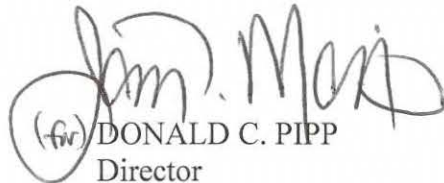May 6, 2015

MEMORANDUM FOR DOD ACTIVITY ADDRESS DIRECTORY (DoDAAD) PROCESS REVIEW COMMITTEE (PRC)

SUBJECT: Approved Defense Logistics Management Standards (DLMS) Change (ADC) 1143 for DoDAAD Data Security Controls (DoDAAD)

The attached change to DLM 4000.25, Defense Logistics Management System, is approved for immediate implementation.

Addressees may direct questions to Tad DeLaney, DoDAAD PRC Chair, at 703-767-6885, DSN 427-6885, or email: DODAADHQ@DLA.MIL. Others must contact their Component/Agency designated representative.

(for) DONALD C. PIPP
Director
Defense Logistics Management
Standards Office

Attachment
As stated

cc:
ODASD(SCI)
ODASD(DPAP)
OUSD(C)

ADC 1143
DoDAAD Data Security Controls
(DoDAAD)

1. ORIGINATING SERVICE/AGENCY AND POC INFORMATION:

    a. Technical POC: Defense Logistics Management Standards Office, DoDAAD PRC Chair, Tad DeLaney, at 703-767-6885, e-mail: DODAADHQ@dla.mil

    b. Functional POC: Defense Logistics Management Standards Office, DoDAAD PRC Chair, Tad DeLaney, at 703-767-6885, e-mail: DODAADHQ@dla.mil

2. FUNCTIONAL AREA:

    a. Primary Functional Area: DoDAAD

    b. Secondary Functional Processes: MAPAD, Supply, and Finance

3. REFERENCES:

    a. DLM 4000.25, Defense Logistics Management System (DLMS), Volume 6, Chapter 2, Department of Defense Activity Address Directory.

    b. ADC 385, DoD Activity Address Directory (DoDAAD) Enhanced Inquiry and Download for Multiple DoDAACs (DoDAAD).

    c. OSD Director of Administration Determination of December 18, 2014.

    d. DoDD 8550.01, DoD Internet Services and Internet-Based Capabilities, September 11, 2012.

    e. DoDM 5200.01, DoD Information Security Program: Marking of Classified Information, Volume 2, February 24, 2012.

4. APPROVED CHANGE(S): (Changes from PDC 1143 are highlighted in yellow.) For the purposes of this DLMS Change, "DoDAAD data" means multiple DoDAACs and/or RICs and their associated data elements. It does not mean a single DoDAAC or RIC and its own data elements. Additionally, for the purpose of this DLMS Change, the access to DoDAAD data being addressed is that of read access that enables a user to dynamically query the database and extract multiple DoDAACs, RICs, and/or their respective data attributes, en masse -- also known as Enhanced Defense Automatic Address System Inquiry (eDAASINQ).

    a. Brief Overview of Change: Implement additional controls for access to DoDAAD data that safeguard the handling of DoDAAD data, which has been designated as Controlled Unclassified Information (CUI) For Official Use Only (FOUO), and that assure proper management control on behalf of the Federal Departments to whom the data belongs (i.e., Department of Defense (DoD), Department of Justice (DOJ), Department of Transportation (DOT), etc.). Note: For the purposes of this DLMS Change, use of the term "Components" used herein is intended to mean all Departments of the Federal Government who use the DoDAAD (i.e., DoD, Federal Agencies, etc.).

b. Background: Reference 3.b. requested designation of DoDAAD data as being For Official Use Only (FOUO). In response to this, a pop-up screen was implemented in eDAASINQ that notified users that the "capability to download eDAASINQ data is restricted to Common Access Card (CAC)/Public Key Infrastructure (PKI) protection and requires a System Authorization Access Request." This is not the same as designating the data (in all its various exportable formats) as being FOUO and does not meet the requirement levied by the Intelligence Community to assure the data is safeguarded. In response to this, reference 3.c. determined that the DoDAAD meets the criteria for "Exemption 3 of the Freedom of Information Act (5 U.S.C. § 552(b)(3)) because it meets the requirements for exemption under 10 U.S.C. § 130e." Specifically, the Director of Administration made the following determination:

"In accordance with 10 U.S.C. § 130e, I reviewed the information provided to me by the Defense Logistics Agency concerning the Department of Defense Activity Address Directory (DoDAAD) database as a single authoritative source for the Department of Defense (DoD) business enterprise architecture and determined that it qualifies as DoD critical infrastructure security information (CISI). As defined by 10 U.S.C. § 130e, CISI includes:

'…sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security.'

"The DoDAAD meets this definition of CISI because it is comprised of both Department of Defense Activity Address Code (DoDAAC) and Routing Identifier Code (RIC) identifiers in an interactive relational database serving as a single authoritative source of identification, routing, and address information for authorized users, including Military Components and Agencies, participating Federal Agencies, authorized contractors, and authorized special program activities such as state and local governments (DLM 4000.25 Volume 6, December 19, 2013). DoDAAD supports business application systems data and interoperability requirements, including (but not limited to) supply chain, materiel procurement, and acquisition systems. Each activity that requisitions, contracts for, receives, has custody of, issues, or ships DoD assets, or funds/pays bills for materials and/or services is identified by a DoDAAC (six-position alphanumeric code).

"DoDAACs are used in a myriad of business systems spanning the entirety of the DoD's business enterprise architecture, including acquisition, procurement, contracting, requisitioning, shipping, billing, pay, maintenance, installations management, human resources, energy resources, and the accountability and requisition of ordnance, ammunition, and perishables in logistics systems across the DoD. DoDAACs are also used for business operations involving the accountability of property and facilities, as well as for hazardous material management. Access to the DoDAAD allows access to these DoDAACs. When coupled with access to other unclassified logistic systems, users are provided with multiple data points which, when combined, disclose

location of materials and operational status and plans. If the DoDAAD is released it would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD.

"The contents of the DoDAAD are sensitive for a number of reasons:

- DoDAACs are created to support sensitive operations and to facilitate the business process associated with them.
- DoDAACs for the following locations include names of employees and Service members as well as duty station addresses for:

  a. Department of Defense installations and ports that are outside the contiguous United States (OCONUS)
  b. Deployed units and activities performing real world contingency operations or exercises from both contiguous United States (CONUS) and OCONUS bases
  c. Ships afloat
  d. Ships still in CONUS ports but scheduled to go afloat
  e. Ships still in OCONUS ports but scheduled to go afloat
  f. Embassies
  g. War Reserve Equipment sets pre-positioned OCONUS

"If an adversary had the DoDAAD they could determine the issuance of orders; the movement of specially qualified personnel to units and the installation of special capabilities, as well as the conduct of activities in a way that will reveal intensification of preparations before initiating operations. From this information, the adversary could identify very sensitive DoD activities including clandestine locations of DoD activities, force structure, and even troop movement.

"In addition, a DoDAAC could be used in an unauthorized way whereby the internal controls of the Agency can be circumvented and appropriations obligated without the proper authority being involved in the process. A DoDAAC is very much like a credit card number which, in the wrong hands, can be used to spend money without the rightful "owner" of the code (i.e., the entity with authority to use the code) being aware that the Agency's appropriations are being spent. Individuals have been prosecuted who have used a DoDAAC to purchase items (i.e., televisions) for personal gain. Therefore, effective management, control, and use of DoDAACs by all DoD Components is critical to ensure DoD fiscal responsibility. Moreover, the public interest in disclosure of the DoDAAD is minimal. FOIA requests for the DoDAAD are made by commercial entities with commercial interests. Therefore, the public interest consideration in the disclosure of this information does not outweigh preventing the disclosure of the information."

c. Handling of DoDAAD Data. Currently, the manner in which DoDAAD data is treated has remained unchanged since the DoDAAD was created, in spite of the implementation of system access controls. Anyone with access to the system can download and retransmit data through unclassified means without any published guidance as to the sensitivity of this data or the potential damage that can be caused by its open release. There is currently no guidance provided on how to assure users

requesting access have a legitimate need to know. That determination rests with the owners of the data and not necessarily those who maintain the system.

(1) **System Management**. Management of the DoDAAD as a system is the shared responsibility of DLMSO and DLA Transaction Services. To that end, the security protocols that have been put in place to safeguard access, and which require a Common Access Card (CAC), or Public Key Infrastructure (PKI) Certificate, and an approved System Access Request (SAR) through the DLA Transaction Services Customer Support Desk, do not address the underlying and more important criterion of ensuring need to know has been determined by the rightful owners of the data, as well as providing further guidance on how the data should be handled and safeguarded by those granted access to it. Although the DoDAAD was reengineered into a database, and updates to it (write access) were modernized away from individually-submitted transactions at the unit/user level to a web-based update tool (the DoDAAD Update Application) that facilitates Service-level management, aggregate read access to the database itself (eDAASINQ) has remained largely as it was decades ago – granted at the individual unit/user level by the DLA Transaction Services Customer Support Desk.

(2) **Data Management**. Data management of the DoDAAD is the responsibility of the Components who actually own the activities who have DoDAACs in the DoDAAD, and thus the data entered therein for each. Management of this data is accomplished by two functions: write access and read access.

(a) Write access to the DoDAAD is facilitated through the use of the DoDAAD Update Application. Accounts are established for this application by formal appointment of Central Service Points (CSP) and Monitors by the Components to the DoDAAD Administrator at DLMSO. The Administrator forwards the appointment letters to the System Access Control Point (SACP – formerly known as the Central Control Point or CCP) at Transaction Services. Once the SACP receives the formal appointment letter, the CSPs/Monitors submit System Authorization Access Requests through the DLA Transaction Services website which are subsequently approved by the SACP who, in turn, establishes access controls for these individuals in the Application based on the information provided in their appointment letter (i.e., Service Series, MAJCOM, Range, etc.). The SACP thus serves as the System Access Control Point for the ability to update the database.

(b) Read access to the DoDAAD (in aggregate) is facilitated through the use of the Enhanced DAAS Inquiry (eDAASINQ) application. These accounts are established by any user requesting access through the submission of a System Authorization Access Request to the DLA Transaction Services Customer Support Desk. There is currently no review by the Components for access requests by its members. Read access can be granted to contractors, as well as Civilian and Military personnel of the Federal Government. In the case of contractors, however, there is an additional requirement for a U.S. Government Sponsorship letter to be submitted along with the System Authorization Access Request. eDAASINQ accounts are not limited to read access to the DoDAAD. An eDAASINQ account also affords read access to the MAPAD, and allows single-record searches (i.e., DAASINQ) for Communication Routing Identifier (COMMRI), Distribution Code, and National Item Identification Number (NIIN). Additionally, it has several file downloads available for various other types of data: Fund Code, DoDAAD, MAPAD, and United States Postal Service (USPS) City/Zone Improvement Plan (ZIP) Code errors.

(3) **Read Access Controls**. While write access to the database is formally approved and controlled by the Components at the Service level through the appointment of CSPs to the Administrator, there is currently no read access control on the part of the Components that safeguards

the data content of the DoDAAD and whether or not the individuals requesting access to this data have a need to know, as determined and approved by the owners of the data – the Components. This DLMS Change is intended to identify the requirement for Components to implement the proper controls for read access to the DoDAAD that is in keeping with Reference 3.c, and safeguards the proper labeling and handling of this data as CUI/FOUO.

     d. **Describe Approved Change in Detail:** To implement this Change, the following actions are to be taken:

     (1) All Users. Per references 3.d. and 3.e., all users with eDAASINQ access shall handle the data as FOUO and shall not re-transmit, save, or otherwise share this data in any means that would jeopardize its security except on a need-to-know basis. The following applies:

     (a) Printouts or Reports Containing FOUO Data. Each page of a printout or report generated from databases containing FOUO data will display a pre-programmed header and footer containing the FOUO handling legend. Where practical, the legend may be rubber stamped on the document.

     (b) Unclassified Electronic Mail (E-Mail) Messages Containing FOUO Data. When transmitting FOUO data via electronic mail (E-mail), the E-mail message will be encrypted and digitally signed using Common Access Card (CAC) based DOD public key (PK) certificates. The opening line of an E-mail message is to call attention to the fact that it contains FOUO data, e.g., "This message is to be handled as For Official Use Only." Similarly, if a FOUO document has been attached to the E-Mail, the opening line of the message is to state that fact; e.g., "The attachment to this E-Mail message is to be handled as For Official Use Only." Within the body of the message, each part containing FOUO information will be marked at the beginning with the FOUO legend in parentheses.

     (c) Facsimile Cover Sheets. Where FOUO data is sent via facsimile message, the facsimile cover sheet is to call attention to the fact that the attachment is to be handled as FOUO."

     (d) Marking Other Types of Housing Devices. Compact Disks, diskettes, canisters, cartridges, tapes, cassettes, and similar housing devices used to permanently store FOUO data will be marked "For Official Use Only" or "FOUO" in a manner that ensures that a recipient or viewer is aware of the status of the information therein. DLA Label 1804, For Official Use Only Pressure Sensitive Label, may be used for this purpose. If the data is also subject to the Privacy Act, DLA Form 1462, Pressure Sensitive Privacy Act Label may be used to mark housing devices in lieu of DLA Label 1804.

     (2) DLMSO. Update DLM 4000.25, Volume 6, Chapter 2 to include the process outlined in this DLMS Change. See paragraph 4.e. below.

     (3) DLA Transaction Services. Per references 3.d. and 3.e., the following changes will be necessary to implement this DLMS Change (see also the enclosures to this attachment).

     (a) Prominently label all user screens for eDAASINQ, and the DoDAAD Update Application with the FOUO handling legend. Access screens to these applications will display, at a minimum, the following warning:

"The DoDAAD is DoD Critical Infrastructure Security Information (CISI), in accordance with 10 U.S.C. § 130e, and is designated as Controlled Unclassified Information For Official Use Only (FOUO). This data is maintained and owned by the Departments of the Federal Government via their respective DoDAAD Central Service Points (CSPs). The designation and protective marking of the DoDAAD, identifying it as FOUO, deems that its disclosure to the public would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the Freedom of Information Act (FOIA). Because there is a potential for abuse in the use of these DoDAACs and RICs, and the data associated with them in the DoDAAD, Departments of the Federal Government shall establish stringent internal controls to ensure that the codes and data are used only by authorized personnel. It is imperative that all requests for activity address codes, deletions to codes, or changes thereto, be forwarded to the appropriate CSP, or delegated Monitor, in order to assure proper validity of the request. Furthermore, personnel with access to the DoDAAD are responsible for safeguarding it, and will ensure that *further distribution is restricted to personnel with an official need to know and proper authorization*. Any such further distribution will be minimized, encrypted, and documented accordingly as FOUO."

(b) **Output.** Each page of a printout or report generated from the database containing FOUO data will display a pre-programmed header and footer containing the FOUO handling legend -- For Official Use Only (FOUO). The following applies:

1. DAASINQ. Since the FOUO requirement applies to aggregate data, beyond the initial DAASINQ warning screen, there is *no need* to label follow-on screens or any printed output obtained by users via DAASINQ.

2. eDAASINQ. Since eDAASINQ allows the ability to download aggregate data, all screens and every format of output obtained through this application shall be subject to the warnings and FOUO marking labels (i.e., delimited downloads, TA_ format downloads, Excel output, .dat output, etc.).

(c) For DAASINQ, implement an additional CAPTCHA test after every tenth DoDAAC query attempt. This would limit the number of back-to-back queries by a customer to ten queries before having to revalidate, thereby precluding users from extracting aggregate data through DAASINQ.

(4) **Components**. To safeguard DoDAAD data, Components shall review requests for access to eDAASINQ by their members, prior to them being submitted to the DLA Transaction Services Customer Support Desk. Recommend the following be implemented to facilitate this:

(a) Recommend that the Central Service Points be responsible for receiving, reviewing, and formally approving all access to the DoDAAD through the eDAASINQ, before any user submits a request to the DLA Transaction Services Customer Support Desk. As the only Service-appointed personnel responsible for managing the DoDAAD, the CSPs could ensure need-to-know status is verified on the part of users within their Service who request access to the DoDAAD. CSPs should maintain record of requests they've approved at their level as part of their overall DoDAAD management responsibilities.

(b) Contractors who request/require access to eDAASINQ must not only request access through their CSP, but they must obtain a Government Sponsorship letter. Contractor requests will

only be granted access if they include a CSP-approved request and the approved sponsorship letter, both of which should be kept on file by the CSP.

(c) Component system requirements for aggregate DoDAAD data should be submitted to the CSP for review and approval before forwarding to the DoDAAD Administrator to obtain enterprise-level DoDAAD output (i.e., system-to-system interface).

(d) Update Component-level policies and procedures to include the process and procedures outlined in this DLMS Change. *Any system dependent upon DoDAAD data, or which receives and stores DoDAAD data, and allows users to download the data and/or retransmit it, must apply the same warning statement as identified above, to ensure FOUO compliance is maintained (e.g., USTRANSCOM TRDM, GSA, DSS, et al.).* See paragraph 9.c. below.

e. **Revisions to DLM 4000.25 Manuals:** The following paragraph will be added to Chapter 2 of Volume 6:

C2.8. DoDAAD Data Security. The DoDAAD shall be marked and handled by all users as Controlled Unclassified Information For Official Use Only (FOUO).

C2.8.1. The aggregated content of the DoDAAD (i.e., multiple DoDAACs and/or RICs and their respective data elements) is exempted from Public Release under the Freedom of Information Act (5 U.S.C. § 552(b)(3)) because it meets the requirements for exemption under 10 U.S.C. § 130e. Specifically, the DoDAAD database, as a single authoritative source for the Department of Defense (DoD) business enterprise architecture, qualifies as DoD critical infrastructure security information (CISI). CISI is categorized as FOUO, and as defined by 10 U.S.C. § 130e, it includes:

"…sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security."

C2.8.2. The DoD Director of Administration and Management (DA&M) has issued a Determination that the DoDAAD meets this definition of CISI, because it is comprised of both DoDAACs and RICs in an interactive relational database serving as a single authoritative source of identification, routing, and address information for authorized users, including Military Components and Agencies, participating Federal Agencies, authorized contractors, and authorized special program activities such as state and local governments.

C2.8.3. DoDAAD supports business application systems data and interoperability requirements, including (but not limited to) supply chain, materiel procurement, and

acquisition systems. Each activity that requisitions, contracts for, receives, has custody of, issues, or ships DoD assets, or funds/pays bills for materials and/or services is identified by a DoDAAC (six-position alphanumeric code).

C2.8.4. DoDAACs are used in a myriad of business systems spanning the entirety of the DoD's business enterprise architecture, including acquisition, procurement, contracting, requisitioning, shipping, billing, pay, maintenance, installations management, human resources, energy resources, and the accountability and requisition of ordnance, ammunition, and perishables in logistics systems across the DoD. DoDAACs are also used for business operations involving the accountability of property and facilities, as well as for hazardous material management. Access to the DoDAAD allows access to these DoDAACs. When coupled with access to other unclassified logistic systems, users are provided with multiple data points which, when combined, disclose location of materials and operational status and plans. The contents of the DoDAAD are sensitive for a number of reasons:

• DoDAACs are created to support sensitive operations and to facilitate the business process associated with them.

• DoDAACs for the following locations include names of employees and Service members as well as duty station addresses for:

a. Department of Defense installations and ports that are outside the contiguous United States (OCONUS).
b. Deployed units and activities performing real world contingency operations or exercises from both contiguous United States (CONUS) and OCONUS bases.
c. Ships afloat.
d. Ships still in CONUS ports but scheduled to go afloat.
e. Ships still in OCONUS ports but scheduled to go afloat.
f. Embassies.
g. War Reserve Equipment sets pre-positioned OCONUS.

C2.8.5. In addition, a DoDAAC could be used in an unauthorized way whereby the internal controls of the Agency can be circumvented and appropriations obligated without the proper authority being involved in the process. A DoDAAC is very much like a credit card number which, in the wrong hands, can be used to spend money without the rightful "owner" of the code (i.e., the entity with authority to use the code) being aware that the Agency's appropriations are being spent. Individuals have been prosecuted who have used a DoDAAC to purchase items (i.e., televisions) for personal gain. Therefore, effective management, control, and use of DoDAACs by all DoD Components is critical to ensure DoD fiscal responsibility.

C2.8.6. If the DoDAAD were released, it would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD.

C.2.8.7. If an adversary of the United States Government had the DoDAAD, they could determine the issuance of orders; the movement of specially qualified personnel to units and

the installation of special capabilities, as well as the conduct of activities in a way that will reveal intensification of preparations before initiating operations. From this information, the adversary could identify very sensitive DoD activities including clandestine locations of DoD activities, force structure, and even troop movement.

    f. <u>**Alternatives**</u>**:** None.

5. **REASON FOR CHANGE:** See Background above.

6. **ADVANTAGES AND DISADVANTAGES:**

    a. <u>**Advantages**</u>**:**

        (1) Implements required security controls for CISI/FOUO data.

        (2) Transfers the responsibility for granting access to the content of the DoDAAD away from the DLA Transaction Services Customer Support Desk and places it upon the individuals appointed by the Components with overall responsibility for the data – the CSPs.

    b. <u>**Disadvantages**</u>**:** None.

7. **ADDITIONAL FUNCTIONAL REQUIREMENTS:** None noted.

8. **ESTIMATED TIME LINE/IMPLEMENTATION TARGET:** This change will be authorized for immediate implementation when this DLMS change is released as an ADC. DLA Transaction Services will implement these additional controls within 30 days of this ADC.

9. **IMPACTS:**

    a. <u>**New DLMS Data Elements**</u>**:** No new DLMS data elements.

    b. <u>**Changes to DLMS Data Elements**</u>**:** No changes to existing DLMS data elements.

    c. <u>**Automated Information Systems (AIS)**</u>**:** Any system dependent upon DoDAAD data, or which receives and stores DoDAAD data, and allows users to download the data and/or retransmit it, must apply the same warning statement as identified in paragraph 3.d.(2)(a) above, to ensure CUI/FOUO compliance is maintained, and that proper handling instructions for such data is both published and adhered to accordingly. This applies to systems which obtain data directly from the DoDAAD, as well as any systems which obtain DoDAAD data via manual downloads by users from eDAASINQ. The following organizations/systems currently obtain data directly from the DoDAAD through replication:

        (1) <u>OSD</u>: Joint Organization Query (JOQ)
        (2) <u>DLA</u>:
            (a) DLA Logistics Information Systems (DLIS)
            (b) Enterprise Business System (EBS)
            (c) Wide Area Workflow System (WAWF)
            (d) Distribution Standard System (DSS)
        (3) U.S. TRANSCOM
        (4) <u>U.S. Air Force</u>: AFMC LSO

(5) <u>U.S. Army</u>:
     (a) Army Surface Deployment and Dist. Command (SDDC)
     (b) Logistics Support Activity (LOGSA)
     (c) Joint Munitions Command (JMC)
(6) <u>U.S. Navy</u>:
     (a) Navy NCDOC
     (b) Navy Supply Information Systems Activity (NAVSISA)
(7) <u>U.S. Marine Corps</u>: USMC Master Data Repository (MDR)
(8) General Services Administration (GSA)
(9) FAA Logistics Center Support
(10) Coast Guard Business Intelligence (CGBI)

    d. **DLA Transaction Services:** See detailed change section above.

    e. **Non-DLM 4000.25 Series Publications:** The changes identified in this DLMS Change will need to be incorporated into the relevant Component-level DoDAAD management publications, including (but not limited to) the following:

(1) U.S. Army: AR 725-50
(2) U.S. Navy: NAVSO P-1000-2-5
(3) U.S. Air Force: AFI 24-230
(4) U.S. Marine Corps: MCO 4420.4H
(5) U.S. Coast Guard: COMDTINST M4000.2
(6) Defense Logistics Agency: DLAI 1401
(7) Defense Information Systems Agency: DISA Instruction 270-50-10
(8) USTRANSCOM: DTR 4500.9-R

10. STAFFING RESPONSE/COMMENT RESOLUTION:

PDC 1143 Comments		
Submitted	**Response**	**Resolution**
Air Force	Concurs without comment	Noted
Army	Concurs without comment	Noted
DLA	Silent Concurrence	Noted
DLA Transaction Services	Concurs with comment	Noted
Marine Corps	Concurs without comment	Noted
Navy	Concurs with comment	Navy commented on the implementation timeline.