UNITED STATES MARINE CORPS
3D MARINE LOGISTICS GROUP
UNIT 38401
FPO AP 96604-8401

IN REPLY REFER TO:
5239
G-6
03 AUG 2012

COMMANDING GENERAL'S POLICY LETTER 1-12 Ch 1

From: Commanding General
To: Distribution List

Subj: 3D MARINE LOGISTICS GROUP (MLG) CYBER SECURITY TACTICAL COMMUNICATIONS CONNECTION REQUIREMENTS POLICY

1. Situation. To make changes to the Policy Letter.

2. Execution

a. Replace the word "systems" in paragraphs 3c(1)(b) and 3c(2)(c) with "computers".

b. Replace the words "Information Assurance Officer (IAO)" in paragraph 3c(1)(h) with "Cyber Security Officer (CSO)".

c. Replace the acyronm "(IAO)" in paragraphs 3c(1)(i) and 3c(2)(a) with "(CSO)".

d. Replace paragraph 3c(2)(e) with the following:

"(e) When required sign for the appropriate deployable server suite/s from 3d MLG G-6 for Non-Secure Internet Protocol Router Network (NIPERNET), Secret Internet Protocol Router Network (SIPRNET), Republic of Korea and United States Internet Protocol Router Network (RIPRNET), and/or Combined Enterprise Regional Exchange network (CENTRIX). Provide a minimum of 10 working days notification IOT properly transfer equipment."

e. Replace the words "local helpdesk or Information Assurance" in paragraph 3c(1)(i) with "designated Cyber Security".

f. Replace paragraph 3c(2)(j) with the following:

"(j) IAW reference (h), in order to avoid the use of secondary removable storage devices, all classified client and server USB ports must be disabled by default."

g. Add the following paragraph to 3c(2):

"(m) When required, deploy a minimum of two Deployed Security Interdiction Device (DSID) trained operators."

h. Remove paragraph 3d(3) and 3d(4).

i. Add the following paragraph to 3d:

"(3) CISCO IOSs are a limited distribution item, unauthorized use or distribution of this software is a violation of copyright laws."

3. Filing instructions. File this transmittal in front of the letter head page of the basic Policy Letter.

W. T.

W. T. ANDERSON
Chief of Staff
Acting

UNITED STATES MARINE CORPS
3D MARINE LOGISTICS GROUP
UNIT 38401
FPO AP 96604-8401

IN REPLY REFER TO:
5239
G-6
18 JUN 2012

COMMANDING GENERAL'S POLICY LETTER 1-12

From: Commanding General, 3d Marine Logistics Group
To: Distribution List

Subj: 3D MARINE LOGISTICS GROUP (MLG) CYBER SECURITY TACTICAL COMMUNICATIONS CONNECTION REQUIREMENTS POLICY

Ref: (a) DoD Directive 8500.1
(b) DoD Instruction 8500.2
(c) SECNAVINST 5239.3A
(d) MCO 5239.2
(e) EIAD 018
(f) MCBUL 5234
(g) MARADMIN 647/08
(h) MARADMIN 590/05

Encl: (1) Baseline Image List

1. Situation. As of January 2012, 3d MLG G-6 began deploying one Cyber Security Marine (0689) to every exercise/operation. Some of the reoccurring problems these Marines have identified during the exercises include: out of date antivirus software and patches on deployed clients and servers, improperly configured routers and switches, and installation of unapproved network devices or end client assets.

2. Mission. This policy provides connection requirements for the installation of tactical data communication networks in order to provide the most secure environment possible during 3d MLG exercises/operations.

3. Execution

a. Commander's Intent

(1) Purpose. To provide deploying units direction by ensuring risks to 3d MLG tactical data networks are identified, prevented, or mitigated to the maximum extent possible.

Distribution Statement A: Approved for public release; distribution is unlimited.

(2) Method. Mitigate risk by implementing a defense in depth strategy outlined in this policy.

(3) Endstate. Provide the 3d MLG and its Major Subordinate Elements (MSE) with secure tactical communication services operating within an acceptable level of risk.

b. Concept of Operations. To ensure risks to 3d MLG tactical network assets are prevented or mitigated prior to units deploying, 3d MLG G-6 will provide preconfigured operating systems and servers to deploying units. Furthermore, if available one cyber security Marine will deploy forward to each exercise/operation in order to ensure risks are mitigated to the maximum extent possible.

c. Tasks and Responsibilities

(1) Assistant Chief of Staff (AC/S), G-6

(a) Per reference (e), 3d MLG G-6 will complete the Marine Corps Certification and Accreditation Process for all tactical exercises/operations where communications is provided. Provide a copy of the (Interim) Authority to Operate/Connect ((I)ATO/C) to requesting units.

(b) Create and maintain baseline images for standard client and Combat Operations Center (COC) Capabilities Set (CAPSET) systems.

(c) Download and archive the weekly Marine Corps Network Operations and Security Center (MCNOSC) Access Control Lists (ACL).

(d) Ensure 3d MLG tactical servers have the most current and secure configurations and updates (antivirus, Microsoft updates, etc) installed.

(e) Issue 3d MLG deployed server suites when requested by MSEs.

(f) When available, provide one cyber security Marine (0689) for each exercise/operation as well as any communication exercise conducted in preparation for the deployment.

(g) Assess deployed networks and provide assistance to ensure they remain as secure as possible. Provide the supported communications officer a written assessment of their network vulnerabilities within three weeks of exercise/operation completion.

(h) Prior to each exercise or operation issue baseline images for all client and COC CAPSET systems to the deploying unit's system administrator or Information Assurance Officer (IAO). Refer to enclosure (1) for a comprehensive list of all makes and models currently provided.

(i) Prior to each exercise or operation, issue the latest Access Control Lists (ACLs) and router/switch templates to the deploying unit's system administrator or IAO.

(j) Upon deploying unit request, issue the most current CISCO Internal Operating System (IOS) software.

(2) <u>Regimental and separate Battalion Commanding Officers</u>

(a) Appoint an IAO for each exercise or operation.

(b) Prior to and during each exercise/operation receive and maintain a current approved accreditation package and (I)ATO/C from the 3d MLG G-6 Operations section. Ensure all connections and systems are in accordance with the approved (I)ATO/C and associated network diagrams.

(c) Prior to each exercise/operation, implement the latest baseline images received from 3d MLG G-6 for all client and COC CAPSET systems.

(d) Implement the latest ACL modifications on all applicable devices.

(e) When required sign for the appropriate deployable server suite/s from 3d MLG G-6 for Non-Secure Internet Protocol Routed Network, Secret Internet Protocol Routed Network, and/or Republic of Korea and United States Internet Protocol Routed Network.

(f) When required, obtain and implement the latest CISCO IOS software with the approved router and switch configuration templates from the 3d MLG G-6.

(g) Comply with MCNOSC Operational Directives released during deployments.

(h) Provide any laptops, not identified in enclosure (1) to 3d MLG G-6 to ensure they are loaded with the appropriate software, updated with the most current patches, and made available at all times.

(i) In accordance with (IAW) reference (g), ensure government hard drives used on any unclassified networks are first scanned for malicious code by local helpdesk or Information Assurance personnel and labeled with a SF 710 classification sticker.

(j) IAW reference (h), all classified system USB ports must be disabled by default for the use of secondary removable storage devices. This includes clients and servers.

(k) Immediately notify the local helpdesk and/or IA staff of any suspected network incident(s) (e.g., spillage, network intrusion, virus, etc). The designated IAO must notify the 3d MLG Information Assurance Manager (IAM) immediately or as soon as practical.

(l) Obtain approval via 3d MLG G-6 prior to connecting any systems not issued by the 3d MLG G-6 to 3d MLG tactical networks.

d. Coordinating Instructions

(1) Exercise IAOs, with the assistance from 3d MLG G-6, will ensure all deployed networks are operating within an acceptable level of risk.

(2) Only baseline images, servers, router and switch templates issued by 3d MLG G-6 or pre-approved systems are authorized for use on tactical networks. Requests to change the security posture on any pre-approved system must be made to the 3d MLG G-6 prior to applying changes. Unapproved changes that affect the security posture of 3d MLG tactical networks may result in a recommendation for disconnection from the network.

(3) Only baseline images, servers, router and switch templates issued by 3d MLG G-6 or pre-approved systems are authorized for use on tactical networks. Requests to change the

security posture on any pre-approved system must be made to the 3d MLG G-6 prior to applying changes. Unapproved changes that affect the security posture of 3d MLG tactical networks may result in a recommendation for disconnection from the network.

(4) CISCO IOS' are a limited distribution item, unauthorized use or distribution of this software is a violation of copyright laws.

4. Administration and Logistics. Recommendations for changes to this policy should be submitted to the AC/S G-6 via the appropriate chain of command. The point of contact for this policy is the 3d MLG IAM and may be reached via phone by DSN 315-637-1840 or by e-mail at 3mlgg6ia@usmc.mil.

5. Command and Signal

a. Command. This Order applies to all units within 3d MLG.

b. Signal. This Policy Letter is effective on the date signed.

S. E. ERDELATZ
Chief of Staff

Unclassified

Baseline Image List

Model	Baseline		COC - INT		COC - LOG		COC - OPS	
	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR	NIPR	SIPR
T-510	X	X	X	X				
R500	X	X						
R61	X	X						
Dell - COC Machines			X	X	X	X	X	X
Toughbook CH-19	X							

Enclosure (1)