Privacy Impact Assessment

National 800 Number Employer Verification Automated Telephone Application

- **Name of project**

  National 800 Number Employer Verification Automated Telephone Application

- **Describe the information we collect, why we collect the information, how we use the information, and with whom we share the information.**

  The National 800 Number Employer Verification (TNEV) Automated telephone application will allow employers or authorized third-party submitters (e.g., a payroll provider) to verify employee Social Security numbers (SSN) using the automated telephone portion of the Social Security Administration's (SSA) National 800 Number Network (N8NN). Only users who have successfully registered to use the SSA's Social Security Number Verification Service (SSNVS) online application will be able to use the automated TNEV application.

  Additional information about SSNVS may be found at www.socialsecurity.gov/employer/ssnv.htm. Employers and third-party submitters will be able to verify up to 10 employee SSNs using speech recognition technology through this automated telephone application.

  Collection of Information

  The TNEV application requires the use of the user ID and self-selected password acquired at the time of registration with SSA's Integrated Registration Services (IRES) Access Control Utility. The IRES user ID and password will be used to authenticate the identity of a user who chooses to verify employee SSNs using the TNEV application.

  Users will be prompted to speak their user ID and password and will only have a single attempt to pass authentication. If we successfully authenticate the user's credential in our records, the user will be prompted to speak the Employer Identification Number (EIN) of the company for which the names and SSNs are being verified. If the correct EIN is provided, the user will then be prompted to speak the employee's data elements (SSN, first and last name, date of birth (optional) and sex (optional)).

  SSA's telecommunications vendor will match the user's spoken user ID against a standard alpha/numeric 2.8 trillion grammar database. The vendor will subsequently collect and transmit the user's information (user ID and self-selected password) and the employees' data elements to our computer systems to provide the appropriate response code for each SSN verification request.

  We will match the data elements of the employees for which the names and SSNs are being verified with information in our Privacy Act system of records entitled, *Master Files of Social Security Number (SSN) Holders and SSN Applications,* (60-0058). We will match the EIN of the company of the employees for which the names and SSNs are being verified with

information in our Privacy Act system of records entitled, *Earnings Recording and Self-Employment Income System*, (60-0059). If the information provided by the user matches information in our records, the user will be provided the SSN verification. If the information provided by the user fails to match information in our records, the user will be advised to contact our Employer Reporting Service Center or the call will be transferred to a N8NN agent, as appropriate.

The information provided by TNEV will be shared only with users of the application. The TNEV application will not retain any of the information spoken by the user. All the information collected by the telecommunications vendor and transmitted to and used by the TNEV application will be dropped at the end of the call.

- **Describe the administrative and technological controls we have in place to secure the information we collect.**

  There is comprehensive IT Security Policy that provides technological and administrative controls over this process to ensure the electronic housing of records is controlled. Logical access is strictly limited to need to know and is supported by a separation of duties policy and strict adherence to least privilege access allowances.

  We annually provide authorized individuals with appropriate security and privacy awareness training that includes reminders about the need to protect personally identifiable information (PII) and the criminal penalties that apply to unauthorized access to, or disclosure of PII. Furthermore, authorized individuals with access to databases maintaining PII must annually sign a Systems Sanctions Violations – Agency Policy and Acknowledgment Statement, acknowledging their accountability for inappropriately accessing or disclosing such information.

  Additional access controls include the use of armed security guards that control entrances and exits to buildings housing the original records and the use of access controls such as personal identification numbers and passwords to gain access to records that are maintained electronically.

- **Describe the impact on individuals' privacy rights.**

  The agency collects information only where we have specific legal authority to do so. When we collect personal information from individuals, we advise them of our legal authority for requesting the information, the purposes for which we will use and disclose the information, and the consequences of their not providing any or all the requested information. Individuals can then make informed decisions as to whether they should provide the information.

- **Do we afford individuals an opportunity to consent to only particular uses of the information?**

  We advise individuals of the purpose for which we will use the information via the various forms/applications we use to collect information from individuals. We advise individuals that we will not disclose this information without their prior written consent unless we have specific legal authority to do so (e.g., per the Privacy Act).

- **Does the collection of this information require a new system of records under the Privacy Act (5 U.S.C. § 552a) or an alteration to an existing system of records?**

  No. We have established systems of records that govern the information we collect, use, and maintain for business purposes through this system and its various sub-systems. For example:

  - *Master Files of SSN Holders and SSN Applications,* (60-0058); and
  - *Earnings Recording and Self-Employment Income System*, (60-0059).

  Additionally, the authentication information that the user will provide to use the TNEV automated application will not be retained by the application.

Matthew Ramsey
Digitally signed by Matthew Ramsey
Date: 2025.02.11 14:25:42 -05'00'

Matthew D. Ramsey
Executive Director
Office of Privacy and Disclosure

Grace M. Kim
Digitally signed by Grace M. Kim
Date: 2025.02.11 17:50:26 -08'00'

Grace M. Kim
Chief Legal Counsel (General Law) and
Senior Agency Official for Privacy Delegee