UNITED STATES MARINE CORPS
I MARINE EXPEDITIONARY FORCE
U. S. MARINE CORPS FORCES, PACIFIC
BOX 555300
CAMP PENDLETON, CA 92055-5300

IN REPLY REFER TO:
5500
IMO
10 MAY 2011

POLICY LETTER 8-11

From: Commanding General
To: Distribution List

Subj: INFORMATION/DATA CONTENT STAGING AND RE-DEPLOYMENT STANDARD OPERATING PROCEDURES

Ref: (a) DoD Directive 8910.1-M, "Management and Control of Information Requirements," June 30, 1998.
(b) I MEF Policy Letter 6-09

Encl: (1) I MEF guidance on Shared Drive allocation

1. Situation. The I Marine Expeditionary Force Command Element (I MEF CE) has identified a requirement to manage information, specifically electronic secure and non-secure data generated through operations, exercises, deployments to guard against the loss of institutional knowledge caused by transfer, separation and retirement of personnel.

2. Mission. Pursuant to reference (a) and (b), this document establishes standard operating procedures for migrating, archiving, and maintaining information stored on secure and non-secure electronic media.

3. Execution. Information assembled by a command/individual is recognized as a capability and over time leads to institutional knowledge. This information should be retained to guard against the loss of knowledge. However, this information must be continuously managed by the information owner(s) to determine its relevancy. Information that is deemed beneficial to follow on exercises, operations or deployments should be archived. All other information should be deleted.

a. Information/content returning from deployment

(1) Electronic data returning from deployment on external hard drives will be catalogued by the I MEF Security Manager to ensure the hard drives are tracked and reported in accordance with I MEF policy.

(2) Information from deployed external hard drives will not be directly introduced to the I MEF garrison collaborative environments or shared drives without being validated by an action officer from the executive, principal, special staff, or command the information supports. Historically, 80% of the information returning from deployment is no longer current or relevant. 20% of the data can be used to build institutional knowledge; 10% of that content is current and relevant to the daily battle rhythm locally, the other 10% supports future planning relevant to redeployment.

(3) I MEF G-6 will establish a Kiosk of appropriate clearance (NIPR, SIPR, CENTRIX) to physically connect and receive the deployed content. The Kiosk will have an ability to write to removable media and can be located within the deployed work space area or locally with the G-6 helpdesk. The Kiosk will normally be in the form of a laptop connected to the external hard drives, however on occasion the G-6 may need to re-animate the content by restoring a server or virtual server to allow access.

(4) Sections/units/individuals will access the information stored on the external hard drives using the Kiosk. Users will transfer relevant information from the external hard drives to a defined folder/sub-folder structure on the Kiosk. Once the user has completed identifying the relevant information required to move using the forms and categories described above, the G-6 will write the data to removable media. The relevant information will then be scanned by the Information Assurance section and loaded to the collaborative portal (under responsible section/unit) or appropriate shared drive. The process is explained in detail below:

(a) External media/hard drives must be taken to the Information Assurance section for scanning prior to being connected to the Kiosk/server.

(b) G-6 will provide the stand alone Kiosk (laptop) or server.

(c) G-6 will connect the external hard drives to the Kiosk to provide access. Sections may bring their own external hard drives if possessed (ensure IA performs a scan first.)

(d) Users will log on to the local laptop to access the data on the external drives.

(e) Users will build the folder structure on the Kiosk to move the data from the external drives to the designated folder.

(f) The G-6 will write the relevant information to external media and erase the folder structure on the Kiosk to prevent it from becoming overloaded.

(g) Users will then load the relevant information into the appropriate SharePoint site, shared file, or local computer as required.

(h) User is responsible for destroying external media.

(i) All external media/hard drives must be accounted for by the Security Manager.

(5) Kiosk support/infrastructure will be available immediately upon receiving the deployed content and exist for 270 days (can be adjusted as required). The first 30 days users are understood to be available but occupied by reintegration. The next 30-90 days are critical to migrate the information. At the end of 180 days, the deployed content will be taken off-line and after 270 days, the contents of the external hard drives and Kiosks will be wiped in preparation for the next evolution.

b. Information/content preparing for deployment

(1) The IMO will establish a local collaborative portal in support of the mission to provide a location to conduct planning and coordination. The portal will be accessible from local computers and allow users to read and write (by permission) as required.

(2) When directed the IMO will coordinate with the G-6 to replicate with the deployed server infrastructure and push the relevant information required to conduct operations forward. The goal is to extend the reach of collaboration from local to deployed operations allowing both commands to access one instance of information.

(3) If the information cannot be replicated or pushed forward, the information will be loaded to external hard drives for deployment. External hard drives will be cataloged by the I MEF Security Manager to ensure the hard drives are tracked and reported in accordance with I MEF policy.

(4) Sections/units/individuals will load the information onto the external hard drives using a Kiosk provided by the G-6. Users will transfer the information from the collaborative portal or shared drives onto the external hard drive and into a defined folder/sub-folder structure on the Kiosk.

(5) Upon arrival in theater or deployment, the G-6 will scan the external hard drives and load the information onto the deployed environment.

c. Information associated with an individual/billet.

(1) Email records requiring migration between computers or locations will be exported to a personal storage table (PST) file and saved in one of the following formats:

(a) Written to a CD/DVD using an external media and provided to the individual requiring the information.

(b) Saved to the section shared file and then transferred using large file transfer applications Safe Access File Exchange (SAFE) system through Army Knowledge Online.

(2) Web Favorites/links required to be migrated between computers or locations will be:

(a) Written to a CD/DVD using an external media and provided to the individual requiring the information.

(b) Saved to the section shared file and then transferred using large file transfer applications like the Safe Access File Exchange (SAFE) system through Army Knowledge Online or links can be embedded into a Word Document and emailed by another staff member.

4. Administration and Logistics. Requirements for moving information from low to high or high to low classifications will be handled in accordance with reference (c) and through the I MEF Information Assurance Manager in accordance with I MEF Policy.

5. Command and Signal. The point of contact for this SOP is the I MEF Information Management Officer who may be reached at (760) 725-9136 or DSN 365-9136.

G. M. RYAN
Chief of Staff

DISTRIBUTION LIST: I