



PERSONNEL & READINESS  
FORCE RESILIENCY

## OFFICE OF THE UNDER SECRETARY OF DEFENSE

4000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-4000

JUN 26 2018

### MEMORANDUM FOR DEFENSE PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY DIVISION

THROUGH: OFFICE OF THE SECRETARY OF DEFENSE/JOINT STAFF PRIVACY

OFFICE      SHORT.MARY.V.1      Digitally signed by  
229496880      SHORT.MARY.V.1229496880  
Date: 2018.06.27 11:00:43 -04'00'

SUBJECT: Justification for the Use of Social Security Numbers Defense Sexual Assault  
Incident Database

Reference attached initial justification for the use of social security numbers (SSN) in the Defense Sexual Assault Incident Database (DSAID) dated May 2014. DoD Instruction 1000.30 requires this office to resubmit a justification when the System of Record Notice (SORN) was amended. The requirement to collect the SSN remains authorized.

Public Law 110-417, the Duncan Hunter National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2009, required the Department of Defense (DoD) to develop a centralized, case-level database for the collection and maintenance of information regarding sexual assaults involving a member of the Armed Forces. To fulfill this requirement as well as the reporting requirements outlined in 10 United States Code (U.S.C.) 113 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces, the Department developed and deployed DSAID. As the system of record for the Annual Report to Congress on Sexual Assault in the Military, DSAID maintains information (if available) about the nature of the assault, the victim, the alleged offender, investigative information, and case outcomes in connection with the assault. For reference, the DSAID DoD Information Technology Portfolio Repository (DITPR) number is 11499 and the Unique Investment Identifier (UII) number is 000003659.

Additionally, Public Law 114-328, the National Defense Authorization Act for Fiscal Year 2017, required the inclusion of new information in the Annual Report to Congress on Sexual Assault in the Military, specifically information on each claim of retaliation in connection with a report of sexual assault made by or against a member of the Armed Forces. DSAID, therefore, was amended to include information about the nature of such complaints of retaliation, the retaliation reporter, the alleged retaliator, the actions taken to support the reporter of retaliation, and nature and findings of the retaliation investigation.

The use case justifying the collection of the SSN in DSAID and on the DD Form 2965 is "Legacy System Interface" as outlined in DoD Instruction 1000.30, Enclosure 2, paragraph 2c(11) remains unchanged from the reference document. DSAID must continue to interface with Military Criminal Investigative Organization (MCIO) case management systems, which are legacy systems. Specifically, DSAID must interface weekly with the Department of the Army Law Enforcement Reporting and Tracking System, the Department of the Navy Consolidated

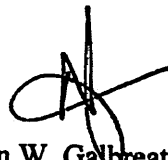
Law Enforcement Operations Center, and the Department of the Air Force Investigative Information Management System to capture case investigation data required for congressional reporting. These legacy systems report and track individuals, and make application information available to other agencies through the use of the SSN. The use of the SSN allows data matching and verification to be conducted to ensure the correct sexual assault case information is being pushed from the MCIO system to DSAID.

The legacy MCIO systems with which DSAID interfaces continue to use the SSN as the primary form of identification collected. The inclusion of the SSN in DSAID, therefore, remains necessary for the successful interface between DSAID and these systems. Once the legacy MCIO systems transition from the use of the SSN to another primary form of identification (e.g. the DoD Identification Number), DSAID will also transition from the use of the SSN. This office, in coordination with the DSAID Change Control Board, will continue to assess options for removal of the SSN as they become available.

We take safeguarding SSNs and other personally identifiable information collected and maintained in the system seriously. DSAID records are maintained in a controlled facility. Physical entry is restricted by the use of guards, identification badges, key cards, and locks. Access to case files in the system is role-based and requires the use of a Common Access Card, password, and can only be accessed from a .mil account.

DSAID continues to reside on the Office of the Secretary of Defense network. The protections on the network include firewalls, passwords, encryption of data, and use of a virtual private network. The local drive resides behind the firewall on the safe side and the direct database cannot be accessed from the outside. The system rests on the Nonsecure Internet Protocol Router Network. DSAID completed and met the requirements of the DoD Information Assurance Certification and Accreditation Process, receiving accreditation and authority to operate on April 4, 2016.

We are committed to continuously monitoring and evaluating the DSAID program and safeguarding the privacy of individuals whose information is contained in the system remains a priority. My point of contact is Ms. Darlene Sullivan, DSAID Program Manager, who may be reached at [darlene.l.sullivan.civ@mail.mil](mailto:darlene.l.sullivan.civ@mail.mil).



Nathan W. Galbreath, Ph.D.  
Deputy Director, Sexual Assault Prevention  
and Response Office

Attachment:  
As stated