DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

MEMORANDUM FOR DEFENSE PRIVACY CIVIL LIBERTIES AND TRANSPARENCY DIVISION

SUBJECT: Social Security Number Justification for Defense Logistics Agency Joint Contingency and Expeditionary Services (JCXS) Portfolio, Civilian Armed Authorization Management System (CAAMS) Information System

Department of Defense Instruction (DODI) 1000.30, "*Reduction of Social Security Number (SSN) Use Within DoD*," (August 1, 2012), requires all DoD personnel to reduce or eliminate the use of SSNs wherever possible, except when the use of the SSN meets one or more of the acceptable use criteria DoDI 1000.30 establishes. To continue use of the SSN in a system or form, DLA must provide a memorandum justifying the continued use to the Defense Privacy, Civil Liberties, and Transparency Division.

This memorandum serves to justify the continuing need for the collection and use of CAAMS. The CAAMS information system has a Privacy Impact Assessment (PIA) and maintains records from the following DLA Privacy Act systems of records notices (SORNs):

Joint Contingency and Expeditionary Services (Pending SORN)

Under the DODI 1000.30, Enclosure 2, section 2, paragraph c, there are 13 designated acceptable uses for SSNs. The designated acceptable use for the CAAMS information system is as follows:

> *"(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 of the 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."*

Information collected directly from the public is captured via DD Form 2760 – Qualification to Possess Firearms and Ammunition. This collection is in accordance with Sections 3501-3520 of the Paperwork Reduction Act.

The SSN is used within the DLA CAAMS information system by DLA Contingency Capabilities Portfolio, DLA Installation Support, DLA Office of the Inspector General, DLA Office of General, Department of Defense, and United State Armed Forces –Afghanistan (USFOR-A), Armed Contractor Oversight Directorate (ACOD). Counsel personnel to refer and investigate reported incidents; to ensure proper maintenance and safekeeping of privately owned firearms by personnel residing on DoD controlled premises or who are required to register firearms with DoD.

The SORNs used for the CAAMS information system cite several authorities for the collection and maintenance of the records it contains. These include: FRAGO 16-143 MOD-1, Arming Exception to Policy Contractors, and Title 18, United State Code, Section 922(g)(9), purpose of use of DD Form 2760.

DLA Contingency Capabilities Portfolio gathers this information and safeguards it. The CAAMS information system will be protected by DLA policies on Information Assurance. All infrastructure supporting the CAAMS information system will have all applicable Security Technical Implementation Guides (STIGs), checklists, and vulnerability scans applied. Additionally, only DLA Contingency Capabilities Portfolio, DLA Installation Support, Security and Emergency Services (DM-S) personnel, and DLA Office of General counsel attorneys are authorized access to records within or from CAAMS. Personnel are vetted by the designated CAAMS installation application administrative officer, prior to granting access to the system. Each CAAMS installation application administrator has the ability to add, modify, and deactivate users from their site-specific portion of the CAAMS information system. Access requires Common Access Card (CAC) authentication and use of a unique user identification and DoD-compliant password. Insider and outsider threats for information theft, hacking, etc., are mitigated through the use of encryption,; and ensuring compliance with information assurance and other DOD Directives, policies and procedures for DOD use and implementation of Commercial-Off-the-Shelf (COTS) applications. The assigned Information System Security Manager (ISSM) reviews associated risks and provides detailed information to both the DLA Chief Privacy and FOIA Officer and the DLA decision authority for acceptable/non-acceptable use and maintains applicable Plan of Action and Milestones (POA&M) for security and privacy controls. Significant changes to the (NOS) information system are reviewed for privacy implications by the DLA Chief Privacy and FOIA Officer.

My signature below constitutes approval and justification for continued use and storage of SSNs in the CAAMS information system.

My points of contact are Mr. Greg Riley, Contingency Capabilities Portfolio, at 571-767-3996, DSN 392-767-3996, e-mail: greg.riley@dla.mil and Ms. Stacy Simmons, Contingency Capabilities Portfolio, at 571-425-7409, e-mail: stacy.simmons@dla.mil.

PATRICK J. DULIN
Acting Director, DLA Information Operations
Chief Information Officer

The below signature serves as acknowledgement that this document has been reviewed by the DLA Chief Privacy Officer.

Kathy Dixon, CIPP/US/G
DLA Deputy Chief FOIA and Privacy Officer