

# CONNECTIONS WEEKLY SYSTEM UPDATE



Happy Thanksgiving

**To:** CONNECTIONS Implementation Coordinators  
**From:** CONNECTIONS Communications  
**CC:** LAN Administrators/Security Coordinators, Keyusers,  
OCFS~Directors of Services, CONNECTIONS Project  
Team  
**Date:** November 20, 2003  
**Re:** Activities for the week of November 21<sup>st</sup> ~ 28<sup>th</sup>, 2003

---

## 1. Build 16 Readiness Checklist for Implementation Coordinators

The CONNECTIONS Build 16 Readiness Checklist ~ CPS Enhancements is available on the CONNECTIONS Intranet website on both the Home page under “What’s New” and the Implementation page under “Build 16 Information”.

The checklist is a tool, designed to aid local districts in their preparation for the implementation of Build 16. It is recommended that both Implementation Coordinators, as well as Implementation Teams, review their district’s readiness in symmetry with the items identified on the checklist and begin to take any necessary actions to prepare for a smooth transition into the Build 16 environment.

## 2. Build 16 Preview Application

This notice is to inform you that the Build 16 Preview Memo and Build 16 Preview Request form were forwarded to Directors of Service, CONNECTIONS Implementation Coordinators and Staff Development Coordinators on November 7, 2003. These documents are also available on the CONNECTIONS website on both the Home page and the Implementation page.

Availability of the Preview Application offers local district staff an advance look at the Build 16 system modifications, enhancements and changes prior to the “live” date of the Build. It should be noted that although the Preview Application was made available as an icon on users desktops as of Tuesday, November 18<sup>th</sup>, local districts have to request a test case in order for staff to work with the Build 16 functionality.

The instructions to access the Preview Application icon were forwarded to CONNECTIONS Coordinators on, Monday, November 17<sup>th</sup>. The Instructions have been posted on the website on both the Home and Implementation pages.

### 3. **OFT Workstation Policy – Workstation Lockdown**

On Monday, December 1, 2003 the New York State Office for Technology (OFT) will be implementing a new policy to automatically lock workstations after a period of fifteen (15) minutes of inactivity. The policy will be applied to all computer workstations that authenticate through the HSEN domain. This policy is in response to the Information Security Policies document released by the New York State Office of Cyber Security and Critical Infrastructure Coordination. It is intended to increase security on the network by helping to prevent unauthorized access to workstations when staff are away from their desks.

In order to help CONNECTIONS users understand what the implementation of this policy will mean and the actions that will have to be taken in response to it, we are providing the information below.

#### **What You Should Know About The New Policy**

- As long as you are working on your workstation, pressing keys on the keyboard or moving the mouse, nothing will change.
- If you stop pressing the keys or moving the mouse for a time period longer than 15 minutes, your screen will blank out or, your screen saver will be activated. When you press a key, you will have to re-enter your user name and password to unlock the workstation. This will most likely occur when you are engaged in long telephone conversations, when you leave your desk to go to meetings, or leave your desk to take your lunch break.

You will see a screen that looks something like this:



If it does not already appear, you will have to enter your User ID (i.e. NYS123, AB0200, etc.) in the box next to "User name:". You will then

have to enter your password in the box next to “Password:”. Then click on the “OK” button and your desktop will reopen. Any Applications, documents, spreadsheets, mail notes, etc. that you had open when the workstation locked will still be open when you unlock the workstation. It should be noted that in an environment where there are shared workstations, re-booting will unlock the workstation and allow another user to sign on.

- You may force the workstation to lock if you know you will be away from your desk by pressing the CONTROL-ALT-DELETE keys simultaneously.

The following screen will then appear:



Please note that when you select “Lock Computer”, no one can use your desktop until it has been unlocked with your password.

- You cannot override this policy by changing the settings on the workstation. The OFT policy will override any changes that you may make. Please note that all OFT workstation policies are updated routinely on the workstation.
- You should still logout of the workstation before you go home for the day to insure that your files are properly backed up. While the new policy prevents unauthorized access, it does not close any open files and open files are not backed up. Outlook must be closed for the personal folders to be backed up.

If you have any questions or need further assistance, please contact your CONNECTIONS Regional Field Support Staff.

#### **4. HSEN Password As It Relates To FAD/CPS Approvals**

It should be noted that users who have been migrated to the HSEN environment might be having difficulties completing approvals. In order to validate the approval, users must create a password that includes

characters that are alpha-numeric only. **Do not include punctuation marks or other characters.**

## **5. Multiple Person Report**

This notice is to advise you of the availability of the Multiple Person Report in the Public Folders. This report identifies multiple instances of the same person within CONNECTIONS and allows the user to consider them for person merge.

If users have questions related to the report they may contact their CONNECTIONS Regional Office Field Support Representative.

## **6. CONNECTIONS-In-A-Box (CIAB) Replacement Project**

The 2003 CONNECTIONS-In-A-Box (CIAB) Replacement Project is moving forward. The rollout of the new CONNECTIONS-In-A-Box (CIAB) Windows 2000 workstations is as follows:

- Region II (the Rochester Region) ~ rollout of new CIABs completed
- Region I (the Buffalo Region) ~ rollout of new CIABs completed
- Region III (the Syracuse Region) ~ rollout of the new CIABs completed
- Region IV (the Albany Region) ~ rollout began the week of November 17, 2003
- Region V (the Yonkers Region) ~ early December 2003
- Region VI (the NYC Region) ~ mid-December 2003

Targeted communication regarding the 2003 CIAB Replacement Project has been sent to agency systems coordinators and contact persons for districts/agencies located in the Rochester, Buffalo, Syracuse, Albany, Yonkers and NYC regions. If there remain any CONNECTIONS CIAB sites in New York State that have not received communication materials regarding the 2003 CIAB Replacement Project, please contact Patrick Jones by phone (518) 473-4770 or email at [Patrick.Jones@dfa.state.ny.us](mailto:Patrick.Jones@dfa.state.ny.us) immediately so that arrangements can be made to provide you with the necessary information.

**Early Preparation Activities:** \*\*\*Reminder\*\*\*, the OFT Coordination Center will be calling district/agency site contacts approximately two weeks prior to your district/agency implementation date to schedule a date for our vendor (IBM) to install and replace your new equipment. In addition to scheduling the date for installation, staff from the OFT Coordination Center will also be asking for a list of NT Log-on ID's of any staff who will be using the new Windows 2000 CONNECTIONS-In-A-Box workstations at your site. As an early preparatory task, we encourage Security Coordinators, or other identified site contacts, to collect all appropriate NT ID's of staff. This will facilitate the installation and log-on process of the new Windows 2000 CONNECTIONS-In-A-Box (CIAB) into the HSEN domain.

Please check the NT ID's of all staff who will be using the new CIAB devices and make sure the NT accounts are still active. In our experience thus far, there have been numerous instances of NT Log-on ID accounts no longer being valid due to inactivity. We recommend that Security Coordinators begin the process of collecting the NT Log-on ID's of staff and verify that the accounts are still active. If the accounts are no longer active, the Security Coordinator at each site should immediately create new accounts for staff using WEBSTAR. If there is not a designated Security Administrator at your site who has rights to administer new accounts please contact your OCFS CONNECTIONS Regional Office Field Representative so that they may provide you with the necessary instructions and procedures for designating a Security Administrator.

As a matter of good practice, is it important that all users, especially CIAB users, dial-in to the network and log-on at least one time each week. The new CIABs workstations authenticate through the HSEN domain, therefore, any long-term in-activity in dialing in and logging on to the Network will result in the workstation and NT Log-on ID being rendered inactive in the HSEN domain structure.

#### **7. RAS Dial Up Maintenance**

RAS (Remote Access Server) dial-up services for laptops and CONNECTIONS-In-A-Box (CIAB) will not be available 11/21/03 between the hours of 3AM-7AM so that Network system maintenance can be completed.

#### **8. CONNECTIONS System Down Time**

Due to regularly scheduled maintenance CONNECTIONS will be unavailable on:

***Friday, 11/21/03 from 5:00 AM - 7:00 AM***

***Wednesday, 11/26/03 from 5:45 AM - 6:30 AM***

***Friday, 11/28/03 from 5:00 AM - 7:00 AM***

#### **9. Microsoft Exchange Mail Servers**

Due to regularly scheduled maintenance on MS Exchange E-mail 5.0 servers, all Exchange E-mail 5.0 servers will be unavailable on:

***Sunday, 11/23/03 from 1:00 AM - 6:00 AM***

***Sunday, 11/30/03 from 1:00 AM - 6:00 AM***