

Supporting Statement, Part A

Collection of Required Data Elements to Verify Eligibility OMB Control Number 0704-TBD

A. Justification

1. Circumstances Requiring Collection of Information.

This is a new collection of information necessitated by the Office of Personnel Management (OPM) cybersecurity incident in which approximately 21.5 million security clearance background investigation records containing personally identifying information (PII) were compromised.

The Department of Defense (DoD) is providing breach notification and facilitating the provision of breach mitigation services due to the number of DoD affected individuals. DoD entered into agreements with OPM to handle the breach notification and mitigation services. In response to this incident, OPM has partnered with all affected federal agencies; and, on behalf of these agencies, the DoD [Naval Sea Systems Command] has awarded a contract to provide identity protection and credit monitoring services to all impacted individuals and their minor children.

In order for impacted personnel to register themselves or their minor children for the services, they must provide a personal identification number (PIN). DoD commenced mailing out PINs to impacted individuals via U.S. Postal Service on September 30, 2015, and will continue for several weeks until all notifications have been mailed.

In September 2015, the Government determined it does not have current addresses for over 30% of the impacted population and therefore cannot mail out notification letters containing PINs to all impacted individuals. Consequently, those individuals whom the Government cannot notify do not have the necessary PIN to enroll for identity protection services. In order to provide the greatest likelihood for letter notification and opportunity for impacted individuals to take advantage of these services, the Government has established a secure website for individuals to request verification status by voluntarily providing the minimum PII needed to validate the individual's identity and U.S. mail contact information. To request verification status, individuals may either go directly to a secure OPM website screen and personally input the required data fields, or may call a helpdesk number where a contractor helpdesk attendant will take the information via telephone and input the information for the

caller. Thus, this collection of information is necessary for individuals to determine whether or not they were impacted by the OPM cybersecurity incident and, if impacted, provide the means to obtain a PIN to receive Government-provided identity protection services.

2. Purpose of the Information.

The information collected will be used only to verify whether or not an individual was impacted by the OPM cybersecurity incident involving background investigation records and to send a letter confirming status as "impacted" or "not impacted" by this incident. Once the minimally required information has been input into the OPM secure portal, it will be compared to an electronic master file and verification will be accomplished electronically. After the Government has validated the individual's status, the DoD Defense Manpower Data Center (DMDC) will generate and mail a response letter. This letter will either confirm eligibility and contain a PIN for impacted individuals, or confirm that the individual was not impacted by this cybersecurity incident.

The DoD DMDC will retain the information collected in a "holding file" until the contract end of performance on December 31, 2018. This will allow individuals who lose or never receive their PINs to use the portal and helpdesk to determine eligibility throughout the entire contract period.

3. Use of Information Technology.

If individuals desire to request verification they can provide the required information using the following options:

- a. Access the OPM website and submit the required data directly via secure OPM portal hosted by DMDC.
- b. Call a helpdesk number listed in the publicly accessible OPM website and provide the required data to a helpdesk attendant who will then enter and submit the data directly via a secure OPM portal hosted by DMDC.

The use of technology (online access) will decrease the burden on respondents to provide any more than the minimal data needed to verify eligibility. The online data entry portal allows respondents to enter data quickly and easily, as well as access additional helpful information such as frequently asked questions (FAQs).

4. Efforts to Identify Duplication.

The Government has convened an interagency task force to coordinate efforts on all matters concerned with the OPM

cybersecurity incident involving background investigation reports. Through this comprehensive task force, the chances of duplication or contradiction of efforts is mitigated.

5. Methods to Minimize Burden to Small Business.

This section is not applicable, as the requirement to collect information applies to individuals and not business entities.

6. Consequences to the Government.

The consequence of not collecting this data is that the Government cannot verify individuals' identity to determine if they are eligible for themselves and their minor children to enroll for identity protection and credit monitoring services. This results in impacted individuals being deprived of Government-provided services to which they are entitled.

7. Special Circumstances.

Collection of this information is consistent with 5 CFR 1320.5(d) (2). No special circumstances are required.

8. Publication for Comments.

As part of this request for an emergency submission, a 30-day Federal Register Notice soliciting public comments was published on 10/14/2015 in the Federal Register; Vol. 80, page 61796. Any public comments that are received by OMB will be addressed.

9. Payments or Gifts to Respondents.

The Government will provide no payment or gifts to respondents, other than remuneration of contractors in accordance with the terms of their contracts.

10. Assurance of Confidentiality to Respondents.

This information is disclosed only to the extent consistent with statutory requirements, current regulations, and prudent business practices. The Privacy Act Statement of the System of Records Notice (SORN) includes stipulations related to the release and disclosure of information collected.

In developing the system of records notice for this collection, the DMDC program manager carefully reviewed the safeguards established for the system to ensure they are compliant with all applicable requirements and are appropriate to the sensitivity of the information stored within this system. Any specific routine uses have been narrowly drafted to ensure the minimum amount of personally identifiable information is provided to accomplish a specific purpose.

11. Justification for Sensitive Questions. No questions of a sensitive nature are involved. Only the minimum information to validate an individual's identity and U.S. mail contact information is required.

12. Estimates of Information Collection Burden.

This collection of information allows any individuals who believe they were impacted by the recent OPM cybersecurity incident involving background investigation records to provide required data to validate their identity and notify them by letter sent via U.S. mail as to whether or not they were impacted by this incident. If they were impacted, the letter will contain a PIN to enroll for identity protection services. If they were not impacted, the letter will advise accordingly.

The Government has determined just under 21.5 million individuals were impacted by this incident. Out of this total population, the Government anticipates approximately five (5) million impacted individuals will choose to provide the required information to verify eligibility to receive identity protection services either by entering the information into the OPM secure website or calling the helpdesk and providing the required information to an attendant so the attendant can input the information into the OPM secure website. In addition to the impacted individuals, the Government estimates an additional approximately 14 million individuals who were not impacted by the incident will desire to provide the required information to determine whether or not they were impacted. For purposes of this information collection, the Government estimates a total of 19 million individuals who may choose to voluntarily provide the required information to verify eligibility to obtain Government-provided for identity protection services.

A. Number of respondents	19,000,000
B. Responses per respondents	1
C. Total responses	19,000,000
D. Hours per response (rounded)	.14
E. Total public burden hours	2,650,000
F. Cost per hour (average)	\$42
G. Total annual estimate of public burden	\$111,300,000

Note: For civilians, the hourly rate is based on the Base General Schedule Pay Scale for 2015, GS11, Step 5 of \$27.86 plus 36.25% overhead is \$37.96, rounded to \$38. For military, the rate is based on an O3 hourly rate of \$31.89 plus 36.25% overhead for a burdened hourly rate of \$43.45, rounded to \$43. The prorated combined hourly rate is \$42.07, rounded to \$42.

13. Annual Cost Burden to Respondents.

DoD does not estimate any burden hours apart from the hours estimated in items 12.

14. Annual Cost Burden to Federal Government.

The time estimate for responding to individual verification requests is based on the time it will take determine whether or not an individual has provided the necessary information required to validate his or her identity and send a letter, prepare a letter notification to send via U.S. mail, and provide oversight to all activities associated with verification. The total estimated time associated with this task is .021 hours per response.

A. Total responses	19,000,000
B. Hours per response	.021
C. Total hours	395,833
D. Cost per hour	\$38
E. Total Cost	\$15,042,000

Note: The hourly rate is based on the Base General Schedule Pay Scale for 2015, GS11, Step 5 of \$27.86 plus 36.25% overhead is \$37.96, rounded to \$38.

15. Program Changes or Adjustments.

This information collection is a new collection.

16. Publication.

Results of this information will not be tabulated or published.

17. Display of Expiration Date.

The Government is not requesting approval to omit display of the expiration date of OMB approval on the instrument of collection.

18. Exception to Certification Statement

The Government is not requesting exception to satisfy the statutory requirements.

19. Collections of Information Employing Statistical Methods:

The information collection under the program does not employ statistical methods.