



DEPARTMENT OF DEFENSE
NATIONAL SECURITY EDUCATION PROGRAM
1101 WILSON BOULEVARD, SUITE 1210
ARLINGTON, VIRGINIA 22209-2248

November 13, 2013

MEMORANDUM FOR DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE

THROUGH: OSD/JS PRIVACY OFFICE

SUBJECT: Justification for the Use of the Social Security Number (SSN) - for National Security Education Program net (NSEPnet)

NSEPnet is used by the National Security Education Program (NSEP) to track and record scholarship and fellowship recipients' progress in fulfilling their federal service requirements as mandated by federal law: 50 U.S.C. §1902, section (b). The use of the SSN within NSEPnet falls under acceptable use (8) Computer Matching. NSEP award recipients, who are not in compliance with the terms and conditions of their service agreement, are reported to the U.S. Department of Treasury for collection; the Department of Treasury requires the SSN as a unique identifier of the debtor. Recouping funds from NSEP award recipients is mandated by 50 U.S.C. §1902.

NSEP award recipients not in compliance with the terms and conditions are sent to the U.S. Department of the Treasury for collection. Because NSEP takes punitive action prior to interagency coordination, it is necessary to be absolutely certain that an award recipient under review, and not another award recipient sharing his or her name in good standing, is in fact delinquent. A SSN ensures that the records of an individual who receives two or more awards are linked within NSEPnet. Randomly generated database IDs cannot serve as a substitute for the SSN because a new record within NSEPnet is created each time an individual wins a new award. If that same individual receives a second award, using the SSN ensures that the second award record will be linked with the first (under the individual), and not generated separately. Using the SSN ensures that records of individuals sharing the same name remain distinct.

An individual accepting an NSEP award incurs a service requirement. Each award won comes with its own service requirement and accompanying terms and conditions. If multiple records pertaining to a single individual are not linked, it becomes impossible to concretely and authoritatively track his

or her progress towards fulfilling the service requirement. Conversely, if records pertaining to two separate individuals with the same name are not distinct, it is impossible to ensure that each award recipient is tracked appropriately according to his or her terms and conditions.

NSEPNnet is registered in the DoD IT Portfolio Repository (DITPR) with the DITPR identification number 14164. The applicable Systems of Records Notice is DHRA 09, located at <http://privacy.defense.gov/notices/osd/DHRA09.shtml>. A Privacy Impact Assessment, as well as a Paperwork Reduction Act Submission form, were submitted as parts of the OMB 83-I package for OMB 0704-0368 (OMB approval expires October 31, 2014).

To reduce the vulnerability of the SSN, paper and electronic media containing information is restricted to those who require the data in the performance of their official duties. Data systems that include SSNs are hosted in a DoD Information Assurance Certification and Accreditation Process-compliant facility, which is approved to operate by the Information Management Division of the Undersecretary of Defense for Personnel and Readiness. Ad hoc report files containing SSNs are encrypted, password-protected, and labeled For Official Use Only. Physical entry to the workstations engaging in SSN use is restricted by locks, guards, and administrative procedures. Contract officers are required to incorporate all appropriate Privacy Act clauses and contractor personnel are required to sign non-disclosure documents requiring them to comply with Privacy Act provision.



Judy Collier
Director of Outreach and Service