Technical and Security Requirements for CFSR Online Monitoring System

March 2020

The Children's Bureau has developed the Online Monitoring System (OMS) for the Child and Family Services Reviews (CFSRs) to facilitate data collection related to Round 3. The OMS encompasses a Web-based application for entering case-level review data through the Onsite Review Instrument and Instructions (OSRI) and stakeholder interview data through the Stakeholder Interview Guide (SIG), as well as reporting capabilities and data visualization. The OMS is available to all states for use in the CFSR and for non-CFSR Continuous Quality Improvement (CQI) activities, including Program Improvement Plan (PIP) monitoring.

The security, confidentiality, and integrity of data collected through the CFSR process is of the utmost importance to the Children's Bureau. The security systems used in the OMS comprise a variety of integrated protections, including managerial, operational, and technical controls.

All users must agree to the Privacy Policy, Confidentiality Agreement, System Use Notification, and Rules of Behavior, below. This document also includes System Specifications that are also accessible via the OMS User Manual (available from the OMS Help page).

CFSR OMS System Specifications

The OMS is a Web-based application accessible to authorized users on most common platforms, including desktop computers, laptop computers, and some mobile devices. For platforms smaller than a tablet, use of the OMS may be available, but such platforms are not supported at this time.

Full OMS use can be achieved on a laptop, multi-function tablet, or desktop when the equipment has a minimum level of hardware and software. States can access the OMS through the CFSR Information Portal using any major Web browser. Laptop, desktop, and multi-function tablet minimum system specifications include:

- Windows 8.1, or 10.x with latest updates, or OS X 10.13.x or later (patched with latest updates)[1]
- CPU: Intel Core i5 (or competitor equivalent), with 2 gigabytes (GB) of RAM (4 GB recommended) and minimum 200 megabytes (MB) of free disk space
- Screen resolution: XVGA (1024 x 768) or higher recommended to format OMS content properly on the screen
- Browser: These four supported browsers, which must be updated with the latest patches and updates: Google Chrome; Mozilla Firefox; Microsoft Edge; Microsoft Internet Explorer (IE) 11.x
- Browser Setting: JavaScript and cookies enabled

[1] The OMS may run in environments other than those listed above; however, use has not been thoroughly tested in all environments and may not be supported.

- Additional applications that may be required to view reports: Adobe Acrobat, Microsoft Office 2010 or higher, and/or MS Office 365
- Broadband Internet or Wi-Fi connection

Privacy Policy

On behalf of the Children's Bureau, the Child Welfare Reviews Project, managed by JBS International, Inc., has created this application to support state child welfare administrators, state staff, federal staff, and JBS employees or consultants working on the CFSRs, CQI reviews, and state child welfare Program Improvement Plans (PIPs).

When you visit the OMS, we collect limited personal information about you to help us understand who visits the site and how it is being used. Here is how we handle information about your visit.

What We Collect and Store Automatically

If you log in and browse through the website, read pages, or download information, the system automatically collects and stores the following information about your visit:

- Your name, organization, email address, and phone number;
- Your username and what you view on the site;
- The IP address (an IP address is a number that is assigned to each computer connected to the Internet) from which you access our site;
- The type of browser and operating system used to access our site;
- The date and time you access our site;
- The pages you visit;
- The amount of data transferred between our server and your computer; and
- If you linked to our website from another website, the address of that site.

How We Use Your Personal Information

This website uses the information collected, including your personal information, for four purposes:

- We may use your name, phone number, or email address to contact you if we have questions about any of the data you enter into the system.
- We may use the information we collect to count the number and type of visitors to the different pages on our site and to help us make our site more useful to visitors.
- We may use your email address to keep you informed of any reporting deadlines or documents awaiting your attention, or to let you know in advance when the site will be down for maintenance for longer than 2 hours.
- If you choose, you may indicate your name, organization, and/or email address when you contact us either via email or by submitting a Help request.

If You Email Us or Request Help

You may choose to provide us with personal information as an email with a comment or question or as a Help Desk request. We use the information to improve our service to you or to respond to your request. Sometimes we forward your email or Help request to other government or contracted employees who may be better able to help you. Except for authorized law enforcement investigations, we do not share our email or Help requests with any organizations outside the Children's Bureau and authorized contractors of the Children's Bureau.

Use of Cookies or Other Tracking Devices
A persistent cookie is a small text file that is stored on your computer and makes it easy for you to move around a website without having to continually re-enter your name, password, preferences, or other information. Consistent with the Department of Health and Human Services' policy on the Usage of Persistent Cookies, our website does not use persistent cookies. A session cookie is a small text file that is not stored on your computer but is kept in memory while you are connected to our site and is deleted when you close your browser or click "Logout" on the home page. We use session cookies only to make your visit more productive for you.

Securing the Information We Collect Online
We are committed to properly securing the information we collect online. To accomplish this, we take the following steps:

- We employ internal access controls to ensure that the only people who can see your information are those with a need to do so to perform their official duties;
- We train relevant personnel on our privacy and security measures so that our personnel know what is required for our compliance;
- We use technical controls to secure the information we collect online, including encryption, firewalls, and password protections;
- We periodically test our security procedures to ensure personnel and technical compliance; and
- We employ external access safeguards to identify and prevent unauthorized attempts by outsiders to hack into, or cause harm to, the information in our systems.

Tampering with this website is punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

Links to Other Sites
Our website has links to a limited number of public and private organizations. When you click on a link to another site, you are no longer on this site and are subject to the privacy policy of the new site.

System Use Notification—Reviewers, Site Leaders, Observers, State Administrators

JBS International, Inc. (JBS), under contract with the Children's Bureau, U.S. Department of Health and Human Services (HHS), actively monitors this system and activity to maintain system security and availability and to ensure appropriate and legitimate usage. Any individual who intentionally accesses a federal computer or system without authorization, and who alters, damages, makes unauthorized modifications to, or destroys information in any federal-interest computer, or exceeds authorized access, is in violation of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Any evidence of possible violations of proper use or applicable laws found as a result of this monitoring may be turned over to the Children's Bureau, HHS, and law enforcement. Any individual found to be in violation of the system's proper use rules or law could be punished with loss of system access, fines, and/or imprisonment. By proceeding, you hereby acknowledge your agreement with these terms and the system's rules of behavior and consent to such monitoring and information retrieval for law enforcement and other official purposes.

Confidentiality Agreement

All data and reports on the Child and Family Services Reviews (CFSR) Online Monitoring System (OMS) are confidential, may contain sensitive information, and are intended for authorized users. JBS does not accept liability for the contents herein.

Rules of Behavior

POLICY FOR USE OF OMS RESOURCES FOR THE CFSR MUST BE FOLLOWED.

- As a user of the CFSR OMS, you are required to be aware of, and comply with, all applicable policies and guidelines on authorized use and security of the OMS computer resources and data.
- You must inform OMS management and/or JBS if you are departing your position or organization and should no longer have access to the OMS.

YOU ARE RESPONSIBLE FOR ALL ACTIONS PERFORMED WITH YOUR PERSONAL USER ID.

- User IDs and passwords are for your individual use only and, as confidential information, are not to be shared.
- You must not disclose your password to anyone, and you must take necessary steps to prevent anyone from gaining knowledge of your password.
- As an OMS user, you will be expected to employ good password management practices as defined and enforced by system management prompts dictated by the system.

POLICY, STANDARDS, AND PROCEDURES MUST BE FOLLOWED.

- Use of OMS computer resources is restricted in accordance with federal policy and guidelines.
- Violations of the "Computer Fraud and Abuse Act of 1986" (Public Law 99–474), the Privacy Act, the Trade Secrets Act (18 U.S.C. § 905), and other federal regulations applying to unauthorized use of federal computer systems, files, records, and data, are punishable by law.
- Be aware that all OMS computer resources used and accessed by authorized OMS users are subject to periodic testing, review, monitoring, and auditing. Any evidence of security violations or illegal activity will be immediately turned over to OMS management or law enforcement for action. Penalties could include loss of access, fines, and/or imprisonment.

ACCESS TO INFORMATION MUST BE CONTROLLED.

- Access only the information for which you have been authorized and have a "need to know/access."
- Do not leave computers logged on to OMS and unattended. Log off at the end of each session or use access control software (for example, a screen saver with password) during unattended use.
- If you know that another person has used or is using your credentials, you must report the incident immediately to OMS management and JBS.

- Take steps necessary to maintain security of computer files and reports containing OMS information.
- Do not email personally identifiable information (PII) such as case names, names of children and families, or demographic information that may be identifiable. If you need to email case information, use descriptions that do not contain PII, such as the reviewer, site, and/or case status. This includes email within your organization, as well as with the Help Desk.

For State Administrators Only

STATE ADMINISTRATOR RESPONSIBILITIES MUST BE FULFILLED.

- State Administrators must oversee the case finalization and de-identification process for your state's CQI review site. It is recommended that cases be finalized within 60 days of creation in the OMS, and de-identified within 14 days of finalization.
- State Administrators must inform OMS management and/or JBS of any departing staff who should no longer have access to the OMS.
- If for any reason you will no longer serve in the role of State Administrator, you must inform OMS management and/or JBS regarding who, from the state, will serve as State Administrator in your place. If a replacement will not be identified before you leave, you must inform OMS management and/or JBS, as well as your Children's Bureau Regional Office.

Last Updated March 2020