OFFICE OF THE CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

OVERSIGHT AND
COMPLIANCE

April 3, 2019

MEMORANDUM FOR THE DEFENSE FINANCE AND ACCOUNTING SERVICE

SUBJECT: Justification for the Use of Social Security Numbers in OnePay, DITPR ID # 29 - Accepted

Thank you for completing a review of Social Security Number (SSN) use within this system. The Defense Privacy, Civil Liberties and Transparency Division (DPCLTD) has reviewed this request and has accepted your justification to use the SSN for the purpose of Acceptable Use (7) Federal Taxpayer Identification Number, to prepare IRS Form 1099. This system must be reviewed on a continuous basis and a new justification must be provided if any change to the System of Records Notice is submitted.

Acceptable Use (4) Interactions With Financial Institutions, was not accepted. OnePay only outputs data to the Automated Disbursing System (ADS) and does not directly interact with any financial institution.

While this system has been identified as requiring the collection, maintenance and use of the SSN, you must ensure this data is afforded the highest protections practicable through use of appropriate administrative, technical and physical safeguards. Also, please maintain a copy of your justification and this memo in your records.

SSN Justifications must be renewed three (3) years after the date of this memorandum if the associated System of Records has not been updated.

If you have any questions, please contact Ms. Cheryl Jenkins at (703) 571-0026 or e-mail, cheryl.d.jenkins2.civ@mail.mil.

ALLARD.CINDY.L.1231656614 Digitally signed by ALLARD.CINDY.L.1231656614 Date: 2019.04.03 11:54:21 -04'00'

Cindy L. Allard
Chief, Defense Privacy, Civil Liberties,
and Transparency Division

DEFENSE FINANCE AND ACCOUNTING SERVICE
8899 EAST 56TH STREET
INDIANAPOLIS, IN 46249-3300

DFAS-ZTC

MEMORANDUM FOR DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE

SUBJECT: Justification for the Use of the Social Security Number (SSN) and/or Tax Identification Number (TIN) - One Pay

The Defense Finance and Accounting Service employs a system called One Pay which is an online commercial entitlement (accounts payable) system. The single payment system is operated in a teleprocessing environment, but is designed to accept batch invoice input from both Electronic Data Interchange (EDI) and remote site batching systems. The system provides invoice tracking, online inquiry, invoice status reports and disbursing reports. One Pay also provides a report of expenditures to the U.S. Treasury in electronic and hardcopy form. One Pay is fully operational and deployed worldwide to Navy and DFAS Locations. The last signed Privacy Impact Assessment performed as part of the accreditation process was completed and signed on December 15, 2017.

The justification for the use of the SSN and/or TIN is DoDI 1000.30, Enclosure 2, Paragraph 2.c. (4) “Interactions with Financial Institutions”, necessary to ensure payment to payees; and 2) DoDI 1000.30, Enclosure 2, Paragraph 2.c (7) “Federal Taxpayer Identification Number”, necessary for the preparation of IRS Form 1099.

The authority for this DoD information system to collect, use, maintain, and/or disseminate Personally Identifiable Information (PII) 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). The DOD IT Portfolio Repository (DITPR) identifier for this system is 29.

Justification for the use of the SSN does not constitute blanket permission to use the SSN. One Pay has taken steps to safeguard SSN's by limiting the access to persons authorized to service or to use the system in performance of their official duties (requires screening and approval for need to know). Additionally, One Pay has implemented the use of various technical and administrative controls which provide added security. Technical controls for the protection of all PII, including SSN (identified in the PIA) include user identification, password use, intrusion detection system, encryption, firewall, virtual private network, DoD public key infrastructure certificates, and common access card. Administrative controls (identified in the PIA) include periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel access to PII, and backups secured at offsite locations, among others.

BLUE.TERESA.1229141208 Digitally signed by BLUE.TERESA.1229141208 Date: 2017.12.20 06:58:22 -05'00'

Ronald Murlin
Director, I&T Accounting Services