

COMOMAGINST 5239.1D
N6
31 Mar 03

COMOMAG INSTRUCTION 5239.1D

Subj: INFORMATION SYSTEM SECURITY PLAN (ISSP)

Ref: (a) SECNAVINST 5239.3
(b) COMLANTFLTINST 5239.1 CHG-1
(c) COMINWARCOMINST 5239.1D
(d) OPNAVINST 5239.1B
(e) COMOMAG/MOMAGINST 5230.1C
(f) COMINWARCOMINST 5231.1A

Encl: (1) COMOMAG Hardware and Software Inventory Summary

1. Purpose. To establish the Commander, Mobile Mine Assembly Group (COMOMAG) Information System Security Plan (ISSP) as directed by references (a) through (c). All MOMAG units/detachment are required to implement an Information System Security Plan. Enclosure (1) may be used as a reference.

2. Cancellation. COMOMAGINST 5239.1C. This instruction is a major revision and should be reviewed in its entirety.

3. Scope. COMOMAG is tasked with maintaining COMLANTFLT, COMPACFLT and COMUSNAVEUR mines and mine exercise training assets at predetermined states of readiness consistent with general wartime contingency plans developed by Commander, Mine Warfare Command (COMINWARCOM) and with peace time exercise and training requirements imposed by fleet commanders. To accomplish this, COMOMAG maintains seven permanently manned mine assembly sites world-wide. Under the Department of Defense's current force reduction trend, the use of information systems (IS) has become essential in COMOMAG's effort to meet its mission objectives.

The Information System Security Plan will serve as a central guide in managing the IS security environment at COMOMAG and define the security environment under which IS equipment will operate. The plan will document the current security environment and IS security objectives, assign information system security responsibilities and outline a Plan of Action and Milestones (POA&M) for achieving and maintaining information system accreditation.

4. Commanding Officer's Policy Statement. All information system equipment installed within COMOMAG will be accredited and operated in accordance with IS security requirements outlined in references (a) through (d). To meet these requirements, the IS security staff will develop and implement the information system security plan described herein which defines the steps required to achieve accreditation

31 Mar 03

status and outlines the timeframes within which those steps will be accomplished. This plan will receive the full support of all staff members and will be reviewed and updated on a continuing basis.

5. IS Security Organization and Responsibilities. COMOMAG has established an IS security team to assist in IS security matters. The duties and responsibilities of the commanding officer/officer-in-charge and the information system security team are defined in reference (e). The IS security team consists of the following:

- a. Information System Security Manager (ISSM)
- b. Information System Security Officers (ISSO)
- c. Network Security Officer (NSO)
- d. Terminal Security Officers (TSO)
- e. Primary and Alternate Information Vulnerability Alert (IAVA) Representative.

6. IS Security Objectives. COMOMAG's IS security objective is to provide a secure processing environment for all IS processes and equipment used by command personnel. This ISSP is designed to establish and maintain an environment imposed by constant growth and change. The specific objectives are:

- a. Establish an information system security instruction and an information system security plan for command IS equipment.
- b. Establish an Activity Accreditation Schedule (AAS).
- c. Submit the information system security plan to the Designated Approving Authority (DAA) for their review and request an Interim Authority to Operate.
- d. Develop an adequate IS security staff who are designated in writing and are properly trained.
- e. Complete those steps required to achieve accreditation for staff Information Systems Technicians (ITs) that include:
 - (1) Completing a risk assessment and implementing cost effective countermeasures.
 - (2) Developing and implementing an IS contingency plan.
 - (3) Conducting a security test and evaluation.
 - (4) Assembling and submitting accreditation support documentation to the DAA.

(5) Requesting a statement of accreditation.

f. Establish a schedule for accreditation review.

g. Develop and implement a comprehensive IS security awareness program for all staff personnel.

7. Current IS Security Environment. COMOMAG currently operates under an accreditation issued by the DAA dated 7 September 2001. COMOMAG's current IS environment is described as follows:

a. Hardware and Software. Enclosure (1) is a listing of all hardware and software used by COMOMAG staff personnel.

b. Physical/Facility Security. The COMOMAG headquarters, Building 36, is a two-story, wood framed, stucco building located onboard NAS Corpus Christi, TX. Security is provided by NAS Corpus Christi Security personnel and is limited to periodic motorized patrols. Fire fighting support is provided by the NAS Corpus Christi Fire Department.

The headquarters building is a secure facility that is manned during normal working hours. The building is secured outside of normal working hours, during which time an alarm system is activated. Access to the building is controlled by a quarterdeck watch who is responsible for ensuring visitors are properly recorded in a visitor's log, that a color coded visitor's pass is issued and escorts are provided for command visitors and uncleared personnel. In addition, each department is responsible for maintaining security within their spaces.

c. Personnel. COMOMAG has a complement of nine officers, 27 enlisted and six civilian personnel assigned. All members receive an IS security brief from the ISSM within thirty days of their arrival and an annual IS security brief is required. All staff members, as a minimum, are cleared for secret access.

d. Communications. Selected classified data and voice communications are provided via National Security Agency (NSA) approved STU-III devices. Classified e-mail and web access are available via SIPRNET. Unclassified e-mail and web access are available via NIPRNET. Some workstations are configured to access WEB-based applications via SIPRNET/NIPRNET links, boards and on-line processes, such as BUPERS Access. Examples include the Standard Accounting and Reporting System-Field Level (STARS-FL) and the Naval Ammunitions Logistics Center (NALC), Single Integrated Electronic Filing Cabinet for Ordinance Logistics Enterprise (SIEFC) web site.

e. Emanations. While all naval activities located on a secure naval facility are exempted from TEMPEST review requirements, COMOMAG continues to observe proper TEMPEST profiles.

f. Administrative/Operating Procedures. References (e) and (f) outline COMOMAG's standing security and operational procedures for IS equipment.

g. Data. Aside from daily data back-ups to magnetic tape, the safeguarding and handling procedures required for data is determined by its classification level. The following percentages are representative of the annual volumes processed by COMOMAG:

<u>Level</u>	<u>Quantity</u>	<u>Percent</u>
Level I (classified)	TS - 0 S - 2,066 C - 3,500	0 10 17
Level II (sensitive unclassified)	- 200	1
Level III (unclassified)	- 15,000	72
Total:	<hr/> 20,766	100

8. Training. Prospective ISSMs, ISSOs, NSOs and TSOs are required to attend formal IS security training prior to assuming their duties. All user security training is accomplished via mandatory annual security briefs.

9. ISSP Review. This ISSP will be reviewed each time major changes occur in the command's organizational structure, hardware or software configuration, user population, data classification levels and/or security profile. At a minimum, the plan will be reviewed and updated every three years.

10. Life Cycle Management (LCM). References (a), (e) and (f) outline LCM requirements for IS equipment. The ISSM is responsible for ensuring appropriate LCM documentation is developed and submitted for COMOMAG IS requirements.

11. Hardware/Software Configuration Control. The ISSM is responsible for maintaining accurate records of all hardware and software purchased for COMOMAG. In addition, the ISSM will review all IS procurement requests to ensure they comply with IS security requirements.

/s/
T. W. AUBERRY

Distribution:
COMOMAGINST 5216.1T
List I
List II (Case A, Case B (COMINEWARCOM only))
List III

HARDWARE AND SOFTWARE INVENTORY SUMMARY

I. Hardware:

<u>Item</u>	<u>Quantity</u>
1. Pentium 2GHZ Workstation 256mb RAM PCI Video 20gb IDE Drive 17 inch Flat LCD Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	1
2. Pentium 1GHZ Workstations 128mb RAM PCI Video 6gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	15
3. Pentium 933 Workstations 256mb RAM PCI 16mb Video 10gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	3
4. Pentium 733 Workstations 256mb RAM PCI Video 10gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	5
5. Pentium 700 Workstations 256mb RAM PCI Video 10gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	1

Encl (1)

COMOMAGINST 5239.1D
31 Mar 03

<u>Item</u>	<u>Quantity</u>
6. Pentium 600 Workstations 128mb RAM PCI Video 10gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	1
7. Pentium 500 Workstations 128mb RAM PCI 16mb Video 6gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	2
8. Pentium 450 Workstations 128mb RAM PCI 4mb Video 6gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	9
9. Pentium 350 Workstations 128mb RAM PCI 4mb Video 4gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	2
10. Pentium 300 Workstations 128mb RAM PCI 4mb Video 4gb IDE Drive 17 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse	2

HARDWARE AND SOFTWARE INVENTORY SUMMARY (Cont.)

<u>Item</u>	<u>Quantity</u>
-------------	-----------------

11. Del M50 Laptop 512mb RAM SVGA Color LCD 20gb IDE Hard Drive	1
12. Del C840 Laptop 256mb RAM SVGA Color LCD 20gb IDE Hard Drive	7
13. Gateway Solo 9300 Laptop 128mb RAM SVGA Color LCD 10gb IDE Hard Drive	4
14. Gateway Solo 5150 Laptop 128mb RAM SVGA Color LCD 10gb IDE Hard Drive	1
15. Panasonic CF-27 Laptop 128mb RAM SVGA Color LCD 10gb IDE Hard Drive	3
16. HP Netserver LP6000 File Server 1gb RAM PCI Bus Dual PCI SCSI Controllers 60gb RAID SCSI Hard Drives 14 inch VGA Monitor 101 Enhanced Keyboard Microsoft Mouse	1
17. Gateway 6400 File Server 512mb RAM PCI Bus Dual PCI SCSI Controllers 60gb RAID SCSI Hard Drives 14 inch VGA Monitor 101 Enhanced Keyboard Microsoft Mouse	1

HARDWARE AND SOFTWARE INVENTORY SUMMARY (Cont.)

Item Quantity

18.	Dual PENTIUM 300mhz File Server 256mb RAM PCI Bus Dual PCI SCSI Controllers 16gb RAID SCSI Hard Drives 14 inch VGA Monitor 101 Enhanced Keyboard Microsoft Mouse	2
19.	Pentium P5-166 CD-ROM Server 96mb RAM 4gb SCSI Hard Drive 15 inch SVGA Monitor 101 Enhanced Keyboard 3COM LAN Interface Card Microsoft Mouse SMS Dual CD-ROM Tower 14 12X Speed CD Drives Pentium 120 CR-ROM Server	1
20.	HP 6000 Color Printer	2
21.	HP LaserJet 4si Printer	1
22.	HP LaserJet 5si Printer	2
23.	HP LaserJet 5 Printer	3
24.	HP LaserJet 4050 Printer	3
25.	10/100 Ethernet Switches	9
26.	Cabletron 10/100 Ethernet Switch	1
27.	Sun ULTRASPARC	1

HARDWARE AND SOFTWARE INVENTORY SUMMARY (Cont.)

II. Software:

Item

1. ADPINV 1.0
2. ArchServ Tape Back-up
3. Corel Draw Ver 8.0
4. DPVS 5.0
5. EPSQ
6. FASTDATA
7. FEDLOG
8. FAMP
9. GOPAS
10. JFTR/JTR for Windows
11. MDS Ver 4.5
12. Microsoft Windows NT 4.0
13. Microsoft Office Pro 97
14. Microsoft Project 5.0
15. Microsoft Windows 98
16. MSORTS
17. NDSP
18. PCMETRL
19. TAMPS
20. UMPUM
21. VISIO