DRAFT SUPPORTING STATEMENT
FOR
IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT SYSTEM

(3150-XXXX)
NEW

Abstract

The Nuclear Regulatory Commission (NRC) collects information from external partners and members of the public that have a need to use NRC's secure web-based applications. An applicant can request an external partner digital credential using NRC's web-based credential enrollment system. Once the applicant has obtained an NRC digital credential, it can be used to access select NRC secure web-based applications directly over the internet. The information collected is limited to identity information required for credential issuance processes and includes:

- Phone Numbers
- Email Addresses
- Physical Mailing Addresses
- Facial Photographs
- Photo Identity Documents
- Date of Birth
- Identity information from a U.S. Driver's License, U.S. Government PIV Card, U.S. Passport, U.S. Military ID card, U.S. Military dependent's ID card, Permanent Resident Card, Alien Registration Receipt Card (Form I-551) or Employment Authorization Document (Form I-766)

A. JUSTIFICATION

1. Need For the Collection of Information

The U.S. Federal Government has long valued secure credentialing and strong authentication for both federal employees and others accessing government information technology (IT) systems. Collecting information to perform identity proofing processes, consistent with the strength of the credential being issued, is an integral and necessary step.

The Office of Management and Budget (OMB) Memorandum, M-22-09, titled "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles" is the latest in a series of guidance and requirements to agencies in this area. Specifically, OMB M-22-09 reiterates that agencies should follow guidance from the National Institute of Standards and Technologies (NIST) as released in their Special Publication (SP) series. NIST SP 800-63-3, "Digital Identity Guidelines," and the sub-document, SP 800-63A, "Enrollment

and Identity Proofing," cover requirements for credential issuance and management. These requirements include collecting the subject information for purposes of identity proofing as the basis for credential issuance.

2. Agency Use and Practical Utility of Information

   All information received is used only for the purpose of identity proofing and credential issuance. The identity attributes collected are consistent with identity proofing guidance to Federal agencies published in NIST SP 800-63-3, "Digital Identity Guidelines," and the sub-document, SP 800-63A, "Enrollment and Identity Proofing."

3. Reduction of Burden Through Information Technology

   There are no legal obstacles to reducing the burden associated with this information collection. The NRC encourages respondents to use information technology when it would be beneficial to them.

   Respondents can submit the requested information via NRC's External Credentialing Service using fillable forms and/or computer-readable formatted forms. It is estimated that 100% of the potential responses are filed electronically.

4. Effort to Identify Duplication and Use Similar Information

   No sources of similar information are available. There is no duplication of requirements.

5. Effort to Reduce Small Business Burden

   Not applicable. Information is collected from individuals for the purpose of issuing individual identity credentials.

6. Consequences to Federal Program or Policy Activities if the Collection Is Not Conducted or Is Conducted Less Frequently

   If the information is not collected the NRC would not be able to verify the identities of application and system users and administrators. The information is collected once, at the time access is requested. Less frequent collection is not possible.

7. Circumstances Which Justify Variation from OMB Guidelines

   There are no variations from OMB Guidelines.

8. Consultations Outside the NRC

   Opportunity for public comment on the information collection requirements for this

clearance package has been published in the *Federal Register.*

9. Payment or Gift to Respondents

   Not applicable.

10. Confidentiality of Information

    Confidential and proprietary information is protected in accordance with NRC regulations at 10 CFR 9.17(a) and 10 CFR 2.390(b).

    This information is maintained in a system of records designated as NRC-45 Electronic Credentials for Personal Identity Validation and described at 84 FR 71538 (12/27/2019). This System of Record notice can be located at: https://www.nrc.gov/docs/ML2002/ML20022A257.pdf

11. Justification for Sensitive Questions

    Not Applicable.

12. Estimated Burden and Burden Hour Cost

    The NRC receives an estimated 250 requests for External Partner credentials annually. Each request takes on average 15 minutes to submit. The total annual burden is 62.5 hours (250 requests x 15 minutes request) at a cost of $18,750 (62.5 hours x $300/hr).

    There are no recordkeeping requirements imposed on requestors.

    The $300 hourly rate used in the burden estimates is based on the Nuclear Regulatory Commission's fee for hourly rates as noted in 10 CFR 170.20 "Average cost per professional staff-hour." For more information on the basis of this rate, see the Revision of Fee Schedules, Fee Recovery for Fiscal Year 2023 (88 FR 39120, June 15, 2023).

13. Estimate of Other Additional Costs

    There are no additional costs.

14. Estimated Annualized Cost to the Federal Government

    There are several annual cost components to the federal government to operate the infrastructure and identity proofing service. The categorical costs and annual cost estimates are below:

    - Application update costs - $10,000
    - Infrastructure (including security scanning and patching) - $6,000

- Government staff time – 15 minutes per request x 250 requests per year x $300/hr - $18,750

The total annual estimated cost is $34,750.

15. Reasons for Change in Burden or Cost

    This is a request for a new OMB clearance.

16. Publication for Statistical Use

    Not applicable.

17. Reason for Not Displaying the Expiration Date

    The expiration date will be displayed.

18. Exceptions to the Certification Statement

    There are no exceptions to the certification statement.