DEPARTMENT OF THE NAVY
COMMANDER MILITARY SEALIFT COMMAND
914 CHARLES MORRIS CT SE
WASHINGTON NAVY YARD DC 20398-5540

REFER TO:

COMSCINST 5235.3
N6
27 February 2001

COMSC INSTRUCTION 5235.3

Subj: REMOTE ACCESS TO UNCLASSIFIED SYSTEMS

Ref: (a) Chief of Naval Operations (CNO) Washington DC//N6 memo of 8 Jun 99
(b) NAVCIRT Advisory 00-028 of 13 Jul 00

1. Purpose. To disseminate Military Sealift Command (MSC) policy for accessing the unclassified e-mail systems from remote locations.

2. Background. MSC requires a secure, enterprise wide solution for providing remote dial-in access to unclassified e-mail systems. The remote dial-in access solution must support MSC employees and contractors who are performing mission-related functions at locations that lack direct connectivity to MSC's messaging systems and unclassified LANs. This need exists for MSC's smaller offices, employees on travel, personnel temporarily working at non-MSC locations (such as shipyards) and for employees working from home.

3. Policy

a. Any device remotely accessing MSC's e-mail systems or unclassified LANs is subject to monitoring in accordance with reference (a). Use of MSC's remote access system is for official U.S. Government business only. All activity is subject to monitoring at all times to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity and for other similar purposes.

b. Remote dial-in access from MSC field commands and MSC owned laptops will be fully supported by the Director, Command, Control, Communication and Computer Systems (C4S) (N6). Documentation and software will be provided to support non-MSC devices such as employee's home computers.

c. Remote dial-in access for Personal Digital Assistants (PDA) will not be supported. In accordance with reference (b), password, combinations, PINs and classified information should not be entered into a PDA.

d. All devices remotely accessing an MSC e-mail system or unclassified LAN must be running a current version of MSC's specified Anti-Virus Protection Software.

e. All devices remotely accessing an MSC e-mail system or unclassified LAN must be running one of the following Windows Operating System (OS): NT, Windows95 or Windows98. Windows 2000 will be considered for future implementations.

f. Each user remotely accessing an MSC e-mail system or unclassified LANs will be required to use a RSA SecurID Key Fob, which supports a two-factor, token based identification authentication system.

4. Responsibilities

a. Director, C4S (N6) is responsible for:

(1) Hardware and software required to implement a remote access solution. In particular, N6 will maintain the network access server, the SecurID Key Fobs and the Remote Access Security Software.

(2) Managing and distributing the remote access accounts and the Key Fob tokens.

(3) Providing training and documentation for remote access users.

(4) The installation and configuration of the remote access components on MSC-owned devices such as workstations and laptops. Individual users will be responsible for installation and configuration of non MSC-owned devices such as home computers.

(5) Monitoring and maintaining the remote access logs for security violations.

(6) Maintaining copies of the current Anti-Virus Software release.

b. Remote Users are responsible for:

(1) Abiding by DOD Computer Systems regulations in accordance with reference (a).

(2) Maintaining and ensuring the physical security of the SecureID key fobs; reporting any theft or loss to the helpdesk immediately. Do not write down the PIN number associated with the assigned token. The PIN comprises the first part of the token based identification authentication system.

(3) Ensuring that non MSC-owned devices are running a current version of MSC's specified Anti-Virus Protection Software.

5. Action. Program Managers/Functional Directors/Special Assistants should give this policy the widest dissemination as possible.

//S//
G. S. HOLDER

Distribution:
COMSCINST 5215.5
List I (Case A, B, C)
SNDL 41B (MSC Area Commanders)
41C (NFAF East/West)
41D (MSC Offices)
41E (APMC)
41K (COMAPSRON FOUR)
41L (COMPSRONs)
41M (TAGOS Project Office & Det)