



UNITED STATES MARINE CORPS
1ST MARINE AIRCRAFT WING
UNIT 37101
FPO AP 96603-7101

IN REPLY REFER TO:
5271
10

12 NOV 2002

COMMANDING GENERAL'S POLICY LETTER 13-02

From: Commanding General
To: Distribution List

Subj: AUTHORIZATION TO MONITOR USERS' NETWORK ACTIVITIES

Ref: (a) CNO WASHINGTON DC 041950Z Oct 02
(b) MARADMIN 162/00

Encl: (1) Request For AC/S G-6 Support For Investigations

1. Purpose. Define internal policy authorizing network administrators to research or monitor a user's activity on any of the 1st Marine Aircraft Wing (1st MAW) networks.

2. Background. As defined in the references, government computer systems are a valuable resource to ensure effective command and control during combat operations. The privilege of using government systems have been extended to designated individuals for official and authorized purposes only. The intent of this policy is to identify misuse without the appearance of bias or inequality. The 1st MAW network will employ Public Key Infrastructure (PKI) technology. This allows users to have added security and protection of their mailbox contents.

3. Policy

a. Pursuant to this policy, commanders may request that the network administrator access and analyze the contents of a mailbox that belongs to a user who is the subject of a related investigation under the following guidelines:

b. Electronic Mail (E-mail)

(1) A network administrator may open any mailbox exceeding authorized Exchange Server limits to determine if there is any misuse as defined by the references and this policy.

(2) Any user whose name is found on an e-mail or web content or extract with questionable materials (e.g. porno-graphy, derogatory comments of any type, threats to anyone, unprofessional conduct or harassment) will have their mailbox opened by an

administrator to determine if there is any misuse as defined by the this policy.

(3) A commander may request Private Keys from the Assistant Chief of Staff G-6 (AC/S G-6) in order to support an investigation in which the content of an individual's mailbox is relevant.

c. Internet. Any user who attempts to go to web sites blocked for questionable or inappropriate content is subject to having all of his Internet sessions searched by an administrator for misuse as defined by the references.

d. Workstations. During routine help desk support, any member of the AC/S G-6, S-6 or Information Systems Coordinator (ISC) staff who discovers potential misuse as defined by the references will report it via his chain of command for appropriate follow-on monitoring or investigative action.

e. Command Action. Commanders may request access to e-mail and Internet content belonging to a user under investigation.

4. Action

a. The AC/S G-6 will ensure compliance with the above policy effective immediately.

b. In any cases of suspected child pornography, the Naval Criminal Investigative Service (NCIS) will be immediately notified by the command.

c. The AC/S G-6 is authorized to suspend the Internet and e-mail account of any user who is reportedly in violation of this policy until a command decision can be made following a preliminary inquiry.

d. A commander who desires the AC/S G-6 to access the network account of a user under investigation shall complete enclosure (1) and submit it to the AC/S G-6. The AC/S G-6 will forward a copy to the Staff Judge Advocate (SJA) prior to acting on the request.

e. The SJA will provide advice regarding the legality of any search conducted under this policy.


J. F. GOODMAN

Distribution List: List 1/2/3

Request For AC/S G-6 Support For Investigations

1. Date of request: _____
2. Name of user being investigated: _____
3. Computer name: _____
4. Suspected infraction: _____
5. Is there a need to maintain covertness concerning monitoring/auditing activities? Yes / No. If yes, explain.

6. Action requested: (describe type of logs or data to be provided or activity to be monitored, i.e., email, internet usage, log in/out times, etc.)

7. End product requested: (log data, log data analysis, email routes, email contents, internet sites, etc.)

8. Beginning and ending date/time of period being investigated: _____
9. Lock user's network account? Yes / No
10. Disable user's e-mail account: Yes / No
11. Other pertinent information: _____
12. ISSO: (list the ISSO for the area/system): _____
13. Requestor/Point of Contact: (full name, rank, phone, e-mail)
14. Requestor Signature: _____ Date: _____
15. Authorizing Official (Commanding Officer, OIC)
Printed Name: _____ Title: _____ Phone: _____
16. Authorizing Official Signature: _____ Date: _____

=====

TO BE COMPLETED BY G6

To be completed by NOC:

17. Feasibility / Estimated man-hours: _____

To be completed by ISSM:

18. Approved _____ Disapproved _____

19. ISSM Signature: _____ Date: _____