

Child Support Portal Registration

OMB Information Collection Request

0970 - 0379

Supporting Statement

Part A - Justification

October 2021

Submitted By:
Office of Child Support Enforcement
Administration for Children and Families
U.S. Department of Health and Human Services

A. Justification

1. Circumstances Making the Collection of Information Necessary

The federal Office of Child Support Enforcement (OCSE), Division of Federal Systems, maintains the Child Support Portal (Portal) as part of the Federal Parent Locator Service (FPLS). The Portal is a secure, web-based gateway to various child support applications for authorized users to view, update, upload, send, and receive vital information to support effective and efficient enforcement of child support cases.

To provide authorized users with secure access to the Portal, OCSE creates profiles within the Portal for employers, insurers, and financial institutions from information provided in “Employer Services” (ES) and “Insurance Match Debt Inquiry” (IM) Agreement and Profile forms (see OMB No: 0970-0196 for the financial institution Profile form), and sets up Portal preferences using information from the program-specific electronic National Medical Support Notice (e-NMSN), the electronic Incoming Withholding Order (e-IWO), and Multistate Financial Institution Data Match FAST Levy (MSFIDM FAST Levy) Profile forms. State child support agencies do not register for the Portal through OCSE because they manage and authenticate authorization for individual users via the state proxy server; however, states must provide OCSE with a profile form containing information for OCSE to establish account preferences.

The federal Child Support Portal Registration information collection activities are authorized by 1) 42 U.S.C. § 653(m)(2), which requires the Secretary to establish and implement safeguards to restrict access to confidential information in the Federal Parent Locator Service to authorized persons and to restrict use of such information to authorized purposes; 2) E-Government Act of 2002 and Office of Management and Budget (OMB) Circular 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, which requires agencies to ensure program integrity by verifying access to data; and 3) 44 U.S.C. § 3554, which requires OCSE to implement security protections to prevent unauthorized access to information maintained by OCSE.

This request is for a revision of a currently approved collection. See A.15 for an explanation of changes.

2. Purpose and Use of the Information Collection

OCSE creates secure profiles for employers, insurers, and financial institutions based on information provided in the ES and IM Agreement and Profile forms. Once a profile is created and an authorized user registers, OCSE authenticates the registrant. To do so, information obtained during the registration process is compared to information in the National Directory of New Hires (NDNH) to

verify the authorized user's name, Social Security number, and employment information. OCSE administrative staff also call the employer to verify employment of registrants.

After verifying an authorized user's information, OCSE administrative staff set the account to "verified" status for Portal access and notify the authorized user via email to activate the account. Instructions and security procedures for account activation are provided in the email notification. If a registration authentication fails, the email notification will contain a notification of denial.

Upon activation of the account, the authorized user can log into the Portal using the FPLS Security Framework to access specific Portal programs for which the authorized user is approved. The login process accepts user credentials (user ID, password, and access code) and then validates credentials against a data store, which is a table of authorized users. If the credentials are valid, access to the Portal is permitted. If the credentials are not valid, the login page displays an "access denied" alert and prevents access.

In addition to creating authorized user profiles and accounts from the ES and IM Agreement and Profile forms information, OCSE developed the e-NMSN, e-IWO, and MSFIDM FAST Levy Profile forms to set up authorized users' process and capture preferences based on information collected from these program-specific profile forms.

OCSE also created a state profile form and uses information collected from states to establish certain process and capture preferences.

The information collected via the Portal registration process is also used by OCSE to track login activity, to provide general account and technical support, and to conduct an annual certification process against information in the NDNH to verify users that are active on the Portal but whose last certification date is greater than a year. A list of users with unverifiable information is sent to the Portal help desk for manual intervention.

3. Use of Improved Information Technology and Burden Reduction

The technology used to complete the ES and IM Agreement and Profile forms, and the e-NMSN, e-IWO, and MSFIDM FAST Levy Profile forms minimizes respondents' hourly burden because users populate the forms electronically, which eliminates the need to populate time-consuming paper forms or to contact the help desk to provide the profile information. OCSE can quickly create user registration profiles and authenticate the user from key information provided on the profile form. Additionally, the automated registration process immediately

captures information from the registration screens for use in verifying the authorized user, thereby eliminating the burden costs for users to mail paper forms.

4. Efforts to Identify Duplication and Use of Similar Information

The ES and IM Agreement and Profile, and the e-NMSN, e-IWO, and MSFIDM FAST Levy Profile forms request some of the same information that OCSE requests for other program requirements, such as name, employer, address, etc.; however, the purpose for which OCSE requires the information is unique to creating Portal profiles, authenticating Portal users, and establishing user preference. There is no possibility for duplication or use of similar information for the Portal registration and profile process because the Portal is unique to OCSE and allows only one account per authorized user.

5. Impact on Small Businesses or Other Small Entities

There is no impact on small businesses or other small entities.

6. Consequences of Collecting the Information Less Frequently

Submitting the Agreement and Profile, preferences Profile forms, and registering for Portal access is a one-time process. Not collecting the information required to authenticate users and Portal preferences will prevent OCSE from fulfilling a statutory requirement to restrict access to confidential information and its use by verifying the identity of authorized users. Consequently, this will increase the risk of unauthorized access to and use of sensitive child support case information and personally identifiable information.

7. Special Circumstances Relating to the Guidelines of 5 CFR 1320.5

There are no special circumstances.

8. Comments in Response to the Federal Register Notice and Efforts to Consult Outside the Agency

In accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104-13) and Office of Management and Budget (OMB) regulations at 5 CFR Part 1320 (60 FR 44978, August 29, 1995), OCSE published a notice in the Federal Register at 86 FR 38724 on July 22, 2021. The notice announced OCSE's intention to seek OMB approval of collection of information and to provide a 60-day comment period for the public to submit written comments about this information

collection activity. OCSE received a support letter from Washington state on September 20, 2021, complimenting OCSE on the benefits of the Portal.

9. Explanation of Any Payment or Gift to Respondents

Not applicable.

10. Assurance of Confidentiality Provided to Respondents

FPLS Security Framework provides secure access through the registration process. To ensure the confidentiality and security of the user's information and to prevent unauthorized access to the Portal, OCSE requires the following:

- Passwords on the OCSE Network are hashed using SHA-256.
- The Portal application uses TLS encryption. The Portal has its login server in the firewall's demilitarized zone (DMZ). Communications with the login server from outside must use TLS encryption.
- The OCSE Network employs custom-developed monitoring tools, such as Cisco IDS integrated in the routers and firewall, and techniques, such as port scanning, to monitor events and detect attacks on the information system. System log files provide another tool to detect unauthorized activity.
- System alerts are monitored daily for applicable advisories for the OCSE Network. Updates and security patch notifications are received and reviewed by network personnel to determine if they are applicable to the OCSE Network and to recommend appropriate actions, if any, in response to the alert or advisory.
- Social Security number (last four digits), date of birth, and responses to challenge questions are stored encrypted using the Advanced Encryption Standard, developed by the National Institute of Standards and Technology.
- A user ID, password, and a one-time access code are required to access the protected applications and data in the Portal.
- Session authenticity is ensured by integral HTTPS and TLS encrypted session management functionality. Multiple logins for the same user ID are not permitted. The system warns after 10 minutes of inactivity. After 15 minutes of inactivity, the session is ended. If the user closes the browser without logging out, the user is locked out and must wait 15 minutes to log in again.
- The Portal uses security software that monitors unsuccessful login attempts and will lock authorized user accounts after three failed login attempts. The user may attempt to access the Portal again in 120 minutes or call the Portal help desk.
- Account passwords expire every 60 days. The Portal monitors account

password expirations for all users. Notification is sent to the user on the 53rd day after the last date the password was changed advising that their password must be changed in seven days. On the 61st day, the password will expire, and users will need to use the password change function to reset their account.

- Password change processes require the user to know the registered email address and the answers to their five challenge questions that were set up at the time of registration. If the user answers three to four of the challenge questions correctly, the user is asked for the last four digits of their Social Security number and date of birth for further verification. Less than three requires the user to contact the Portal help desk.
- User accounts are inactivated after 15 months of inactivity. The user is notified on the 451st day of inactivity that their account will be inactivated in seven days. On the 459th day of inactivity, the account is inactivated. The user will need to reregister.

11. Justification for Sensitive Questions

OCSE's operation of the FPLS is a federal requirement for the primary purpose of helping child support agencies locate, establish, enforce, and collect child support. Sensitive information, if any, is justified because states are required to obtain sensitive information pertaining to the establishment of parentage and the establishment, modification, and enforcement of support obligations.

The Social Security number (last four digits) of an authorized user is collected during the registration process to verify the individual user's employment information through the NDNH. Additional information collected includes the name, date of birth, and employer information, which is necessary to ensure proper verification of individuals before creating an access account.

12. Estimates of Annualized Burden Hours and Costs

OCSE staff populated the collection instruments and completed the Portal registration screens to determine the following burden estimates:

ANNUAL BURDEN ESTIMATES

Information Collection Instrument	Total Number of Respondents	Total Number of Responses Per Respondent	Average Burden Hours Per Response	Total Annual Burden Hours	Average Hourly Wage	Total Annual Cost
Employer Services Agreement and Profile	9,508	1	0.08	760.64	\$34.58	\$26,302.93
Insurance Match Debt Inquiry Agreement and Profile	18	1	0.08	1.44	\$34.58	\$49.80
e-NMSN: Plan Administrator Profile	5	1	0.22	1.10	\$34.58	\$38.04
e-NMSN: Employer Profile	5	1	0.22	1.10	\$34.58	\$38.04
e-NMSN: State Profile	5	1	0.22	1.10	\$34.58	\$38.04
e-IWO S2S Profile	4	1	0.22	0.88	\$34.58	\$30.43
e-IWO NPO Profile	46	1	0.22	10.12	\$34.58	\$349.95
MSFI-FAST Levy Profile	5	1	0.08	0.40	\$34.58	\$13.83
Portal Registration Screens	1,254	1	0.15	188.10	\$34.58	\$6,504.50
Estimated Annual Burden Hour Total: 964.88					Estimated Annual Burden Cost Total:	\$33,365.56

OCSE calculated the hourly burden cost to respondents using the Bureau of Labor Statistics (BLS) job code for Social and Human Services Assistants [21-1093] and wage data from May 2020, which is \$17.29 per hour.

The increase in the total annualized costs from the previous approval is due to a slight increase in the hourly wage rate estimate derived from the most current BLS figures (<https://www.bls.gov/oes/2020/may/oes211093.htm>) and to the inclusion of fringe benefits and overhead. To account for fringe benefits and overhead, OCSE multiplied the hourly rate by two, or \$34.58.

The estimated annualized burden hour cost to respondents is \$34.58 times 964.88 or \$33,365.56

13. Estimates of Other Total Annual Cost Burden to Respondents and Record Keepers

Respondents and record keepers do not incur any other costs to register for the

Portal.

14. Annualized Cost to the Federal Government

OCSE maintains the registration screens and oversees the authentication process as part of the Portal system, which is a small part of the overall operational activities and cost. Costs for the annual operations, maintenance, and ongoing enhancements of the Portal framework and infrastructure include federal salaries and benefits of \$357,227 and contractor and hardware/software costs of \$6,035,132. Total Estimated Annualized Cost for the Portal system to the federal government is \$6,392,360.

15. Explanation for Program Changes or Adjustments

Adding the e-NMSN, e-IWO, and MSFIDM FAST Levy Profile forms constitutes a program change. This, coupled with the boost in Employer Services registrants, increased the burden hour estimates from the previous approval, which is reflected in the table of item A.12.

Changes to the federal government's annual cost from the previous information collection approval pertain to general increases to operate, maintain, and enhance the Portal framework. Ongoing Portal enhancements improve the services available to authorized users; however, they do not impact the respondent's overall burden to complete the registration process that must first be completed to obtain access to the applications maintained in the Portal system.

16. Plans for Tabulation and Publication and Project Time Schedule

Not applicable.

17. Reason(s) Display of OMB Expiration Date Is Inappropriate

Not applicable.

18. Exceptions to Certification for Paperwork Reduction Act Submissions

Not applicable.