Use of Cognos
A SSD is urged to utilize the new Electronic Signature Report available through Cognos.

Provisioning and Recertifying Users
1. Provisioning Procedure

In order to access the Electronic Signature Report, users must undergo the following provisioning procedures:

Cognos Security Contacts must authorize named users to have access to the reporting projects and the data supporting those projects within the Cognos Reporting Application. Security Contacts for Social Service Districts are the Local Commissioner or his/her designee. Some Commissioners have retained this authority, while others have appointed multiple Security Contacts.

Users are required to have an active HSEN account in order to be authenticated into the Cognos Reporting Application.

In order to provision users or reflect a change in business need for users' access in instances including but not limited to, a change of job duties, retirement, or termination of employment, the appointed Cognos Security Contact for the SSD must submit a completed User Request and Change Form. This form may be accessed electronically via Cognos Report User Request and Change Form. The completed User Request and Change Form must be submitted to the Cognos Shared Mailbox at **Cognos.Reporting@otda.ny.gov**. **The Security Contact should request access to Central SOS data for this report**.

Once the User Request and Change Form is received, ITS personnel will verify that the form is complete and that the request is from an appointed Security Contact. ITS will then log the request in the ITS User Request Tracking SharePoint application and set up the necessary credentials to access the report. The user will be sent a "Welcome to Cognos Reporting" e-mail with a copy to the SSC Cognos Security Contact when the request is complete.

2. Auditing Authorizations

Cognos Administrators regularly audit each SSD's user authorizations. Cognos Administrators will confer with the appointed Security Contact in each SSD, auditing the list of currently provisioned users and the data access levels of each provisioned user. During the audit, the Security Administrator must make any necessary changes to the individual user's accessibility to Cognos data. Data access may need to be modified for a number of reasons including, but not limited to, a change in business need for the user, retirement, or termination of employment.

PLEASE NOTE: An individual user's accessibility should be consistently monitored by a SSD and changed in a timely fashion when necessary. A SSD should not wait until an audit to address such changes.

3. Confidentiality

When granting new user access to Cognos a SSD must be aware of the confidential and sensitive nature of data they are accessing from WMS/WRTS, and of the SSD's non-delegable responsibilities to properly safeguard such data. Cognos, and all data accessed through it, are confidential and proprietary to the State of New York. Access to the Cognos audit tool shall be limited to specifically authorized employees and only for authorized purposes. SSD management must assure the propriety of the use of and access to such confidential and secure information by authorized employees. This access may NOT be delegated to a third party.
That is, access may only be authorized for a specified SSD employee.

C. Using the WMS Audit Tool
Attached is guidance on how to access and use the report (see "How to Access and Use the Electronic Signature Report").

D. Terminating Users Permissions/Notification if Access Should be Terminated
Permission to utilize the Electronic Signature Report may be terminated at any time at the sole discretion of OTDA or upon the request of the Local District Cognos Security Administrator.