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
ISMO
APR 29 2011

POLICY LETTER 6-11

From: Commanding General
To: Distribution List

Subj: COMMERCIAL INTERNET NETWORK ACCESS SERVICE POLICY

Ref: (a) DoDI 4640.14, DISN Connection Process Guide

Encl: (1) Executive sponsorship appointment letter
(2) System Authorization Access Requests (SAAR DD Form 2875)
(3) Commercial internet network access service procurement checklist

1. Situation. The I Marine Expeditionary Force Command Element (I MEF CE) uses "White Lines" for certain areas aboard the installation. These areas are without Navy Marine Corps Intranet (NMCI) service or Outlook Web Access, and White Lines may be used to verify public websites, unclassified bandwidth intensive applications, and to perform those applications restricted on the Marine Corps Enterprise Network Non-classified Internet Protocol Router Network (MCEN NIPRNET) for unclassified communications. White Lines allow access to these otherwise restricted areas of the internet and increased oversight is required to ensure compliance with Information Assurance (IA) policies and guidelines.

2. Mission. Pursuant to the reference, this letter establishes policy for the use of commercial Internet access for official business ("White Lines") in the absence of NMCI support.

3. Execution. White Line access shall be controlled by an appointed Executive Sponsor who is overall responsible for the employment and usage of White Lines. Strict adherence to this policy is required. Executive sponsors are the Executive Officers or Deputy Assistant Chiefs of Staff and shall be appointed in writing. Enclosure (1) contains a sample of an assignment letter.

a. Information Systems Coordinator. Each White Line access area shall have an appointed Information Systems Coordinator (ISC). Responsibilities include but are not limited to:

(1) Ensure all white line clients system patches and antivirus signatures are current. Contact the I MEF G-6 and IA for guidance.

(2) Ensure all White Line clients are scanned for viruses daily.

(3) Ensure only authorized government clients are connected to White Line networks and that they are provided with a Common Access Card (CAC) Card reader.

(4) Establish a separate I-MEF COMMERCIAL (ISP) WHITELINE all user System Authorization Access Requests, (SAAR DD Form 2875), enclosure (2) for anyone requiring access to a White Line.

(5) Ensure users do not have administrative access to clients or network devices and that only authorized users access the White Line. Contact the I MEF G-6 and IA for configuration.

(6) Provide local IA staff with full administrative and physical access to all devices on the network.

(7) Ensure that all White Line users receive a White Line threat and IA brief from the local IA staff.

(8) Ensure that all white line systems are labeled UNCLASSIFIED and connected with white CAT5, CAT5 or CAT6 cabling.

b. White line users. All White Line users will sign for the computer and login using a unique logon and password.

(1) White Line networks will not be connected to any other network.

(2) Computers will not be moved between the NIPRNet and White Line networks.

(3) Data transfers between White Lines and the NIPRNet (either direction) will follow the "Low to High" transfer procedures and be scanned by IA before being uploaded to the NIPR.

(5) Wireless connections are not authorized on White Lines.

(6) White Line deactivation will be reported to the I MEF G-6 Helpdesk.

(7) In the case of suspicious activity or incidents, the local IA staff must be notified immediately, and the client must be disconnected from the network (remain powered on).

(8) Violations of this policy may result in termination of the service.

(9) Misuse of this system with regard to accessing or viewing pornographic images/materials or illegal/restricted sites and activities to include but, not limited to creating, downloading, viewing, storing, copying, or transmitting materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials may be punishable under the Uniform Code of Military Justice.

c. I MEF G-6

(1) White line connections will pass through a software firewall configured by the local IA Staff.

(2) Local IA staff will inspect and scan each White Line monthly Results will be reported to the AC/S G-6.

(3) The I MEF G-6 Helpdesk will configure all clients to the I MEF CE System baseline prior to connection to a White Line. The Department of Defense (DoD) warning banner must be installed. I MEF G-6 will install key logging software on each White Line client.

(3) Software updates and patches, including antivirus signatures, will be configured to update daily. Users will immediately apply any updates requiring their action.

(4) Only government owned systems will be connected to White Lines. Exceptions must be explicitly approved by the I MEF G-6. Personally owned computers are not authorized for connection unless screened by the I MEF G-6.

(5) Unauthorized systems connected to the White Line will be confiscated, scanned for sensitive data, and data wiped prior to its return.

(6) For economy and management, the I MEF G-6 may direct sharing of White Lines between sections or organizations.

4. Adminstarion and Logistics. Purchase Requests (PR) for White Lines require MEF G-6 endorsement and must include:

a. Justification, to include detailed mission requirement, existing infrastructure shortfalls, and applications and sites to be accessed. Morale and related activity is not a valid justification.

b. Detailed proposed network diagram showing office layout, doors, transparent windows, cable modem, and all computers (NIPR, SIPR, White Line, etc.) in the area.

c. All procurements will include the purchase of a router/switch/hub to be configured by the G6 Network Operations Center (NOC). (Contact the I MEF G-6 to determine the brand name and type of router/switch/hub required.)

d. Serialized list of all devices to be connected and their owning unit(s).

e. Executive Sponsor's acknowledgement of this policy letter.

f. Once enclosure (3) is provided by the I MEF G-6 and both the Executive sponsor and Information Systems Coordinator are appointed, the request will be forwarded to the I Marine Expeditionary Force Headquarters Group (I MEF MHG) Supply Officer for processing. Funding must come from the requesting department.

5. Command and Signal. The point of contact for this policy is the I MEF G-6 Information Systems Management Officer who may be reached at 763-2643.

G. M. RYAN
Chief of Staff

Distribution: I, II

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
ISMO

From: Assistant Chief of Staff G-X
To: Rank, FNAME LNAME
Via: Subordinate G-X/S-X

Subj: APPOINTMENT AS (SECTION/ORGANIZATION) WHITE LINE EXECUTIVE SPONSOR

Ref: (a) I-MEF Policy Ltr 6-11 dtd DD MMM 11

1. In accordance with the reference, you are hereby appointed as the Section/Unit White Line Executive Sponsor. You will be guided by the references in the execution of your duties.

2. As the White Line Executive Sponsor, you are responsible for the compliance requirements contained in the reference. If you require assistance in the conduct of your duties, contact the I-MEF G6 Information Systems Management Officer or Chief at 763-2643.

I. M. SECTION HEAD

DD MMM YY

FIRST ENDORSEMENT

From: Rank, FNAME, LNAME
To: Assistant Chief of Staff G-6

1. I have read and understand the reference and have assumed the duties and responsibilities with my appointment.

F. M. LNAME

ENCLOSURE (1)

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST ☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID	DATE *(YYYYMMDD)*
SYSTEM NAME *(Platform or Applications)*	LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*	2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE *(DSN or Commercial)*	
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP ☐ US ☐ FN ☐ OTHER	9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*
☐ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)* _____

11. USER SIGNATURE	12. DATE *(YYYYMMDD)*

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:
☐ AUTHORIZED ☐ PRIVILEGED

15. USER REQUIRES ACCESS TO: ☐ UNCLASSIFIED ☐ CLASSIFIED *(Specify category)*
☐ OTHER _____

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. ☐	16a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)*

17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE *(YYYYMMDD)*
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE *(YYYYMMDD)*

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE *(YYYYMMDD)*

26. NAME *(Last, First, Middle Initial)*

27. OPTIONAL INFORMATION *(Additional information)*

By signing block 11 I agree to the following rules of behavior:

- I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access to my files and e-mails which reside or were created on Government IT resources.
- I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment.
- I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function.
- I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems.
- I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter.
- I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property.
- I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials.
- I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity.
- I will not post Marine Corps information to external newsgroups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in ones official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions.
- I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- I will not modify or attempt to disable any anti-virus program running on a Marine Corps IT system without proper authority.
- I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval.

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(5)Official E-mail Address. The user's official e-mail address.

(6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(7) Official Mailing Address. The user's official mailing address.

(8) Citizenship (US, Foreign National, or Other).

(9) Designation of Person (Military, Civilian, Contractor).

(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.

DD 2875 ADDENDUM
STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

• You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

• You consent to the following conditions:

o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

o At any time, the U.S. Government may inspect and seize data stored on this information system.

o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Initials _____

data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection Of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Initials _____

COMMERCIAL INTERNET NETWORK ACCESS SERVICE, PROCUREMENT CHECKLIST

- Review CG Policy Letter 6-11.
- Provide justification to support mission requirement.
- Appoint a White Line Executive Sponsor.
- Appoint a White Line ISC (can be current section/unit ISC).
- Deliver Executive Sponsor and ISC Acknowledgement Letters to G6 ISMO.
- Deliver complete detailed diagram of building, doors, windows, cable modem and all computers (SIPR, NIPR, WHITELINE) to the G6 ISMO.
- Serialized list of all devices to be connected to the White Line Network.
- Ensure Purchase Request includes a Router/Switch/Hub/CAC Card Reader.
- All users will complete a DD FORM 2875 (SAAR).
- White Line Threat Brief received from G6 IAM.

DD MMM YY

From: I MEF G-6 ISMO
To: MHG Supply Office

1. All above items have been addressed or received from the (Section/Unit) White Line Executive Sponsor.

G. 6. ISMO