Security for CONNECTIONS Case Management
SELF-ASSESSMENT

## Background

The enhancements to CONNECTIONS Security that are being released with Build 17 apply to the new CONNECTIONS Case and Financial Management functions (Family Services Intake, Family Services Stage) that will be implemented in Builds 18-19; these enhancements **will not** affect security for CPS Intake, CPS Investigation or FAD stages. The earlier release of the security functionality enables local districts and agencies to organize their security structure before implementation of the larger case management system.

Build 17 introduces two new windows – Agency Access and Organizational Hierarchy – that will enable districts and agencies to more easily give workers, supervisors and administrators the ability to view and/or maintain cases in which they do not have a direct role. Expanded access may be granted vertically within the organization as well as horizontally to the levels of unit, job function or agency-wide. The use of these features is optional; workers who have a role in a case will continue to be able to conduct work in that case whether or not their district/agency decides to take advantage of the enhanced security features.

In order to effectively use the new security features, it is recommended that district/agency administrators first develop an understanding of basic CONNECTIONS Security as well as the functions that will be performed within CONNECTIONS once Build 18 is implemented. The CONNECTIONS Implementation Management Team will assist administrators to obtain this understanding through the provision of orientations and other support material.

This self-assessment is designed to guide the implementation of both basic and enhanced security. It consists of a series of items – stated as benchmarks – against which to compare your agency's current state of readiness. If a "gap" exists between current readiness and the benchmark, it should be noted in the space under each item. The action steps necessary to eliminate the "gap" should be written in the space provided at the end of each section. These action steps, taken together, comprise the district/agency's Security for CONNECTIONS Case Management Implementation Plan. It is recommended that this plan be completed no later than eight months prior to the district/agency's scheduled implementation of Build 18.

To promote the most comprehensive assessment of the agency's state of readiness, the self-assessment should be conducted by a cross-section of agency administrators and staff. CONNECTIONS Regional Field Staff are available to assist with this effort.

Security for CONNECTIONS Case Management
SELF-ASSESSMENT

**Section I – Organizing the Implementation of Build 17 / General Readiness Issues**

1. The District/Agency's LAN Administrator has the knowledge and skills to fulfill his/her responsibilities related to security, including establishing staff NT accounts in WEBSTAR

Gap:

2. The District/Agency has designated a Security Coordinator and Back-up Security Coordinator who:
    - Have an active NT Identification and mailbox
    - Are active in CONNECTIONS
    - Are on the distribution list for Security Coordinators (otherwise, contact Donna Cramer in OCFS-IT for more information)

Gap:

3. The Security Coordinator and Back-up Security Coordinator are familiar with CONNECTIONS Security through:
    - Attendance at the Security Coordinator training course*
    - Attendance at CONNECTIONS Build 17 Training*
    - Review of the CONNECTIONS Security Step-by-Step Guide
    - Review of resource material available in the Security section of the CONNECTIONS web page.

    * Note: Experienced Security Coordinators should attend Build 17 training that will be offered in April/May 2004. Staff who are new to this role should take the Security Coordinator course after the implementation of Build 17; this course will be updated to incorporate Build 17 content.

Gap:

4. There are a sufficient number of staff who are able to "maintain security" to permit the efficient administration of this function. District/Agencies may determine who on their staff have this capability through the Business Function Report accessible on the Data Warehouse

Gap:

5. In order to be able to make informed decisions about the assignment of business functions to staff and the extent to which staff, supervisors and administrators will have access to records in which they do not have a role, the District/Agency's child welfare administrators have obtained a working knowledge of CONNECTIONS Security, through:
    - Participation in Security for Managers training course (to be provided via Video or computer-based training)
    - Review of the introductory sections (Modules1-5) of the CONNECTIONS Security Step-by-Step Guide
    - Review of resource material available on the Security page of the CONNECTIONS web site.

Gap:

6. The District/Agency has formed a workgroup consisting of a cross-section of agency administrators and staff to recommend how the agency's CONNECTIONS Case Management Security should be structured (see Section II). Team members have obtained a working knowledge of basic security and the enhancements being introduced through Build 17 through the methods described in Item 5).

Gap:

7. The District/Agency's Implementation Coordinator participates in or monitors the implementation of CONNECTIONS Case Management Security with an eye toward completing the process before the release of CONNECTIONS Case Management (Build 18).

Gap :

8. The staff who are implementing CONNECTIONS Case Management Security are familiar with the work processes affected by CONNECTIONS Case Management (Build 18) through:
    - Attendance at OCFS Teleconferences
    - Participation at Regional Forums
    - Review of build 18 Impact Analysis documents

**Gap:**

| **Section I Action Items** | **Responsible** | **Due** |
|---|---|---|

**Section II – Security Data Entry and Clean-up Activities**

1. The district/agency's Security Coordinator is familiar with Data Warehouse reports available to support security clean-up activities. (See Module 9 in the CONNECTIONS Security Step-by-Step Guide.)

Gap:

2. The district/agency has a plan to initially enter, or as needed clean up, CONNECTIONS Security data for staff who perform ongoing services (foster care, preventive, adoption). The plan should address completion of the following activities: (See Modules 6-8 in the CONNECTIONS Security Step-by-Step Guide.)

Security for CONNECTIONS Case Management
SELF-ASSESSMENT

Initial Entry

- Assure that all staff are assigned a NT logon ID and have "standard access" via WEBSTAR (performed by LAN Administrator)
- Create additional units, including their specialization, as necessary (Note: the designation of "unit specialization" may affect access to cases – see chart in the next section.)
- Each worker who needs to be made "case assignable" and is assigned the business functions appropriate to their job function
- Each worker is assigned to the appropriate unit including reassignment of any staff from default unit(s)

Clean-up Existing Data

- Eliminate units with duplicate unit identifiers
- Delete "default" units (units coded as N and two numbers) that contain only "conversion" workers (Note: CONNECTIONS Security is working on a solution to the inability to delete a default unit that has had a stage assigned to it). No unit should exist with the conversion worker as unit approver.
- End Date staff who no longer work for the agency in CONNECTIONS and then delete those staff in NT through WEBSTAR; staff who have already been deleted in WEBSTAR should be end dated in CONNECTIONS.
- Determine that the WMS/CCRS staff identifier is correctly recorded in the Staff Detail Window for all staff who have an ongoing services case assigned to them. **(NOTE: this is a critically important activity in the effort to match cases to workers as part of the Build 18 conversion.)**
- Determine that all staff who are entered in the system as case assignable should be case assignable. (Information about which staff are case assignable may be obtained on the Staff Detail Window within CONNECTIONS or on the Staff Security Report in the Data Warehouse.)
- Determine that staff are assigned the business functions they need and only those that they need.
- Eliminate "out-assignments" that are no longer necessary in light of the Build 17 case access enhancements.

Gap:

**Section II Action Items** **Responsible** **Due**

**Section III – Program and Operational Considerations**

1. The District/Agency has decided whether staff will have View and/or Maintain access or No access to information in Case Management stages in which they do not have a role as follows:

| Level of Staff Person | View | Maintain | None |
|---|---|---|---|
| To Case Assignable* Staff (Caseworkers)<br>• All FSI and FSS stages within their district or agency<br>• All FSI and FSS stages within their unit<br>• All FSI and FSS stages of staff sharing the same "job type" | | | |
| To Unit Approvers (Supervisors)<br>• All FSI and FSS stages within their district/agency<br>• All FSI and FSS stages in units sharing the same "unit specialization" | | | |

| | | | |
|---|---|---|---|
| Direct Supervisory Line (through Organizational Hierarchy)<br>• All staff within the direct supervisory line on the "organizational hierarchy"<br>• All non-clerical staff within the direct supervisory line | | | |

* Information about which staff are "case assignable" may be obtained on the Staff Detail Window within CONNECTIONS or on the Staff Security Report in the Data Warehouse.

2. The District/Agency has decided how to align units within the Organizational Hierarchy Window. **Note: this step is only needed if the district or agency has decided to grant access to cases through the direct supervisory line (per the third row in the above chart.)**
3. In light of the expanded sharing of information that will occur upon the implementation of CONNECTIONS Case Management, administrators have reviewed their district or agency's confidentiality and data security policies and procedures.

Gap:

**Section III Action Items** **Responsible** **Due**