# CCR MASTER EXTRACT POLICY

**Updated 3/5/03**

The following scenario depicts the process in which all DLIS CCR Master extracts will be handled.

Effective immediately TEN files (5 Refresh, 5 Daily) will be created and stored on a secured (User code/password) DLISCCR server in zipped format. These files will contain a complete listing of all current active records. Each file will store a different type of view, **Public**, **Proprietary**, **Sensitive**, **MPIN**, and **Complete** data.

During the same time frame a nightly file of change records will be generated and also stored on the same server. These files are a complete record, but only records that have changed during that given day. These files will stay on the server for 30 days.

The above allows for three types of processing to take place:

- Downloading of the monthly extract each month to refresh a user database.
- Download the monthly database once then by downloading the daily update files each day keeps the database in sync with DLIS.
- A combination of 1 and 2 where a complete refresh is done each month even though the daily updates were processed.

Each user will be assigned a UserId and Password allowing for access to the extract files on the DLISCCR Server. Each UserId will be assigned on an as needed basis for the type of data wanted. Each user that will access the CCR data will be required to sign a Non-Disclosure Agreement (below).

**It will be the users responsibility to pull the zipped extract files from the DLISCCR Server, unzip the extract files once downloaded and load said extract files to their database.**

## Access Limitations and Locations

To comply with the encryption requirements for sensitive CCR information, the transfer of this data will be performed in a secure manner.
The **Public, Proprietary, Sensitive, MPIN, and Complete** extract can be accessed and downloaded through **FTP at** ftp.ccr.dlis.dla.mil (**updated 5/26/02)

(Note:  Security/encryption requirements for the **Proprietary, Sensitive, MPIN, and Complete** will necessitate the use of Secret Agent encryption software.

## FTP FILE DIRECTORY

- **DIR1/FOIA**
- **DIR3.4/PROPRIETARY**
- **DIR3.5/SENSITIVE**
- **DIR3.6/MPIN**
- **DIR3.7/COMPLETE**

The **Public, Sensitive, Proprietary, MPIN, and Complete** extracts can be accessed and downloaded through the Web site https://www.alt1.dlis.dla.mil/ccr_extracts using Microsoft Explorer (version 3 or greater).
Microsoft Explorer encrypts the user-id and password.
Once verification is complete the file transfer is done through SSL.

- **Public files are stored in FOIA Directory**
- **Proprietary files are stored in Proprietary Directory**
- **Sensitive files are stored in Sensitive Directory**
- **MPIN files are stored in MPIN Directory**
- **Complete files are stored in Complete Directory**

## File Naming Conventions

**Position #1 = 'C' to indicate 'CCR' file**
**Position #2 and #3 = file type (below)**
**Position #4 - #8 = Julian Date**

- CR = Complete Refresh
- FR = Public Refresh
- PR = Proprietary Refresh
- SR = Sensitive Refresh
- MR = MPIN Refresh
- CD = Complete Daily
- FD = Public Daily
- PD = Proprietary Daily
- SD = Sensitive Daily
- MD = MPIN Daily

New monthly files are available on the last day of the month by 08:00.
Daily update files are produced Tuesday – Saturday and are available on the server by 08:00.

## Point of Contact Information

CCR Program Management Office/Operations
Defense Logistics Information Services (DLIS)

Thresa Cameron/269-961-4385
Thresa.cameron@dla.mil

Peggy Lockwood/269-961-5574
Peggy.lockwood@dla.mil

## Secret Agent Encryption Process

1. Recipient of encrypted data is to request access to specific data feeds from appropriate DLIS contacts.

2. Approved Recipient of encrypted data is to procure a copy of Secret Agent from AT&T.

3. Recipient of encrypted data is to test their encryption/decryption process in their environment.

4. Decryption key password is mailed to recipient of encrypted data.

5. Decryption key is mailed separately to recipient of encrypted data.

6. Encrypted test data file is made available via ftp to recipient of encrypted data.

7. Recipient of encrypted data decrypts encrypted test data file with decryption key.