DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
OFFICE OF PRIVACY, CIVIL LIBERTIES, AND FREEDOM OF INFORMATION
1137 BRANCHTON ROAD
BOYERS, PA 16018-0618

August 7, 2024

MEMORANDUM FOR DEFENSE PRIVACY, CIVIL LIBERTIES, AND FREEDOM OF INFORMATION DIRECTORATE

THROUGH: *Defense Counterintelligence and Security Agency, Office of Privacy, Civil Liberties, and Freedom of Information*

SUBJECT: Justification for the Use of the Social Security Number (SSN) in Defense Information System for Security (DISS), DITPR ID #1640

1. System / Form Description

This memorandum is written to satisfy the requirement established in Department of Defense Instruction (DoDI) 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," that requires justification of the collection and use of the SSN in the NBIS-DISS application DITPR ID #1640.

DISS is an enterprise system supporting the DoD and expanding to support Federal Agencies for personnel security, providing a common, comprehensive medium to record, document, and identify personnel security actions including submitting adverse information, verification of clearance status (to include grants of interim clearances), requesting investigations, and supporting Continuous Evaluation (CE) activities.

2. Documentation

The information collected in DISS is covered by the Personnel Vetting Records System, DUSDI 02- DoD. (October 17, 2018; 83 FR 52420). DISS is secured to protect Personally Identifiable Information (PII) in accordance with the Privacy Act of 1974 and the system provides a Privacy Advisory to users that they are accessing a system that contains Privacy Act information. The Records Retention and Disposal Schedules for DISS are DAA-0446-2021-0009 and DAA-0446-2019-0004.

3. Authorized Uses

In accordance with DoDI 1000.30, Enclosure 2, paragraph 2.c.(3), use of the SSN within DISS falls under acceptable use *Security Clearance Investigation or Verification*. The SSN is the single identifier that links all aspects of a security clearance process together. The SSN is used to for initiation of personnel vetting (PV) activities, verification and linkage of PV records, the reduction of security clearance vulnerabilities, decreasing processing timelines, and to support simultaneous information sharing within various DoD entities, as well as among a number of authorized federal agencies. The DoD EDIPI is not an acceptable replacement for use of the SSN because DISS records and information are relied upon by other Federal agencies that continue to use the SSN as a primary identifier.

Acceptable Use Case 2.c. (3), Security Clearance Investigation or Verification. The

initiation, conduct, adjudication, verification, quality assurance, and billing fund control of background investigations and security clearances requires the use of the SSN. The SSN is the single identifier that links all aspects of these investigations together. This use case is also linked to other Federal agencies that continue to use the SSN as a primary identifier.

4. Citation and Migration Plan

Citation of statutory requirement for the use of the SSN is not applicable to DISS. Plan of Action for the migration from/elimination of SSN is not applicable to DISS. As explained above, the DoD EDIPI is not an acceptable replacement for the SSN as other Federal Agencies rely upon use of the SSN for subject and record verification, and information sharing.

5. Safeguards

Records and case files are maintained on a DoD network accessible only to authorized personnel who have been properly vetted to access the data. Access to records/case files are limited to only those person(s) responsible for reviewing/analyzing the record in the performance of their official duties and who are properly trained and have a need-to-know. Access to computerized data is restricted by passwords, which are changed periodically.

Access to personal information is restricted to those who require the records in the performance of their official duties, who are appropriately screened, investigated, and determined eligible for access. Access to personal information is further restricted by the use of Personal Identity Verification (PIV) cards, to include the DoD Common Access Cards (CAC), for Joint Verification System (JVS), Appeals, and Case Adjudication Tracking System (CATS). Access to information self-reported by the subject to the Security Officer is available by the use of a PIV. Physical entry is restricted by the use of locks, guards, and administrative procedures. All individuals granted access to this system of records are to have taken annual Information Assurance and Privacy Act training; and all have been through the information technology and/or security clearance eligibility process.

6. Point of Contact

For questions related to this memorandum contact: Sandra M. Langley, (410) 863-9995, sandra.m.langley.civ@mail.mil and/or Corrin J. Flick, (571) 456-9333, corrin.j.flick.civ@mail.mil.

LANGLEY.SANDRA.M.1229729272 Digitally signed by LANGLEY.SANDRA.M.1229729272 Date: 2024.08.12 12:30:22 -04'00'

Sandra M. Langley
DISS Product Owner/ISO
Defense Counterintelligence and Security Agency

ALLEMAN.LISA.M.1572059622 Digitally signed by ALLEMAN.LISA.M.1572059622 Date: 2024.08.13 13:30:47 -04'00'

Lisa M. Alleman
Chief Privacy Officer
Defense Counterintelligence and Security Agency