

CONNECTIONS WEEKLY SYSTEM UPDATE

Memo

To: CONNECTIONS Implementation Coordinators
From: CONNECTIONS Communications
CC: LAN Administrators/Security Coordinators, Keyusers, OCFS -Directors of Services, CONNECTIONS Project Team
Date: September 11, 2003
Re: Activities for the week of September 12, 2003 – September 19, 2003

1. New Microsoft Vulnerability Reported

The following message contains information that was sent from the NYS Office for Technology (OFT) Customer Relations to Local Districts System Coordinators earlier this afternoon 9/11/03:

Due to a critical vulnerability reported on 9/10/03 by Microsoft, the Office for Technology must respond quickly to protect our environment from any malicious exploit. This afternoon OFT will begin to use the Tivoli product to distribute the patch to Windows 2000 workstations statewide, this includes CONNECTIONS replacement workstations and Plan B PCs. The package that we are deploying performs the following actions:

1. Reboot
2. Install Hotfix KB824146
3. Create a desktop Icon
4. Reboot

The process takes about 10 minutes on our test machines. Actual elapsed time may vary depending on the individual workstation. The presence of the icon on the desktop is confirmation that the patch was successfully applied. The icon will appear as a folder on the desktop with the name "Hotfix_kb824146_INSTALLED". **Please do not call the Coordination Center or EHD to report machines that are not patched.** A report of workstations that failed to successfully receive the distribution will be produced and OFT will be addressing them from here. **Please remember to keep your PCs powered-on, including nights and weekends.**

Please share this information with staff in your agency. We apologize for any inconvenience this may cause but it is in our customer's best interest to mitigate this risk quickly.

We will address the installation of the patch on the NT 4.0 workstations after completing the install to the Windows 2000 devices.

Additional Information Regarding the Aforementioned Notification

The Office for Technology (OFT) will be pushing this security update via the Network to Windows 2000 (Tivoli) workstations beginning 9/11/03 at 5pm. The security update packages will also be distributed to non-Tivoli Windows 2000 workstations throughout the night. Special considerations for this security package update have already been taken for workstations at the NYS Child Abuse and Maltreatment Register (SCR). When users leave work on Thursday evening, September 11th, they should be instructed to “save” any open work and log-off of their workstations leaving the workstations powered on. Please make sure to alert staff to leave their CONNECTIONS workstations “powered on” so the workstations can receive the security package. **Do not “power off” or shut down your workstation.** When users “log off” they should do so in the following manner:

- Select “shut down” from the Start menu;
- Select “log off” (This ends your session leaving the computer running on full power. The “ctrl+alt+delete” message will be visible on the monitor).

2. Outages and Welchia/Blaster Worm Virus Remediation

A). Impact on CONNECTIONS

As you know, the recent connectivity difficulties to our HSEN Network that were caused by the power outage of 8/14 and the Blaster and Welchia Worm Virus have had a negative effect on most of our systems and programs.

Due to the aforementioned issues (extended downtimes of our network, and the virus remediation efforts), many districts/agencies have been unable to follow statutory guidelines and timeframes for documenting in the computer systems when required activities occurred. Once districts are confirmed/certified as reconnected to the network and resumption of normal operations have occurred, the State would remind districts/agencies that with respect to CPS records and Foster and Adoptive Home Certification records in CONNECTIONS, the system is designed to allow posting the actual safety assessment and investigation conclusion event dates, as well as foster and adoptive home certification dates, even if those activities occurred at a point in time when the system was unavailable. For FAD workers, if there have been instances where an agency/district foster home certification has lapsed and the home was closed, FAD workers should follow procedures for re-opening homes as specified in the CONNECTIONS FAD Step-by-Step Guide, Module 17.

If there are any questions around the aforementioned advisory, please contact your Regional Office CONNECTIONS Implementation Staff.

B). Voluntary Agency Remediation Efforts

The Blaster and Welchia Worm virus remediation efforts have been highly successful to date with WMS and most critical network services restored statewide. OCFS/IT CONNECTIONS and OFT thank all of you for the tremendous effort districts/agencies have put forth in this crisis.

At this time, OCFS IT/CONNECTIONS would like to remind all voluntary agencies of the critical need to apply the service pack upgrade, hot patches and virus definition files that were made available for the virus remediation effort. Remediation CDs were mailed to each site systems contact or CONNECTIONS Implementation Coordinator. After you have applied the CD service pack upgrade, patch, and anti virus files to your Windows 2000 and NT 4.0 servers and networked PCs, you need to contact the OFT Coordination Center at 1-800-603-0877, and request a scan of your site for any remaining vulnerability, and to have the site certified as cleaned and patched.

If there are any questions around the aforementioned advisory, please contact your Regional Office CONNECTIONS Implementation Staff.

C). Servers/PC's Power Up Reminder

We have been asked to share the following message from OFT Customer Relations:

In order to further assist the OFT Network Technologies Office in their continuing effort to carry out the worm remediation, please remember that all **SERVERS and PC's should be "Powered Up" at all times**, including nights and weekends. This is necessary for OFT to remotely contact and fix those servers and PC's.

Staff may turn their monitors off, but the processing component of the PC must remain on at all times. Servers should never be turned off without first contacting OFT staff.

We ask your assistance in alerting all site managers and staff of these requirements. All facilities should also make sure that power is not being turned off at breakers by cleaning staff in the evenings.

As always, if you have any questions or need assistance, please contact your OFT Customer Relations Representative.

3. OCI Management Reports Postponement (CPS Only)

Reminder: As reported in last week's CONNECTIONS Weekly Update, due to the recent blackout (power outage) and virus remediation efforts, the OCI Management Reports that were scheduled for last weekend (9/5 -

9/7/03) were postponed. The following OCI Reports were impacted by the postponement:

- ❑ Open Case Inquiry Investigations Monthly Management Report
- ❑ Open Case Inquiry Investigations Monthly Management Summary Report
- ❑ Open Case Inquiry Investigations Statewide Total Report

The aforementioned OCI Reports have been re-scheduled for this upcoming weekend 9/12 – 9/14/03. The OCI Reports will be available beginning Monday morning, 9/15/03.

4. Network Integration Services (NIS) Sharepoint

Reminder: As referenced in the CONNECTIONS Weekly Update over the last several weeks, an NIS sharepoint became operational beginning Friday, September 5th, 2003. IT staff at Network Integrated (NIS) agencies or sites that have a need to update software (CONNECTIONS or Network related) are encouraged to contact Cathy Vallee with OCFS IT Operations for instructions on how to access the NIS sharepoint. **Please contact Cathy via email, Cathy.Vallee@dfa.state.ny.us.**

Questions related to NIS should be forwarded to OFT Customer Relations. For information regarding NIS, please visit the OFT Customer Relations Command Center at <http://sdssnet5/crcc/>. To view NIS procedures and the online NIS Form and Survey, click on the NIS form and information link. All completed NIS requests/surveys must be submitted electronically to COMCTRUP.

5. Job Types Review for Security Coordinators

This notice is to alert Security Coordinators to correspondence that they soon will be receiving regarding CONNECTIONS Security Job Types. Job Types will be a new data element in CONNECTIONS Build 17. These new Job Type elements will be used to determine access to Family Services workloads after implementation of CONNECTIONS Build 18, if an agency or district chooses that option. An agency or district will be able to choose to give either “**view**” or “**maintain**” access to cases of all workers with the same Job Type. Job Type will also be used to determine if a worker is considered Clerical or Non Clerical. In order to prepare for these new options, the listing of Job Types must be determined for each Office Type.

Jo Shrader, the OCFS Information Security Officer, will be sending out the aforementioned correspondence in the very near future to all CONNECTIONS Security Coordinators for his or her own Office Type. We have been advised that once the information has been distributed, Jo

will be requesting that Security Coordinators review the Job Types and submit any comments or questions to her.

6. CONNECTIONS-In-A-Box (CIAB) Replacement Project (CIAB Sites Only)

As referenced over the last several weeks, the 2003 CONNECTIONS-In-A-Box (CIAB) Replacement Project is moving forward. Similar to prior CONNECTIONS PC Replacement Projects, the CONNECTIONS-In-A-Box (CIAB) Replacement Implementation Plan will employ a regional approach. The rollout of the new CONNECTIONS-In-A-Box (CIAB) Windows 2000 workstations will begin in Region II (the Rochester Region), followed by Region I (the Buffalo Region), Region III (the Syracuse Region), Region IV (the Albany Region), Region V (the Yonkers Region) and Region VI (the NYC Region). Targeted communication regarding this project will be sent in advance of each region's implementation.

7. CONNECTIONS System Down Time

Please Note that a change to the CONNECTIONS weekly maintenance schedule has been implemented. The new schedule is as follows:

Friday, 9/12/2003 from 5:00 am - 7:00 am

Wednesday, 9/17/2003 from 5:45 am - 6:30 am

Friday, 9/19/2003 from 5:00 am - 7:00 am

8. Microsoft Exchange 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, 9/14/2003 from 1:00 am - 6:00 am

Sunday, 9/21/2003 from 1:00 am - 6:00 am