DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

DISA INSTRUCTION 630-230-30* 6 August 2014

AUTOMATIC DATA PROCESSSING

Defense Message System (DMS)

1. **Purpose.** This Instruction prescribes policy and assigns responsibility for the Defense Message System (DMS) within DISA. It also provides guidance on message release and formatting, managing of and naming conventions for accounts, access, and security practices for messaging.

2. **Applicability.** This Instruction applies to DISA and all users of DISA internal information systems and networks.

3. **Definitions.** Definitions applicable to DISA DMS usage are provided in enclosure 1.

4. **Policy.** The electronic transmission of organizational messages containing Privacy Act, for official use only (FOUO), or other controlled unclassified information (CUI), details of which are found in enclosure 2, shall be protected by Public Key Infrastructure (PKI), encrypted DMS message, or other secure means; e.g., secure facsimile or secure voice or the Secret Internet Protocol Router Network (SIPRNet). The nature of the information will determine whether DMS will be used. If appropriate, page and paragraph markings, along with the proper marking statement such as "FOR OFFICIAL USE ONLY," will be included in the message, as required by DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI).

4.1 DMS is the system of record for organizational messaging and will be used by authorized personnel for the transmission of organizational messages. Selected employees of each organizational element will need the capability to send and receive signed and encrypted DMS messages. DISA will use a Web-enabled organizational messaging system to provide DMS capabilities. DMS messages will be signed and encrypted with a DoD Class 4 certificate via Fortezza Crypto Card in a Cipher Server or Virtual Fortezza Cards (VFCS) on a Type 2 Cryptographic Support Server (T2CSS) board.

4.2 DoD data and information must be provided adequate protection from unauthorized access and use. If simple mail transfer protocol (SMTP) e-mail is used to conduct DISA business, data integrity and security remain paramount considerations. If the individual or aggregate of data warrants, the DISA customer will be informed to submit a Group Certificate Request to send and receive DMS messages on behalf of their organization.

4.3 Access to DMS capabilities shall be limited to DISA military and civilians and contractors directly supporting DISA. A representative of another Federal Government agency that is assigned to or directly supports DISA can be given access to DMS. Access to DISA organizational accounts at the branch level and higher will normally not be afforded to non-DISA and nongovernmental personnel. Contractor personnel may be granted temporary DMS privileges.

5. **Responsibilities.**

5.1 **Principal Director for Enterprise Information Services (EIS)/Chief Information Officer (CIO). The Principal Director, EIS/CIO will.**

5.1.1 Oversee DMS within the Agency.

5.1.2 Perform periodic reviews of the effectiveness and efficiency of DMS messaging within DISA. (These reviews should be performed along with DISA's triennial Information Resources Management Reviews under 44 U.S.C. 3513).

5.1.3 Provide security accreditation on the DISA implementation of the DMS.

5.1.4 Collect and process certificate requests for DMS access, release authority for contractors, and requests of DISA personnel or organizations to have DMS access and issue certificates for DMS services.

5.1.5 Support the development of DMS training and the distribution of training materials to DISA activities.

5.1.6 Oversee archival and retention of organizational messages in accordance with National Archived and Records Administration (NARA) policies.

5.2 **Principal Directors, Directors, Commanders, and Chiefs of Major Organizational Elements**. These individuals will:

5.2.1 Submit approved X.509 Certificate Request Forms to the Local Registration Authority (LRA) for appropriate personnel to draft, review, and release (DRR) organizational messages within their activities.

5.2.2 Direct personnel within their activities to use DMS for all organizational messaging.

5.2.3 Develop unique standard operating procedures, as necessary, to incorporate the implementation of DMS into their business processes and practices.

5.2.4 Ensure DMS accounts within their activities are maintained so that DMS messaging operations will be effective and timely.

6. **Authorizing Official (AO) Duty.** The AO will provide certification and accreditation of DMS on DISA organizational messaging systems.

7. **Message Release and Formatting.**

7.1 DMS organizational messages are sent on behalf of the top (parent) level of a particular organization. Each organization will designate an Authorized Releaser(s) as final approving authority for the transmission of DMS messages for that organization. The releaser shall review and approve the message content, format validation, addressing and setting the final precedence, classification, and other military properties. The DMS system will sign and encrypt DMS messages to provide appropriate protection and data integrity. The approved method of electronic transfer or forwarding of a DMS organizational message is via an authorized DMS messaging system service, thereby, ensuring the level of security initiated by the sender is maintained.

7.2 DMS messages are to be sent in the United States Message Text Format (USMTF). Nearly all data and information can be accommodated within an existing approved USMTF message. If a new message format would benefit a DISA organization or customer, the DISA organization will work with the DISA USMTF program sponsor to generate a new USMTF format for inclusion into the USMTF standard. Maximum use of USMTFs encourages familiarity and improves message completeness and interoperability. A certified and approved USMTF message preparation and validation tool is incorporated in the Web-enabled system and will be used to prepare and validate DMS organizational messages.

8. **Managing of and Naming Convention for Accounts.** In order for DMS to work as designed, it is imperative that DMS accounts be maintained and monitored appropriately. DMS qualified personnel will be made available to perform DMS messaging tasks for their organization. Procedures must be implemented to manage organizational accounts and to handle priority and above messages in a timely manner.

8.1 A means to address the handling of Priority Precedence and above message traffic coming into an organizational account is to be in place to ensure priority matters are handled appropriately. Monthly maintenance is to be conducted of organizational DMS accounts to ensure messages can be sent and received without difficulty. Proper internal distribution of incoming organizational messages is to be defined, and the organizational message account is maintained and well managed. The individuals assigned to the organizational account is to be reviewed semiannually.

8.2 The Distinguished Name (DN) for an organizational account will have the prefix of DISA followed by the role (e.g., Commander). If the combination of DISA roles does not create a globally unique DN, a theater or region suffix shall be added (e.g., CONUS, PAC, or EUR), followed by a numeric suffix, if required. The DISA prefix ensures DMS users easily know who has sent the message, facilitates ease of recognition in the Directory Information Tree (DIT), and colocates DISA entries in the personal address book or contacts listing.

9. **Access.** For DMS privileges and certificates for DISA military and civilians and contractors directly supporting DISA, the responsible supervisor will initiate and sign a Group Certificate Request once a determination has been made that an individual requires access to a DMS

organizational account on the Web-enabled system. The Authorizing Official (AO) will approve the account(s) access and privileges. A request to the LRA is required in order for an X.509 certificate with appropriate privileges and roles to be created by the Certificate Authority (CA).

9.1 For access to DMS for representatives of another Federal Government agency that are assigned to or directly support DISA, the DISA sponsor must acknowledge to the Enterprise Information Services Directorate (EIS) that access can be granted.

9.2 For access to DMS for contractor personnel**,** the Program Manager for a project will validate to the Contracting Officer's Representative (COR) the need for access and submit the request to the Information Technology Operations Center within EIS for contractor access. The COR will revalidate the need for each contractor's continued access whenever there is change in the contract or the individual's direct support to the contract. The COR will request cancellation of a contractor's access at the termination of the contractor's employment on the project or project completion. If a contractor moves to another DISA contract, the COR of that contract must formally assume responsibility for the contractor's account.

10. **Training.** DMS user training is required before a user is given access to the Web-enabled system. To request DMS user training, contact the DISA Training Office at disa.meade.mps.mbx.training-office@mail.mil. Refresher training will be provided when applicable or as requested.

11. **Termination.** The organization's DMS point of contact (POC) will notify the LRA if an individual no longer requires access to the DMS organizational account and, additionally, the DMS POC should submit an updated Group Certificate Request.

12. **Records Management.** DMS messages are not to be destroyed, unless as authorized in accordance with DISAI 210-15-6, Records Management, and are to be archived by the DMS user.

13. **Security Practices for Messaging.** Classified information will not be sent to an unclassified DMS address, and DMS digital encryption is not an acceptable means for transmitting classified data over an unclassified network. Discretion shall be exercised when transmitting CUI via DMS, in accordance with DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI).

HENRY.FREDERICK.ANTHONY.1011175445

Digitally signed by HENRY.FREDERICK.ANTHONY.1011175445
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=HENRY.FREDERICK.ANTHONY.1011175445
Date: 2014.09.02 21:01:07 -04'00'

2 Enclosures a/s

FREDERICK A. HENRY
Brigadier General, USA
Chief of Staff

_____

*This Instruction replaces DISAI 630-230-30, 13 September 2006, and must be reissued, canceled, or certified current within 5 years of its publication date. If not, it will expire 10 years from its publication date and be removed from the DISA issuances postings.
OPR: EIS - disa.meade.eis.mbx.eis-front-office@mail.mil
Distribution: P

Enclosure 1

DEFINITIONS

Authorizing Official (AO). As appointed under DoD Instruction 8500.01, 14 March 2014, formally known as Designated Approving Authority (DAA), individual must be a U.S. citizen and DoD official with the authority to assume responsibility formally for operating DoD at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), official assets, individuals, other organization, and the Nation.

Certification Authority (CA). A CA is the individual responsible for registering end users (including machines), issuing their certificates, placing certificates in the DMS directory, and for programming FORTEZZA cards. A CA is typically the multilevel information system security initiative (MISSI) administrative authority for an autonomous organization, or major unit of an organization, within a policy domain. The term CA can refer to either that authoritarian office or role or to a person filling that office. The CA is also responsible for programming FORTEZZA cards using the Certification Authority Workstation.

X.509 Certificate Request Form. Form(s) is used to generate a Class 4 certificate to allow an authorized user to send and receive organizational messages for designated organizations.

Defense Message System (DMS). The designated messaging system for DoD and supporting agencies. It is a flexible, commercial-off-the-shelf (COTS) based, net-centric application layer system that provides multimedia messaging and directory services capable of taking advantage of the flexible and expandable underlying Defense Information Infrastructure (DII) network and security services. DMS is installed and operational worldwide.

For Official Use Only (FOUO). In accordance with DoD 5400.7-R, DoD Freedom of Information Act Program, unclassified information which may be withheld from the public by one or more Freedom of Information Act (FOIA) exemptions.

Organizational Messaging. Includes messages and other communications exchanged between organizational elements in support of command and control, combat support, combat service support, and other functional activities. Typically, these messages provide formal direction and establish a formal position, commitment, or response for the organization. Organizational messages require approval for transmission by a designated official of the sending organization and determination of internal distri-bution by the receiving organization. Because of their official and sometimes critical nature, such messages impose operational requirements on the communi-cations systems for capabilities such as precedence, timely delivery, and high availability and reliability.

Record. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. [44 U.S.C., section 3301].

Release Authority. A person who is authorized to send a message on behalf of an organization. That person may draft and release a message directly without further coordination or may elect to have the message drafted and coordinated prior to release.

Enclosure 2

CONTROLLED UNCLASSIFIED INFORMATION

Controlled unclassified information (CUI) is unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. CUI includes the following types of information:

1. Information including, but not limited to, such matters as promotion, medical records, performance ratings, security investigative reports and resultant determination information, and home addresses without prior individual consent.

2. Data associated with security controls (e.g., identification, authorization, or passwords that control access to an information system or network, contain audit trail records, assure the integrity of the Trusted Computer Base [TCB] and its extensions, contain electronic signatures, contain encryption keys, contain the private key component of public key cryptography and security inspection reports).

3. Financial information requiring protection for fund control purposes, data accuracy and fund integrity; protecting other fiscal assets from events such as fraud, theft, waste, misuse, abuse, and mismanagement; financial information pertaining to foreign countries; and proposed procurement plans that would provide undue competitive advantage.

4. Predecisional, temporarily sensitive information until it is formally released (e.g., opinions, suggestions, evaluations reflected in the decisionmaking process); inspection reports pertaining to safety or internal management when treated as privileged by the courts; proposed plans to procure or acquire and dispose of materials and facilities; any information or documents characterized as source selection or acquisition sensitive. [41 U.S.C., section 423]

5. Budget information which includes but is not limited to program budget decisions and defense management report decisions; budgetary information being used for procurement up to the point that procurement is complete or for the Presidential budget until it is released; financial program information not yet released; and budget information of a sensitive nature; such as, for purchase or upgrade of critical weapons systems.

6. Trade secrets, proprietary information, or commercial and financial information that is received from a person or organization outside the government with the understanding that the information or record will be retained on a privileged or confidential basis.

7. Personnel information which includes but is not limited to reorganization proposals, policy options affecting employee entitlement, management positions and proposals for negotiating with unions, proposed and finalized disciplinary actions, or information that may reasonably be expected to endanger the life or safety of an individual.