



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

IN REPLY  
REFER TO

DLMSO

April 06, 2010

MEMORANDUM FOR SUPPLY PROCESS REVIEW COMMITTEE (PRC) MEMBERS

SUBJECT: Approved Addendum 361A to Approved Defense Logistics Management System (DLMS) Change (ADC) 361, Requirement for Exception Distribution of a Minimal Content Supply Discrepancy Report (SDR) via Electronic Mail (E-mail) (Staffed as PDC 391)

The attached change to DOD 4000.25-M, Defense Logistics Management System (DLMS), Volume II, Chapter 17, Reporting of Supply Discrepancies, is approved for implementation. This addendum publishes DLMS manual procedures associated with the ADC 361.

This change further documents procedures associated with the e-mail encryption requirement for DoD WebSDR. DoD Components currently receiving SDRs or SDR management reports via e-mail are reminded that that **April 30, 2010**, is the milestone date for adoption of the enhanced controls.

Addressees may direct questions to the DLMSO point of contact, Ms. Ellen Hilert, Chair, Supply Process Review Committee, 703-767-0676, DSN 427-0676; or, e-mail: [Ellen.hilert@dla.mil](mailto:Ellen.hilert@dla.mil). Others must contact their Component designated representative.

A handwritten signature in black ink, appearing to read "Donald C. Pipp".

DONALD C. PIPP  
Director  
Defense Logistics Management  
Standards Office

Attachment

cc:  
SDR Committees (U.S. & SA)  
ADUSD(L&MR)SCI

## ADC 361A

### Requirement for Exception Distribution of a Minimal Content SDR via E-mail

**1. ORIGINATING SERVICE/AGENCY AND POC INFORMATION:** Defense Logistics Management Standards Office (DLMSO), Ms. Ellen Hilert, Chair DoD SDR System Administrator, 703-767-0676; DSN 427-0676; or, E-Mail: [Ellen.Hilert@dla.mil](mailto:Ellen.Hilert@dla.mil) .

**2. FUNCTIONAL AREA:** Supply/DoD WebSDR

**3. REFERENCE:**

a. DLMSO memorandum dated March 15, 2010, subject: ADC 361, Requirement for Exception Distribution of a Minimal Content SDR via E-mail.

b. Presidential Memorandum, May 9, 2008, subject: Designation and Sharing of Controlled Unclassified Information. Defines CUI as: "Unclassified information that does not meet the standard for National Security Classification under Executive Order 12958, as amended, but is pertinent to the national interest of the United States or originated by entities outside the U.S. Federal government, and under law or policy requires protection from disclosure, special handling safeguards, and prescribed limits on exchange or dissemination."

**4. PROPOSED CHANGE:**

**a. Background:**

(1) SDRs prepared by DoD WebSDR have been designated as "For Official Use Only" [also known as "Controlled Unclassified Information (CUI)"] since 2006 and the encryption of FOUO e-mail has been required by DLA beginning in 2008. The DLA Information Security Office reviewed WebSDR in March of 2009 and determined that SDRs meet OPSEC criteria for unclassified FOUO/CUI data and therefore require encryption.

(2) DLA imposed an April 30, 2010 implementation date for DoD WebSDR encryption of all SDR e-mail communications. Beginning in January, all WebSDR e-mail messages directed to an e-mail address without an associated certificate on file at DAAS, have included a notification of the certificate registration requirement with instructions for registration.

(3) ADC 361 documented the process for a new e-mail communication approach for low volume customers reporting supply discrepancies through a third party or otherwise lacking ability to receive encrypted SDR e-mail. This process will be available to users that report discrepancies via the DLA Customer Interaction Center (CIC), Army Non-Army Managed Item (NAMI) office, or other supporting activities, where the customer may not have an e-mail certificate registered at the Defense Automatic Addressing System Center. Beginning April 30, 2010, confirmation copies of SDRs and SDR replies sent via e-mail must be encrypted by DAASC to comply with Operation Security (OpSEC) requirements. In order to receive an encrypted e-mail, users must register their e-mail certificate associated with the e-mail address

receiving the SDR. However, some customers report an SDR very infrequently and don't have access to WebSDR or a Service SDR System which interfaces with DoD WebSDR. Although the CIC or other authorized party may enter the SDR on the customer's behalf, the customer should still receive a confirmation copy and the SDR reply with resolution/disposition instructions via e-mail. Additionally, there may be other parties identified as distribution copy recipients on an SDR where the associated e-mail addresses were not previously registered. In these cases, it is not appropriate to withhold the SDR communication or delay processing pending registration. Instead, the SDR confirmation copies and replies will be sent unencrypted with minimal data content to eliminate the need for "FOUO (CUI)" designation. These unencrypted e-mails will include instructions for certificate registration and how to apply via a DoD WebSDR system access request (SAR) should the customer desire to have full access to the SDR data content.

**b. Description of Change:** This addendum to ADC 361 is provided:

(1) To document and publish updated procedures for SDR processing, especially related to SDR e-mail distribution.

(2) To include terminology for "Controlled Unclassified Information (CUI)" in the DLMS manual per reference 3.b. However, per HQ DLA guidance, WebSDR will retain the "For Official Use Only (FOUO)" designation until further notice.

**c. Procedures:** Revise the DLMS manual, DoD 4000.25-M, Vol 2, Chapter 17, as follows. Changes to existing guidance are identified in ***bold italics***.

**(1) Update Operations Security (OPSEC) applicability:**

"C17.2.2. Operations Security (OPSEC) Applicability. Due to an identified OPSEC requirement, SDRs have been ***recognized as controlled unclassified information (CUI) by the DLA HQ, and must be identified*** as "For Official Use Only (FOUO). Handling and electronic transmission of SDRs must comply with DoD rules for this level of sensitive unclassified information, to include proper labeling and protection. DLA has further directed encryption of all SDR e-mail transmissions. This requirement has been levied on the DoD WebSDR and will impact all participating DoD Components.

***C17.2.2.1 In order to receive encrypted e-mail, individual and group e-mail accounts must have their associated e-mail certificate registered at DAASC. SDRs directed to e-mail accounts which do not have a registered certificate will be significantly abridged to display minimal information, thereby allowing the SDR to be transmitted in an unprotected environment.***

***C17.2.2.2 All action activities using e-mail SDRs must register their certificate, so that all information will be available for SDR resolution. For low volume customers relying on e-mail SDRs, especially those supported by third party direct WebSDR input, registration is encouraged, but not required. These users will receive an abridged SDR***

*reply which will provide disposition instructions and financial action, without the accompanying shipment detail.*

*C17.2.2.3 Unencrypted e-mails with minimal shipment information will include instructions for certificate registration and access to DoD WebSDR. Full SDR data content will be available to authorized users of DoD WebSDR. Refer to DAAS SDR Processing for further details on the abridged SDR procedures and content.*

*C17.2.2.4 SDR management reports shall only be distributed via e-mail if the corresponding certificate has been registered.”*

**(2) Update DAAS procedures:**

“C17.3.21. DAAS SDR Processing

C17.3.21.1. Under DLMS, SDRs shall be integrated with standard logistics transaction processing through DAAS. DAAS shall perform the following actions:

C17.3.21.1.1. Pass/route SDR transactions *(subparagraphs not shown here)*

C17.3.21.1.2. Edit SDR transactions in accordance with business rules specified below.

C17.3.21.1.3. Provide translation capability to support a variety of communications methods for exchanging computer-readable SDR transactions.

*C17.3.21.1.3.1. DLMS transaction formats are available in ASC X12 EDI or EDI-based XML. Guidance for transaction content is provided in DLMS Supplements available at: [http://www.dla.mil/j-6/dlms/eLibrary/TransFormats/140\\_997.asp](http://www.dla.mil/j-6/dlms/eLibrary/TransFormats/140_997.asp).*

*C17.3.21.1.3.2. Until replaced by DLMS, the Army unique transactional interface with Army Electronic Product Support (AEPS) shall be supported.*

*C17.3.21.1.3.3. No other transactional formats are authorized for SDRs.*

*C17.3.21.1.4. Convert SDRs for e-mail distribution where computer-readable SDR transactions are not feasible due to lack of an established SDR application interface.*

*C17.3.21.1.4. 1. Upon determination that an e-mail (vice transaction) is to be prepared for a specific SDR communication, DAASC will check to determine if the appropriate e-mail certificate has been registered. If registered, the SDR e-mail transmission shall be encrypted as “FOUO” per paragraph C17.2.2. The e-mail SDR shall contain all associated SDR content as well as clear text addresses and code explanations to facilitate user interpretation. If not registered, an abridged content SDR report, confirmation, distribution copy, or reply, as applicable, will be prepared. The e-mail sent to the user will also provide*

**information on how to get access to WebSDR and instructions on registering the e-mail certificate.**

**C17.3.21.1.4. 1. 1. Abridged SDR. The abridged unencrypted version of the SDR e-mail will include the following data content. Coded information will not include the corresponding clear-text explanation. The submitter and action activities will not be identified by clear-text addresses.**

- **DoD WebSDR Report Control Number**
- **Additional System SDR Control Number(s)**
- **Customer-Assigned Control Number**
- **Document Number/Suffix**
- **Contract Number**
- **Transportation Control Number**
- **Date of Preparation**
- **SDR Document Type Code**
- **DRMS SDR Type Code**
- **Discrepancy Code(s)**
- **SDR Action Code**
- **SDR Submitter (Activity From)**
- **Action Activity (Activity To)**
- **SDR Point of Contact**
  - **Name**
  - **Commercial Phone or DSN**
  - **E-mail**
- **Attachment /Off-line Flag**

**C17.3.21.1.4. 1.2. Abridged SDR Reply. The abridged unencrypted version of the SDR Reply e-mail will include the following data content. Coded information will not include the corresponding clear-text explanation with the exception of the Reply Disposition Code which must include text for understanding. The submitter and action activities will not be identified by clear-text addresses.**

- **DoD WebSDR Report Control Number**
- **Additional System SDR Control Number(s)**
- **Original Reference Number**
- **Document Number/Suffix**
- **Contract Number**
- **Transportation Control Number**
- **Reply Date**
- **SDR Document Type Code**
- **DRMS SDR Type Code**
- **Reply Disposition Code (s)**
- **Action Activity (Activity From)**
- **SDR Submitter (Activity To)**
- **Comments/Remarks**

- **Reply POC**
  - **Name**
  - **Commercial Phone or DSN**
  - **E-mail**
- **Attachment /Off-line Flag**

**CI7.3.21.1.4. 2. Organizations that are not supported by an SDR application for transactional interface, shall provide to DAASC an e-mail address to be linked with their DoDAAC/RIC for e-mail distribution.**

**CI7.3.21.1.4. 2. Each Component shall designate a specific e-mail account or point of contact to receive unroutable SDRs for manual attention. This is required to ensure operational support where no SDR application or e-mail address has been identified for an SDR recipient, or an attempted e-mail distribution has failed due to an invalid address.”**

**5. REASON FOR CHANGE:** Documentation of procedures within DLMS manual.

**6. ADVANTAGES AND DISADVANTAGES:**

**a. Advantages:** Clarification for all interested parties and future users.

**b. Disadvantages:** None.

**7. Impact:**

**a. DLMS Transactions/Data Content:** There are no changes to DLMS transactions associated with this change. There are no new data elements identified as a result of this change.

**b. DAASC Changes:** DAASC changes to the WebSDR program to produce the abbreviated e-mail SDR and SDR Reply are under development.

**c. Implementation:** April 30, 2010 is the last day full content unencrypted SDRs will be provided. ADC 361/361A will coincide with full implementation of the encryption requirement. The DLMS manual update shall be published as soon as possible.

**d. User Community Impact:** As of the first week of April 2010, only 27% of SDR e-mail distribution is being encrypted due to lack of registered certificates. Components are reminded to register their certificates prior to April 30, 2010 to avoid a conversion to abridged SDRs/SDR replies.