DEPARTMENT OF DEFENSE
DEFENSE PRIVACY AND CIVIL LIBERTIES DIVISION
241 18TH STREET SOUTH, SUITE 101
ARLINGTON, VA 22202-3405

May 18, 2015

MEMORANDUM FOR DEFENSE FINANCE AND ACCOUNTING SERVICE
PRIVACY OFFICE

SUBJECT: Justification for the Continued Use of Social Security Numbers in Case Management System-DITPR #8679 – Accepted Pending Correction

Thank you for completing your review of Social Security Number (SSN) use within your system. Removal of the SSN from your system is an important step towards reducing the Department's reliance on this sensitive information and fulfilling our obligation to protect the individuals about whom we maintain records. After review, the Defense Privacy and Civil Liberties Division (DPCLD) has accepted your justification for SSNs in the system, pending corrections (see attached).

If you have any questions, please contact Mr. Brent Bice at (703) 571-0070 or e-mail brent.j.bice.civ@mail.mil.

ERWIN.WILLIAM.LYLE.1116783610
Digitally signed by ERWIN.WILLIAM.LYLE.1116783610
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=OSD, cn=ERWIN.WILLIAM.LYLE.1116783610
Date: 2015.05.18 09:04:11 -04'00'

William L. Erwin
Acting Chief

Attachments:
As stated.

SSN Use Justification Memo for DEFENSE FINANCE AND ACCOUNTING SERVICE May 18, 2015		
DITPR Number/ System Name	**DPCLD Findings**	**DPCLD Recommend Action**
8679/Case Management System	Use Case on DITPR states 11 "Legacy System Interface", justification memo states use case 8 "Computer Matching"	Update DITPR system to match justification memo, use case 8 "Computer Matching"

DEFENSE FINANCE AND ACCOUNTING SERVICE
8899 E. 56TH STREET
INDIANAPOLIS, IN 46249

DFAS-ZT

MEMORANDUM FOR DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE

SUBJECT: Justification for the Use of the Social Security Number (SSN) Case Management System (CMS)

CMS is a web-based, management tool system used by the Defense Finance Accounting Service for tracking, resolving and reporting on military pay and personnel related cases for Army and National Guard Active Duty and Reserve members. It provides a single source of information for monitoring military pay problems in a timely and efficient manner, including visibility to appropriate levels of management, permitting feedback to service members, and facilitating the identification of problem trends. CMS maintains: System Identification 2410, System of Record Notice Identification T7340b, and DoD Information Technology Portfolio Repository Record No. 8679. The SSN is the method of identification used by the military. The Defense Joint Military System (DJMS) uses the SSN to process and research pay record information. When corrective action needs to be taken on a military pay member account, a case is created and steps to resolve the case are tracked in CMS. The case uses the SSN as the primary identifier for the military member. The intended use of the SSN is for mission-related and administrative use.

The justification for the use of the SSN and/or TIN is DoDI 1000.30, Enclosure 2, Paragraph 2.c. (8) "Computer Matching". Financial institutions may require that individuals provide the SSN as part of the process to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial institutions.

The authority for this DoD information system to collect, use, maintain, and/or disseminate Personally Identifiable Information is found in the following: 5 U.S.C. 301, Departmental Regulations; Department of Defense financial Management Regulations, Chapter 20; 31 U.S.C. Sections 3511, 3512 and 3513; and E.O. 9397 (SSN).

Justification The SSN is currently being used by CMS until a replacement is identified by Military Pay Operations, at which time CMS would fully cooperate to be in compliance with this action.

CMS has taken the following measures to mitigate risk associated with using the SSN:

- Access to the facilities is restricted to authorized DoD employees and authorized contractors.
- Managed firewalls prevent access by other systems or network traffic not specifically identified in the firewall rule base.
- Access controls limit access to the application and/or specific functional areas of the application. Individuals are granted access to the system only after they have been verified to have a defined need to access the information and have gone through background and employment investigations, and are required to take yearly Information Assurance training and Spirit Training. Users are given only those system privileges based on their need to know, and which are necessary for their job requirements.

A security Certification and Accreditation (C&A) for the system was completed in accordance with the requirements of the Federal Information Security Act of 2002. The C&A process is an audit of policies, procedures, controls, and contingency planning, required to be completed for all federal government IT systems every three years, and is also reviewed at least annually for maintenance. The C&A process includes review and renewal of a Privacy Act Assessment (PIA). The last PIA review was conducted in September, 2012.

DFAS adheres to physical protections of Personally Identifiable Information (PII) as described in accordance with DFAS 5200.1-R. IA Policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include PII, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8500.1. Authority for Maintenance of the System: 5 U.S.C. 301, Departmental Regulations; 37 U.S.C. Chapters 1-19; DoD Financial Management Regulations 7000.14-R; and E.O. 9397 (SSN).

GILLISON.AARON.PETER.1180905290

Digitally signed by GILLISON.AARON.PETER.1180905290
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DFAS, cn=GILLISON.AARON.PETER.1180905290
Date: 2015.03.09 12:36:15 -04'00'

Aaron P. Gillison
Director, Information and Technology