF, CQC, District, DFY, Voluntary Agency, OMH, OMRDD**
To be assigned at the discretion of the agency.

Business Function	Security Attribute	Description	Recommendation	Comments
MAINT AGY ACC	Maintain Agency Access	<p>In the <i>Agency Access</i> window, security access is maintained for each District/Agency. District/Agency staff may be granted View privileges, Maintain privileges or no privileges for each staff grouping (Case Assignable Staff, Unit Supervisor, Direct Supervisory Line.)</p> <p>This new functionality will only apply to the new Case and Financial Management (FSI/ FSS) stages.</p>	<p>Only State CONNECTIONS staff with the ASSIGN ACC/HIER Business Function can assign this Business Function.</p> <p>Locally designated workers in each District/ Agency, with this Business Function, will be the only workers able to maintain the <i>Agency Access</i> window for their District/Agency.</p> <p>This is a very powerful Business Function that can allow a great deal of access to a large number of workers. It is very important that a District/Agency designate someone to perform this function who understands Security.</p> <p>It is recommended that this BF only be given to two or three staff in a District/Agency.</p>	Visible on the <i>Staff Security</i> window only if this Business Function assigned to the worker.
VIEW AGY ACC	View Agency Access	<p>Workers in a District/Agency with the proper security will be given access to view the <i>Agency Access</i> window for their District/Agency.</p> <p>This functionality only applies to the new Case and Financial Management (FSI/ FSS) stages.</p>	<p>Only staff with the MAINT SECURITY BF can assign this Business Function.</p> <p>Locally designated workers in each District/Agency, with this BF, will be able to view the <i>Agency Access</i> window for their own District/Agency.</p>	

SYSTEM BUILD 18 BUSINESS FUNCTIONS

To be assigned at the discretion of the agency. See the table below for which Office Type(s) can be assigned these Business Functions.

Although these BFs are in Production now and can be assigned now (in preparation for Build 18), they do not provide any additional system access or functionality until Build 18 is implemented, based on the phased implementation schedule.

Business Function	Security Attribute	Description	Recommendation	Comments
ACC SEALED ADOP	Access Sealed Adoption	<p>The assignment of the Business Function ACC SEALED ADOP will allow a user to access a Child Case Record that has been sealed due to the finalization of an adoption.</p> <p>A Child Case Record (CCR) is created when the child is completely legally freed and the Case Manager checks the Completely Freed for Adoption (Create Child Case Record) check box on the Placement Information tab on the <i>Tracked Children Detail</i> window.</p> <p>The adoption is sealed once the <i>Finalize Adoption</i> window is completed and saved; however, the CCR stage can then remain open or be closed.</p> <p>CCR Stage Remains Open:</p> <p>The <i>Finalize Adoption</i> window has been completed and saved, and stage is still Open.</p> <p>The Case Manager (always a local district worker) assigned to the stage is:</p> <ul style="list-style-type: none"> the only person who does not need the Business Function to access the <i>Finalize Adoption</i> window, the only one who can modify the window. <p>A worker with the Business Function and access to the stage:</p> <ul style="list-style-type: none"> can access the <i>Finalize Adoption</i> window; can only access the window in view-only mode; a worker who could otherwise access the stage, but without the Business Function cannot access the <i>Finalize Adoption</i> window. 	<p>It is recommended that only staff who are Adoption supervisors or those with a specific need to see sealed adoptions be given this Business Function. The Security Coordinator needs to give careful consideration when assigning this Business Function, as there are strict confidentiality laws and regulations regarding sealed adoptions.</p> <p>There should be a regular review of the staff that have this Business function to be sure that it is necessary for all workers who are assigned this BF.</p> <p>Please note: The process to finalize an adoption can be completed without the ACC SEALED ADOPTION Business Function.</p> <p>It is <i>strongly</i> recommended that the CCR stage be closed when the <i>Finalize Adoption</i> window is completed and saved.</p>	<p>If there is an Open or Closed CCR stage for which the <i>Finalize Adoption</i> window has not been completed (the worker does not yet have all of the information to complete the finalization, the child's goal changed or the adoption was never completed) and saved, then the stage is not sealed, so the Business Function ACC SEALED ADOP does not apply. These stages are treated like all other foster care cases.</p>

Business Function	Security Attribute	Description	Recommendation	Comments
ACC SEALED ADOP (con't)		<p>CCR Stage is Closed:</p> <p>The <i>Finalize Adoption</i> window has been completed and saved, and the CCR stage has been closed.</p> <ul style="list-style-type: none"> Workers MUST have access to the stage (through View all in District, Historical Access or Agency Access) and the BF to access a Sealed Adoption stage. Workers who were assigned to the stage at one time, and unassigned prior to stage closure, will be able to view the window if they have the BF. 		
ACC SERPLAN REV	Access Service Plan Review	<p>The assignment of the Business Function ACC SERPLAN REV will permit staff the ability to create and/or modify Service Plan Review information. The new BF allows a clerical or any other worker access to <i>only</i> the Service Plan Review functionality.</p> <p>The worker assigned this Business Function, without a role in the stage, gains access to the Service Plan Review from the <i>Case Search</i> window, but will not have access to other information within the Family Services Stage.</p>	It is recommended that this Business Function be assigned to clerical or other workers who are responsible for Service Plan Reviews.	<p>Please note that the following workers will have the ability to create and modify Service Plan Reviews without the Business Function ACC SERPLAN REV:</p> <ul style="list-style-type: none"> Assigned workers having a role in the stage; Any worker who is in the assigned worker's unit hierarchy; or Any worker who has access to the <i>Assigned Workload</i> of a worker with a role in the case as a result of access granted through the <i>Agency Access</i> window.

Business Function	Security Attribute	Description	Recommendation	Comments
CREATE FSI	Create Family Services Intake	<p>Allows a worker to create a Family Services Intake from the CONNECTIONS Toolbar.</p> <p>Please note: A voluntary agency worker must submit an FSI to an LDSS worker for acceptance.</p>	<p>Recommended for all workers who are responsible for the processing and creation of Family Services Intakes within CONNECTIONS.</p>	<p>Any worker with a role in the stage, or anyone who has access to the <i>Assigned Workload</i> of a worker with a role in the stage, may modify an FSI.</p> <p>A worker can always access any case on his/her <i>Assigned Workload</i> if it is marked as Sensitive whether it is marked Sensitive.</p>
ENTER PROG NOTE	Enter Progress Notes	<p>A worker who is assigned the ENTER PROG NOTE Business Function, and has no other access to a stage, will have the ability to access, view and maintain Progress Notes; however, the access will only be to the Progress Notes tab.</p>	<p>It is recommended that this Business Function be given to workers who need to record progress notes and do not have a role in the stage, such as clerical staff.</p> <p>The worker's role in the stage and his/her need to complete certain tasks dictates the rights that are assigned to that worker.</p> <p>There are three distinct security rights that workers need in order to <i>create</i> progress notes:</p> <ul style="list-style-type: none"> • assigned a role in the stage; • within the assigned worker's unit hierarchy; • assigned the ENTER PROG NOTE Business Function, or • assigned a Progress Note Task To-Do. 	<p>Please see the <i>CONNECTIONS Case Management Step-by-Step Guide</i> for more information on Progress Notes.</p>

Business Function	Security Attribute	Description	Recommendation	Comments
ENTER PROG NOTE (con't)			<p>In order to <i>modify</i> notes a worker must be:</p> <ul style="list-style-type: none"> • the progress note's Author; or • the progress note's Entered By person. 	
PERSON SEARCH	Person Search	This BF allows workers to perform statewide person searches from the CONNECTIONS Toolbar.	It is recommended that this Business Function be assigned to individuals who may need to perform searches outside of working within a case.	<p>Any worker in the process of opening a case, or adding a new person to an existing case, will have the capability to perform a person search without this Business Function. Any person search action returns the following information:</p> <ul style="list-style-type: none"> • Name • Sex • DOB • Case Stage • Stage Status • Assigned Worker • Workers Office • Workers Phone Number

	BUSINESS FUNCTION					
		Acc Sealed Adop	Acc Serplan Rev	Create FSI	Enter Prog Note	Person Search
OFFICE TYPE	CCF					
	CQC				✓	
	DFY		✓	✓	✓	
	District	✓	✓	✓	✓	✓
	OMH			✓	✓	
	OMRDD			✓	✓	
	Regional		✓		✓	
	State	✓	✓	✓	✓	
	Voluntary Agency	✓	✓	✓	✓	✓

Appendix G: Security Report Samples

Staff Security Report as an Adobe Acrobat (.pdf) file:

Staff Security Report							Date: 10/7/2002
Agency Name: <i>Mohawk County Dss A90</i>				As of: <i>05/16/2002</i>			
Name	NT Login	Unit Approver ?	Staff Role	Business Functions	Assignee or Designee ?	Case Assignable ?	
Site: <i>3#0</i> Unit: <i>001</i>							
Coverdale, Claudia	981518	No	Worker	CASE/PERS SRCH MAINT CLSD ADPT MAINT FAD MAINT FAD HIST STANDARD ACCESS VAC AWARD/CLOSE VACANCY MAINT VACANCY SEARCH VIEW ADPT CHILD VIEW PAY HISTRY VIEW SEAL ADOPT	No	Yes	
Doe, Cathy	981132	No	Worker	ACCESS ALL DIST CASE FILE LOCAT CASE/PERS SRCH MAINT CLSD ADPT	No	Yes	

Staff Security Report as a Microsoft Excel file:

	A	B	C	D	E	F	G	H	I	J	K
	Agency Name	Site	Unit	Name	NT Login	Unit Approver ?	Staff Role	Business Functions	Assignee or Designee ?	Case Assignable ?	Conn As Of Dt
1	DSS	051	NO3	May, Sally	1623WWW	No	Worker	ACCESS	No	No	11/21/02 0:38
2	DSS	051	NO3	May, Sally	1623WWW	No	Worker	CASE/PE	No	No	11/21/02 0:38
3	DSS	051	NO3	May, Sally	1623WWW	No	Worker	STANDAR	No	No	11/21/02 0:38
4	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW AD	No	No	11/21/02 0:38
5	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW CAL	No	No	11/21/02 0:38
6	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW CO	No	No	11/21/02 0:38
7	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW IND	No	No	11/21/02 0:38
8	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW RPT	No	No	11/21/02 0:38
9	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW SEC	No	No	11/21/02 0:38
10	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW SE	No	No	11/21/02 0:38
11	DSS	051	NO3	May, Sally	1623WWW	No	Worker	VIEW UN	No	No	11/21/02 0:38
12	DSS	051	NO3	Jay, John	1623WWW	No	Worker	ACCESS	No	No	11/21/02 0:38
13	DSS	051	NO3	Jay, John	1622WWW	No	Worker	ACCESS	No	No	11/21/02 0:38
14	DSS	051	NO3	Day, Pete	1622WWW	No	Worker	CASE/PE	No	No	11/21/02 0:38
15	DSS	051	NO3	Day, Pete	1622WWW	No	Worker	STANDAR	No	No	11/21/02 0:38
16	DSS	051	NO3	Day, Pete	1622WWW	No	Worker	VIEW AD	No	No	11/21/02 0:38
17	DSS	051	NO3	Day, Pete	1622WWW	No	Worker	VIEW CAL	No	No	11/21/02 0:38
18	DSS	051	NO3	Day, Pete	1622WWW	No	Worker	VIEW CO	No	No	11/21/02 0:38
19											

Business Function Report as a .pdf file:

As of: 05/16/2002		Business Function Report		Date: 10/7/2002
Staff Name		Unit	Designee	Unit
Agency Name: Mohawk County Dss				
Agency Code: A90				
			Office Type: District	
Business Function: ACCESS ALL DIST				
Site: 3H0				
Barnham,Brenda	003			
Barnham,Judy	002			
Barnham,Michael	002			
Coverdale,Christine	005			
Coverdale,Michelle	006			
Coverdale,Robert	160			
Doe,Cathy	001			
Doe,Ron	007			
Fletcher,Stacia	003	Spencer,Laurie		003
Grimsby,Jana	006			
Grimsby,Lee	014			
Harding,Andrew	005			
Harding,Lisa	160			
Kennedy,Nigel	053			
Lawrence,David	005			
Lawrence,Michelle	006			
Mitchell,James	005			
Peters,Anthony	006			
Peters,Cindy	002			
Peters,Donna	ILW			

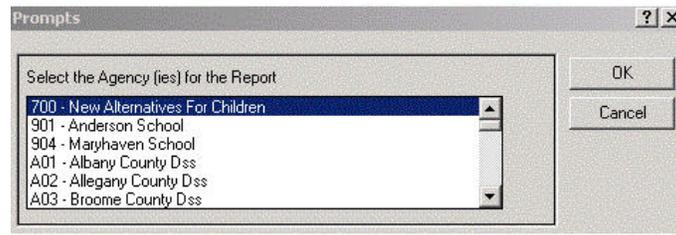
Assignee/Designee Report as a .pdf file:

As of: 05/16/2002		Date: 10/7/2002					
Assignee/Designee Report							
Agency Name: Mohawk County Dss							
Agency Code: A90							
Staff Name	Unit	Assignee	Unit	Date Expires	Designee	Unit	Date Expires
Fletcher,Stacia	003	Spencer,Laurie	003	01/03/2003			
Spencer,Laurie	003				Fletcher,Stacia	003	01/03/2003

Unit Approver Report as a .pdf file:

Unit Approver Report		Date: 10/7/2002
Agency Name: Mohawk County Dss		As of: 05/16/2002
Agency Code: A90		
Staff Name	Approver of Unit	In/Out Assigned
Barnham,Judy	002	In
Doe,Gracelyn	001	Out
Doe,Ron	007	In
Harding,Lisa	160	In
Kennedy,Melanie	005	Out
Kennedy,Nigel	053	In
Kennedy,Thomas	014	Out
Lawrence,Michelle	006	In
Mitchell,Nancy	004	Out
Peters,Donna	ILW	In
	010	Out
Peters,Kathleen	065	In
Peters,Lynne	STF	In
Spencer,Laurie	003	In
Spencer,Steven	008	In

Organizational Hierarchy report Prompt:



Organizational Hierarchy report as a .pdf file:

No Hierarchy Entered

Parent
(3Q1) ACA - Deputy Commission
(3Q1) ACB - Other
(3Q1) ACC - Financial/Claims
(3Q1) ADD - Administration
(3Q1) ADP - Adoption
(3Q1) ALB - Other
(3Q1) AMA - Administration
(3Q1) AMB - Other
(3Q1) AMC - Administration
(3Q1) C96 - Conversion
(3Q1) C97 - Conversion
(3Q1) CPA - Administration
(3Q1) CPB - Support
(3Q1) CPC - Child Prot Services
(3Q1) CPD - Child Prot Services
(3Q1) CPE - Child Prot Services
(3Q1) CPF - Child Prot Services
(3Q1) CPG - Child Prot Services
(3Q1) CPH - Child Prot Services

Appendix H: Information Resources

You can get additional information about topics covered in this guide from the following sources:

Exchange Address Book

The Global Address List in the Exchange address book contains distribution lists for Security Coordinators:

Listing	Definition
CONX-ACS-App-Sec-Coord	Security Coordinators for ACS
CONX-ACS-Backup-Sec-Coord	Backup Security Coordinators for ACS
CONX-App-Sec-Coord	An all-inclusive listing of all Security Coordinators
CONX-Backup-Sec-Coord	An all-inclusive listing of all Backup Security Coordinators
CONX-LDSS-App-Sec-Coord	Security Coordinators for Local Districts
CONX-LDSS-Backup-Sec-Coord	Backup Security Coordinators for Local Districts
CONX-State-App-Sec-Coord	State & Regional Office Security Coordinators
CONX-State-Backup-Sec-Coord	State & Regional Office Backup Security Coordinators
CONX-VA-App-Sec-Coord	Security Coordinators for Voluntary Agencies
CONX-VA-Backup-Sec-Coord	Backup Security Coordinators for Voluntary Agencies

The OCFS CONNECTIONS Intranet site

The OCFS CONNECTIONS intranet site includes:

- A copy of the *Security Step-By-Step Guide*
- Information about other CONNECTIONS trainings
- The CONNECTIONS Security page, which includes:
 - Listings of all CONNECTIONS Business Functions, organized by office type
 - Overview and instructions for Security Reports from the Data Warehouse
 - Additional up-to-the-minute information for Security Coordinators



Step-by-Step: Accessing the CONNECTIONS Security Page

- 1 Open Internet Explorer by clicking on the  icon in the quick start tray at the left end of the Task Bar.
The Internet Explorer window displays.
- 2 If the browser does not display the OCFS intranet site automatically, enter *http://ocfs.state.nyenet* into the browser's address line and press the **Enter** key on your keyboard.
The OCFS intranet site home page displays.
- 3 Click on the **CONNECTIONS** link.
The OCFS CONNECTIONS intranet site home page displays.
- 4 Click on the **Security** link.
The CONNECTIONS Security page displays.
- 5 To close Internet Explorer, click on the **File** menu and select **Close**.

CONNECTIONS Online Help

Context-sensitive help information is available for all elements of CONNECTIONS windows, including tabs, grids, buttons, and individual fields. Click on an element to make it “active” and press the **F1** key on your keyboard. Information about that element of the window will display.

Pressing **F1** displays the Help system window. Information specific to the window element that was active when **F1** was pressed will display.

Besides context-sensitive Help information on window elements such as fields, tabs, and buttons, the Help system includes the following:

- **“How Do I?”**
Information on how to perform various tasks in CONNECTIONS.
- **Guidelines**
Background on the legal, policy, and procedural guidelines followed by workers as they develop and record information in the LDM window.
- **Help on Help**
Instructions on how to use the LDM Online Help system.

Appendix I: Frequently Asked Questions

How do I end-date a worker who has left my Agency?

Workers are end-dated by selecting **Staff** on the **Maintain** menu of the CONNECTIONS Toolbar, conducting a staff search, and then using the *Staff Detail* window for the worker to be end-dated.

For details:	See "End-Dating Staff" in Module 7.
--------------	-------------------------------------

How do I re-assign stages from one workload to another?

Stages are re-assigned using the *Assign* window, which is accessed from the Assigned Workload from which stages are being re-assigned.

For details:	See "Reassigning Stages from a Workload" in Module 7.
--------------	---

How do I move a new worker into a new Unit?

Assigning a worker to a unit is done by selecting **Unit** on the **Maintain** menu of the CONNECTIONS Toolbar and using the *Unit List* and *Unit Detail* windows.

For details:	See Module 6, "Adding Staff in CONNECTIONS."
--------------	--

How do I update a worker's Business Function Profile?

Workers' Business Functions are updated by selecting **Staff Security** on the **Maintain** menu of the CONNECTIONS Toolbar and using the *Staff Security* window.

For details:	See "Assigning Additional Business Functions" and "Removing Business Functions from a Business Function Profile" in Module 7.
--------------	---

How do I change the specialization of Units in my Agency?

Unit Specialization is changed by selecting **Unit** on the **Maintain** menu of the CONNECTIONS Toolbar and using the *Unit List* and *Unit Detail* windows.

For details:	See "Changing a Unit's Specialization" in Module 8.
--------------	---

What does the Unit hierarchy mean in terms of functionality and ability to access stages?

Within a unit, staff is organized in a hierarchy (from lowest to highest) of Workers, Supervisors, Maintainers, and Managers. This allows some individuals within the unit increased access based on their role within the unit. CONNECTIONS will check when a worker attempts to access or perform particular functions in certain windows to make sure the worker has a particular role in the unit hierarchy. Examples of this type of window are: *Assign*, *Case List*, and *Assigned Workload*.

For details:	See "Definitions and Descriptions of Organizational Concepts" in Module 3 and "Main Routes of Stage Access" in Module 4.
--------------	--

How do I update staff names in CONNECTIONS?

Staff names are changed by selecting **Staff** on the **Maintain** menu of the CONNECTIONS Toolbar and using the *Staff Detail* window.

For details:	See "Updating Staff Names" in Module 7.
--------------	---

How do I reinstate a worker who is returning to my Agency?

Workers are reinstated by selecting **Staff** on the **Maintain** menu of the CONNECTIONS Toolbar and using the *Staff Detail* window.

For details:	See "Reinstating Staff" in Module 7.
--------------	--------------------------------------

How do I delete un-needed units from my Agency?

Units are deleted by selecting **Unit** on the **Maintain** menu of the CONNECTIONS toolbar and using the *Unit List* window. All In-Assigned staff must be moved to other units or end-dated, as appropriate.

For details:	See "Deleting a Unit" in Module 8.
--------------	------------------------------------

What do I do if a worker receives the message, "You are not a registered user of CONNECTIONS"?

Do a staff search from the CONNECTIONS Toolbar to make sure the worker has CONNECTIONS access. If not, the worker must be given standard CONNECTIONS access through WEBSTAR. If the worker does appear in a staff search, make sure the NT logon displays correctly in the *Staff Security* window. Your agency's LAN administrator is a good source of assistance for these types of problems.

For details:	See Module 2, "System and Application Access."
--------------	--

Appendix J: OCFS Security Guidelines



OCFS Security Guidelines



Safe Computing Practices

- 🔒 **Be responsible**—Download *only* authorized, work-related executables or documents from the Internet that are from trusted sources **and** that your LAN/Security Administrator has approved. *Never* use commercial e-mail accounts (such as AOL, Hotmail or Yahoo), Instant Messaging, chat rooms or other third-party services on a state computer without prior *written* authorization.
- 🔒 **Be professional**—*Never* use state e-mail services for prohibited activities, including (but not limited to): sharing jokes or any other non-work-related materials; transmitting illegal, offensive or threatening items; and soliciting for unauthorized causes or activities. In addition to being prohibited, these unnecessary electronic transmissions crowd network bandwidth and occupy server capacity needed for legitimate business purposes.
- 🔒 **Be alert** and *immediately* report any suspected virus infection or other system compromise to your LAN/Security Administrator *and* to the OCFS Information Security Officer (Jo Shrader). Proper reporting speeds reaction, recovery and damage control. Be sure you know who your LAN/Security Administrator is *before* you need to contact him/her.
- 🔒 **Be consistent** in complying with the same safety procedures when using remote access or transporting files between PCs via a floppy disk or CD. If you move disks between your home and work PCs, make sure you have up-to-date anti-virus software on your home PC and regularly scan disks and CDs. Viruses can easily be brought into the state network through a laptop, home PC or storage media.
- 🔒 **Be suspicious** of e-mail you weren't expecting, even if it's from someone you know. Computer viruses often send e-mails to all contacts in an unsuspecting sender's address book. *Before* you open the e-mail, call the source to verify that s/he intentionally sent the e-mail.

- 🔒 **NEVER run/download/forward unsolicited files** (e.g., executables, documents, spreadsheets). Any programs that run or execute on your PC must be virus-checked and approved by your LAN/Security Administrator first. *Never* open *any* file with a double file extension (e.g., iamavirus.txt.vbs).
- 🔒 **NEVER forward virus warnings to anyone**
Contact your LAN/Security Administrator to determine how to proceed. (If your LAN/Security Administrator is not available, contact the Help Desk.) Forwarding these items increases risk and creates additional network traffic.
- 🔒 **NEVER attempt to test system weaknesses or vulnerabilities** unless you are specifically authorized to do so.
- 🔒 **ALWAYS leave your PC powered on (being sure to log off, as appropriate)**
This will ensure that your PC will receive security patches. Click on **Start > Shut Down > Log Off** to log off your computer *without* powering off.

Anti-virus software helps protect against computer viruses, but does NOT replace conscious, consistent adherence to established safety procedures.

***If you think your computer may have been exposed to a virus, DON'T PANIC!
Contact your LAN/Security Administrator IMMEDIATELY.***



OCFS Security Guidelines



Protecting Your Password

🔒 **Make it difficult**

Select a password that is easy for you to remember, but difficult for others to guess. Don't be stingy—make your password as long as possible (at least 8 characters and up to a maximum of 13 characters), in order to help reduce the likelihood of allowing someone to guess it. You cannot use all or part of your logon ID in your password, nor can you reuse any of your last 13 passwords.

🔒 **Mix it up**

Your OCFS password *must* contain *at least* one uppercase letter, one lowercase letter *and* one number. CONNECTIONS users must *never* use symbols in their passwords.

🔒 **Keep it to yourself**

Don't share your password with others. Never display your password; if you need to write it down, don't keep the information at your desk or anywhere it can be easily seen by others.

🔒 **Embrace change**

You must change your password periodically—*at least* once every 90 days. If you think your password has been compromised, *change it immediately*. (Don't forget to report the situation to your LAN/Security Administrator as soon as possible!)

🔒 **Be yourself**

Use *only* your logon ID and password; *never* use a current or former co-worker's ID or password.

🔒 **Let your fingers do the walking**

Never store passwords in macros or automatic log-on features. Enter your password manually every time.

Your unique User ID and password not only provide you with “keys” to access the OCFS network (including CONNECTIONS, as applicable), they also serve as a form of identification—linking you to your actions in the system.

YOU are responsible for actions taken with your User ID and password! Always follow established password protocols to help prevent unauthorized use of your User ID and password.

If you think your password has been compromised, change it immediately AND report the situation to your LAN/Security Administrator.

Security is everyone's responsibility!

These guidelines are advisable for *all* of your passwords.



OCFS Security Guidelines



Protecting Confidential Information

Maintain confidentiality 24/7

Protecting confidential information encompasses all spoken, handwritten, printed and electronically transmitted notes and communications. When you make case visits, be sure to keep client-identifiable casework documentation with you at all times and *never* allow unauthorized individuals to view the information. Remember that all case and system information must be used *only* for legitimate business purposes. If you must keep hard copies of confidential information at your desk, *always* lock your desk whenever you are away from it. If hard copies need to be discarded, *always* run them through a cross-cut shredder.

Don't kick this habit

It's easy to become complacent or to think, "I'll only be away from my computer for a few minutes." If you are logged on to the system, *always* lock your computer (or log off the network) by holding down the **Ctrl+Alt+Del** keys at the same time. Do this *every time* you leave your desk; this helps prevent unauthorized individuals from using your User ID and password to access the network. *80% of security breaches are unauthorized people using an authorized user's computer, NOT hacking in from outside.*

Hit the road, but...

Be particularly careful when using portable electronic devices, such as laptop computers, Quick Pads, voice recorders and PDAs. Don't leave confidential information on these devices longer than is absolutely necessary. If the device has the ability to transmit information, avoid transmitting confidential information over wireless connections or unsecured public connections. When traveling with the device, keep it with you at all times; *never* check it into airline luggage systems.

Exercise care with voicemail and e-mail

When conducting casework or other legitimate business contacts by phone, it's inevitable that you may sometimes need to leave a voicemail message or send an e-mail to a contact. *Never* include confidential information in voicemail you leave or e-mail you send.

Don't convey confidential information where others can intercept it

Caseworkers have an obligation to preserve the confidentiality rights of the children and families with whom they work. Other staff may also have legitimate access to this information. If you must discuss confidential information on the phone, avoid areas where your conversation can be overheard. Remember that cellular phone lines are not sufficiently secure to be appropriate when discussing confidential information. *Never* save confidential information to the hard drive of *any* desktop computer. Check the permission levels on your Microsoft Outlook folders; make sure you understand what each level of access means and assign permissions on a need-to-know basis *only*.

The walls have ears

Be mindful of protecting confidential information in areas where you can be easily overheard, such as in cubicle areas.

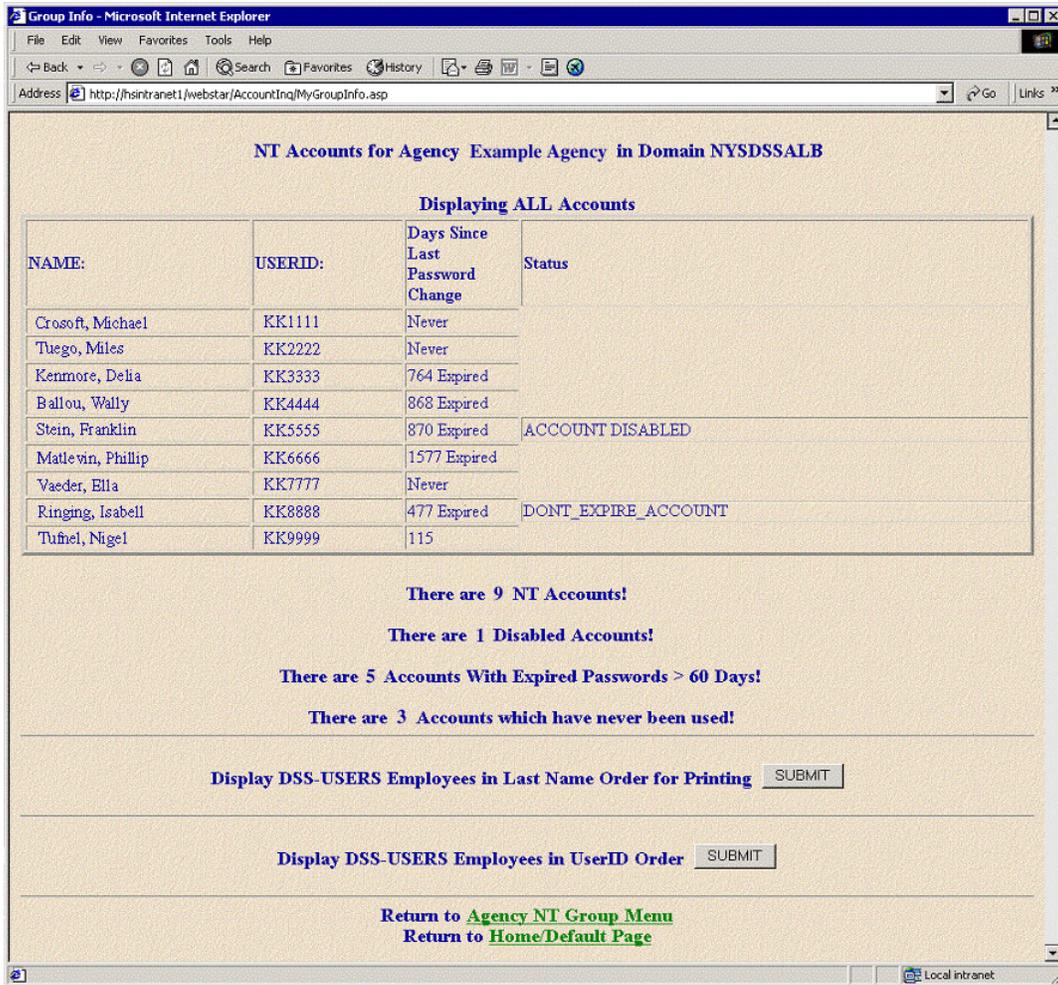
Use follow-through when faxing

If you need to transmit any confidential information via fax, call first *before* sending the fax, in order to alert the intended recipient that you are sending a fax. Be sure to call the recipient afterward, too, to verify that the fax was received *and* that it was not left on the fax machine. Avoid faxing confidential information whenever possible.

Security is everyone's responsibility.

Always follow established security protocols to help protect confidential information.

Appendix K: The WEBSTAR Agency Users Report



Definitions of Entries in “Days since Last Password Change” and “Status” Columns:

Entry	Definition
###	The account is active. “###” represents the number of days since the last password change.
Never	No password was ever set by the user. This could be a very new account, but in most cases it is an old account that has never been used.
### Expired	A password must be reset every 180 days. If 180 days pass without a reset, the password expires 60 days later. “###” represents the number of days since the password was last reset. A worker can reset an expired password as long as the account is not disabled.

Continued on next page ►

Entry	Definition
### Expired ACCOUNT DISABLED	Accounts are disabled by the district/agency. A disabled account can be re-enabled by the NT Security Coordinator. The worker then needs to reset the password in order to be able to use the account.
DON'T EXPIRE ACCOUNT	Allows an account (such as that of an NT Security Coordinator) not to expire even if the is not reset within 240 days. The account can be disabled.
Account Deleted (Not on Report)	The district/agency has deleted the account, the mailbox is gone, and there is no longer any connection between the account and the original district/agency.