



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 PoliceCenter (POLC) 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 the SSN for the Police Center (POLC) information system. The POLC information system has a Privacy Impact Assessment (PIA) and maintains records from the following DLA Privacy Act systems of records notices (SORNs):

- S500.30 – Incident Investigation/Police Inquiry Files
- S500.41 – Vehicle Traffic Incident Files
- S500.42 – Seizure and Disposition of Property Records
- S500.43 – Firearms Registration Records
- S500.50 – Facility Access Records

Please note that DLA is working to combine the above referenced SORNs into a single SORN covering the enterprise collection and administration of DLA police incident investigation, seized property management, firearms registration, and facility access related records. When the new SORN is published a revised SSN Justification Memo will be provided.

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 POLC information system is as follows:

“(2). Law Enforcement, National Security, and Credentialing. Almost every law enforcement application available to Federal, State, and local law enforcement and other criminal justice agencies reports and tracks individuals, and makes application information available to other agencies, through the use of the SSN. This includes, but is not limited to, checks of the National Crime Information Center; State criminal histories; and Federal Bureau of Investigation records checks.”

Information collected directly from the public is captured via DLA Form 635. This collection is in accordance with Sections 3501-3520 of the Paperwork Reduction Act and has an OMB Collection number (0704-0514).

The SSN is used within the DLA POLC information system by DLA Police, DLA Installation Support, DLA Office of the Inspector General, and DLA Office of General Counsel personnel to refer and investigate reported incidents; to monitor the progress of cases; to ensure proper maintenance and safekeeping of privately owned firearms by personnel residing on DLA controlled premises or who are required to register firearms with DLA; to

control access into DLA-managed installations, buildings, facilities, and parking lots; to verify security clearance status of individuals requiring entry into restricted access areas; and to relay threat situations and conditions to DoD law enforcement officials for investigative or evaluative purposes.

The SORNs used for the POLC information system cite several authorities for the collection and maintenance of the records it contains. These include: 5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 303(b), Oath to Witnesses; 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1580, Emergency Essential Personnel, designation; DOD Directive 5210.56, Arming and the Use of Force; 10 U.S.C. 1585, Carrying of Firearms; 10 U.S.C. 1593, Uniform allowance: civilian employees; 18 U.S.C. 499, Military, Naval, or Official Passes; 18 U.S.C. 701, Official Badges, Identification Cards, Other Insignia; 18 U.S.C. 716, Police Badges; National Highway Safety Act of 1966 (23 U.S.C. 401, Highway Safety, et seq.); Section 21 of the Internal Security Act of 1950 (50 U.S.C. 797, et seq.); DOD Instruction 5200.8, Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB); DOD Instruction 6055.17, DOD Emergency Management (EM) Program; CJCSI 3121.01B, Standing Rules of Engagement/Standing rules for the Use of Force for US Forces; DOD Directive 5105.22, Defense Logistics Agency; and E.O. 9397 (SSN) as amended by E.O. 13478.

DLA Police gather this information and safeguard it. The POLC information system will be protected by DLA policies on Information Assurance. All infrastructure supporting the POLC information system will have all applicable Security Technical Implementation Guides (STIGs), checklists, and vulnerability scans applied. Additionally, only DLA Police Officers, 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 the POLC. Personnel are vetted by the designated POLC installation application administrative officer, prior to granting access to the system. Each POLC installation application administrator has the ability to add, modify, and deactivate users from their site-specific portion of the POLC 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 POLC 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 POLC information system.

My points of contact are Mr. Alexander Logan (DLA Police Files) and Mr. Gerald Barb (DLA Access Control Files), DLA Installation Support, Security and Emergency Services, at (571)767-3071, DSN 392-3071, e-mail: alexander.logan@dla.mil or (571)767-5425, DSN 392-5425, email: Gerald.barb@dla.mil.

KATHY CUTLER
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.

LEWIS OLEINICK, CIPP/US/G
DLA Chief FOIA and Privacy Officer