**PRIVACY IMPACT ASSESSMENT**
**For Contractor Tracking System (COTS 2)**

1. **Department of Defense Component:** Defense Logistics Agency.

2. **Name of Information Technology (IT) System:** Contractor Tracking System (COTS 2).

3. **Budget System Identification Number (SNAP-IT Initiative Number):** N/A.

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository):** N/A.

5. **IT Investment Unique Identifier (OMB Circular A-11):** N/A.

6. **Privacy Act System of Records Notice Identifier:** S500.10, entitled "Personnel Security Files."

7. **OMB Information Collection Number and Expiration Date:** OMB No. 3206-0005, expires September 20, 2008. Questionnaires and Supplemental Form for National Security, Public Trust, and Non-sensitive Positions (Standard forms (SF) SF-86, SF-85, SF-85PS, SF-86C, E-QIP, SF-86A).

8. **Authority to Collect Information:** 5 U.S.C. 301, Departmental Regulations; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; E.O. 10450, Security Requirements for Government Employment; E.O. 12958, Classified National Security Information; DoD Regulation 5200.2, DoD Personnel Security Program; and E.O. 9397 (SSN).

9. **Brief Summary or Overview of the IT System:** The IT System is used to track contractor suitability, eligibility, and qualifications for federal contracts or access to classified information.

10. **Identifiable Information to be Collected and Nature / Source:** Individual's name and Social Security Number.

11. **Method of information collection:** Records are collected on paper or electronically from the subject individual or from investigative reports.

12. **Purpose of collection:** Records are collected and maintained for the purpose of determining an individual's suitability, eligibility, or qualifications for federal contracts, or access to classified information.

13. **Data uses:** Personnel Security Specialists in the Public Safety Offices use the records to determine whether an individual is suitable, eligible, or qualified for federal contracts, and whether or not the individual may occupy a sensitive position and/or have access to classified information.

14. **Does system derive / create new data about individuals through aggregation?** N/A.

15. **Internal and External sharing:**
Internal to DLA: Data may be viewed by or shared with DLA Security Managers and DLA Personnel Security Specialists for the purpose of determining an individual's eligibility to occupy a sensitive position and/or access to classified information and to determine suitability, eligibility, or qualifications for federal contracts.
External to DLA: The DOD "Blanket Routine Uses" apply to the Privacy Act system of records, S500.10. DOD blanket routine uses may be found at http://www.defenselink.mil/privacy/notices/blanket-uses.html .

16. **Opportunities to object to the collection or to consent to the specific uses and how consent is granted:** All personal data collected is voluntarily given by the subject individual. Forms that collect personal data to be maintained in this IT system contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises the individual that the information provided is voluntary; and provides the consequences of choosing not to participate with the information collection. Individuals may raise an objection with the DLA HQ Privacy Act office during the public comment period of the Privacy Act system of records notice (if applicable) or during the data collection.

17. **Information Provided the Individual at Collection, the Format, and the Means of Delivery:** A Privacy Act system of records notice has been published in the Federal Register with a 30-day public comment period. Forms collecting personal information contain Privacy Act Statements, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the information. Individuals may raise an objection with the HQ DLA Privacy Act Office during the 30-day public comment period, during data collection, or at any time thereafter. If no objections are received, consent is presumed.

18. **Data Controls:**
Administrative: Access to COTS will be controlled by the Standard Login Interface Module (SLIM). Designated DES-S personnel will be assigned as system administrators and will review and approve all COTS users. COTS users may request an account by completing a registration on the COTS web site. SLIM will notify system administrators and requester that the account request has been received. COTS system administrators will review and approve/disapprove request and user will be notified accordingly. COTS users will be restricted to managing records to their respective organizations but will be able to view all records in the system. DES-S system administrators will have access (view and edit) to all COTS records.
Physical: All personnel entering the building must have appropriate identification, visitors are escorted. Server room is secured and access is restricted to authorized personnel only, visitors are escorted. Servers require CAC or other privileged authentication and access is limited to approved administrators.

Technical: COTS data is stored on a combination of web and database servers. An end user, using their web browser, will pass through the firewall to the appropriate web server. The web server will interface with the database server, process the transaction, and pass data back to the end user's browser. Development and test web and database servers are also used. Access to COTS will be controlled by the Standard Login Interface Module (SLIM). SLIM/COTS users are authenticated by a mandatory username/password combination (or CAC access, if appropriate). Any invalid attempts to access the application are recorded by the system and user accounts are locked after three invalid attempts. Passwords are encrypted in transmission, stored, and expire after 90 days.

19. **Privacy Act Interface.** S500.10, entitled "Personnel Security Files."

20. **Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent or to providing notices to the individual; risks posed by the adopted security measures:**
Threats: Threats to the collection, use, and sharing of data are alleviated by collecting and maintaining the data in a secure and accredited system. All system users are made aware of restrictions on secondary uses of the data by initial and refresher Privacy Act and Information Assurance training. In addition, data sharing occurs only among individuals authorized access to the system of records as stated in the governing Privacy Act system notice.
Dangers: There are no dangers in providing notice of the collection or allowing an individual to object/consent. Therefore, individuals are given this opportunity at times of notice publication and data collection. Afterwards, individuals may raise objections if new threats are perceived.
Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

21. **Classification and Publication of Privacy Impact Assessment:**
Classification: Unclassified.
Publication: This document will be published either in full or in summary form on the DLA public website, http://www.dla.mil/public_info/efoia/privacy.asp .

**Data Owner:** [redacted] (Signature) 02/25/08 (Date)

Name: [redacted]
Title: Staff Director, Public Safety, HQ DLA
Work Phone Number: [redacted]
Email: [redacted]

**Information Assurance Officer:** [redacted] (Signature) 3/20/08 (Date)

Name: [redacted]
Title: Information Assurance Manager [redacted]
Work Phone Number: [redacted]
Email: [redacted]

**Chief Privacy Officer:** [redacted] (Signature) 3/20/08 (Date)

Name: For Lewis Oleinick
Title: Chief Privacy and FOIA Officer
Work Phone Number: [redacted]
Email: [redacted]

**Reviewing Official:** [redacted] (Signature) APR 10 2008 (Date)

for Name: Mae De Vincentis
Title: DLA Chief Information Officer
Work Phone Number: [redacted]
Email: [redacted]