



## DEPARTMENT OF THE NAVY

ENLISTED PLACEMENT MANAGEMENT CENTER  
NEW ORLEANS, LOUISIANA 70159-7900

IN REPLY REFER TO:  
Code 40IT  
2 Apr 01

EPMAC DOCUMENT NUMBER 5230#1 UM-01

From: Commanding Officer, Enlisted Placement Management Center

Subj: READINESS INFORMATION SYSTEM USERS' MANUAL (RISMAN)

Encl: 1 Readiness Information System Users' Manual

1. Purpose. To update and publish the procedures to use the Readiness Information System (RIS).

2. Cancellation. Previous edition cancelled effective 23 March 2001.

3. Background. The Readiness Information Systems Users' Manual (RISMAN) is the official manual used to provide Manning Control Authorities (MCAs) and the Enlisted Placement Management Center (EPMAC) the ability to obtain, via a teleprocessing system, current essential management information. The MCAs, (Naval Personnel Command (NAVPERSCOM), Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), Commander in Chief, U.S. Pacific Fleet (CINCPACFLT), Commander, Naval Reserve Force (COMNAVRESFOR)) and EPMAC require this information to monitor personnel manning and readiness.

4. Action. Effective 23 March 2001.

  
G. B. DYE

# READINESS INFORMATION SYSTEM (RIS)



**USERS ' MANUAL**

**(TABLE OF CONTENTS)**

**[Feedback Form](#)**

## INTRODUCTION

### About the Readiness Information System (RISMAN)

The RISMAN consists of two parts and appendixes.

**INTRODUCTION:** Introduction of the RISMAN describes the Readiness Information System (RIS), how to obtain access to RIS, and how to access RIS. The Introduction is broken into three sections.

**Section A: RIS Functional Description.** Describes the system, its use, capabilities, and security.

**Section B: Obtaining access to RIS.** Explains the procedures to obtain initial or additional access to RIS.

**Section C: Accessing RIS.** Briefly describes hardware/software requirements needed to access RIS.

**TRANSACTIONS:** This part of the RISMAN describes how to use RIS. Transactions are broken into two sections.

**Section A: Using RIS.** Explains the parameters used in the system, system error messages, and the standard abbreviations used in the parameters.

**Section B: File and Program Descriptions.** Describes the files and programs within RIS for the user to determine which program is needed to get the desired information.

**Appendixes:** The appendixes contain additional information about RIS and tables of the different codes used in Enlisted Distribution and RIS.

RIS FUNCTIONAL DESCRIPTION

1-1. Background Information. The Readiness Information System (RIS) provides Manning Control Authorities (MCAs) and the Enlisted Placement Management Center (EPMAC) the ability to obtain, via an Automated Information System (AIS), current essential management information. The MCAs (Navy Personnel Command (NAVPERSCOM), Commander in Chief, U.S. Pacific Fleet (CINCPACFLT), Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), Commander, Naval Reserve Force (COMNAVRESFOR)) and EPMAC need this information to monitor personnel manning and readiness.

1-2. Objectives of the System. The objective of RIS is to provide available management information concerning personnel manning and readiness, which is necessary to EPMAC, MCAs, and subordinate commanders in fulfilling their respective missions. RIS information must be reliable, current, and accessible in a timely manner.

1-3. Personal Privacy. Department of the Navy (DON) policy prohibits disclosure of names and duty addresses or duty telephone numbers of service members when disclosure would reveal classified information or when disclosure "would constitute a clearly unwarranted invasion of personal privacy". Disclosure of names and duty addresses or duty telephone numbers of members assigned to units that are stationed in foreign territories, routinely deployable, or sensitive can constitute a clearly unwarranted invasion of personal privacy. Disclosure of such information poses a security threat to those service members because it reveals information about their degree of involvement in military actions in support of national policy, the type of naval unit to which they are attached, and their presence or absence from their households.

1-4. System Certification. EPMAC became fully accredited 13 May 92 which certifies that appropriate Information System Security (INFOSEC) safeguards have been properly implemented, tested and that each AIS is adequately protected as required by SECNAVINST 5239.3.

1-5. Security

a. Information. Access to RIS is controlled by an identification and authentication process, whereby only a user with a valid Logon-ID and password which is recognized by the host computer will be allowed to sign on to the system.

b. Multiple Logons. Accessing RIS is done through a mainframe session manager. The Logon ID and password must be used each time a user signs on to it. The session manger limits users to one session at a time.

c. Changing Passwords. To preserve the integrity of the system, passwords will be changed periodically. Passwords should also be changed whenever there is a reason to believe that the password has been compromised. All passwords must be six to eight characters in length and are not case sensitive. Both alphabetical and numerical characters can be used.

OBTAINING ACCESS TO RIS

1-6. Procedures for Requesting Initial or Additional Access to the Readiness Information System. Standard procedures for requesting initial or increased access to RIS will expedite RIS access request processing and improve responsiveness. The access request is used to ensure users have a "need to know" and assists in maintaining system responsiveness and integrity. The following information is required for new RIS users, users requesting additional access or discontinuance of services:

a. Requesting Initial RIS Access for Your Command. Formal documentation must be initiated by the command requesting access to RIS with sufficient justification for the need and use of the system. All requests for initial or additional access to RIS must be forwarded to EPMAC Code 40ITB, via your respective Type Commander (TYCOM) and MCA, with their endorsements for approval. The request may include start of new service, change to existing service, or discontinuance of service. Upon approval or disapproval of your request, EPMAC will respond to you in an expeditious manner. Commanding officers and Officers-in-Charge are requested to certify in writing through a Remote Terminal Security Agreement (Refer to Figure 1-1), that their terminal area(s) will comply with the DON AIS Security Program, SECNAVINST 5239.3, and ensure the following security measures are implemented:

(1) Terminal and Microcomputer usage must be controlled. only authorized personnel are allowed to use the equipment. Each individual must use their own unique Logon ID and Password while accessing the RIS.

(2) A Terminal Area Security Officer and Alternate (TASO/ATASO) must be appointed in writing (Refer to Figures 1-2 and 1-3). Forward your designation letter with the Remote Terminal Security Agreement for the initial RIS access. Forward subsequent changes to the TASO and ATASO appointments to EPMAC Code 40ITB as they occur.

(3) All personnel are to be responsible for security awareness and to challenge any and all persons not assigned to the area.

(4) Microcomputers will not be left unattended while on-line to the host computer.

(5) If the general terminal area is to be unattended for an extended period of time it should be locked to prevent unauthorized use of the microcomputer.

(6) After normal working hours, the terminal area should be secured.

b. Procedures for Additional Access. Requests for access to additional RIS transactions that have not been previously approved will be sent to EPMAC via the appropriate MCAs for approval. EPMAC will notify the requesting activity of the MCAs, approval or disapproval.

c. User Account Assignment. The TASO/ATASO will submit a System Authorization Access (SAAR), DISA-41, for each individual requiring access to EPMAC's Information Security/Access Control Office (Code 40ITB). SAAR forms are available for download at <http://www.epmac.nola.navy.mil/aris/>. After approval, EPMAC will generate a unique individual access account for the user. The Logon ID and password will be mailed to the TASO. The TASO/ATASO will forward the Logon ID and password to the user in the same manner. In the event users cannot sign on for any reason, they will notify the TASO/ATASO, who will contact EPMAC to make the necessary adjustments.

d. Removal of User Accounts. When the user leaves the activity, or when the user is assigned duties that do not require access to the system, the TASO will submit a SAAR to EPMAC so that user account may be deleted.

ACCESSING RIS

1-7. Hardware/Software. A microcomputer with a Telnet connection with the Non classified Internet Protocol Routing Network (NIPRNET) is required to access the Active Readiness Information System (ARIS). Recommend the microcomputer be at least a 486DX with 16 MB RAM and Windows 3.1 or higher. No particular brand of microcomputer is necessary.

1-8. Session Manager. Access to ARIS is gained through a mainframe session manager called CL/Supersession. Specific instructions for using CL/Supersession can be found at <http://www.epmac.nola.navy.mil/aris/>.

Figure 1-1

**Sample Terminal Area Security Officer Appointment Memorandum**

**MEMORANDUM**

From: Commanding Officer, Name of Command To: Name of Appointee

Subj: APPOINTMENT OF PRIMARY ALTERNATE TERMINAL AREA SECURITY OFFICER (TASO/ATASO)

Ref: (a) SECNAVINST 5239.3

1. Per reference (a), you are appointed the Primary/Alternate Terminal Area Security Officer (TASO/ATASO) for the Active Readiness Information System (ARTS) microcomputers and associated peripheral devices located in Command Name office spaces.

2. Your responsibilities are listed in reference (a). As the ARTS TASOIATASO, your major responsibilities are to:

a. Monitor computer operations to prevent unauthorized browsing or manipulation of ARTS data.

b. Ensure that the computer(s) is/are signed off or locked when unattended or secured when not in use.

c. Brief each user on Information Systems Security (INFOSEC) requirements.

d. Maintain a current list of personnel authorized access to ARTS.

e. Review all System Authorization Access Request (SAAR) forms for completeness and forward to Enlisted Placement Management Center's (EPMAC) Information Systems Security Manager (ISSM).

f. Inform EPMAC's ISSM when users leave your command or no longer require access to ARTS.

g. Report all INFOSEC violations and abnormalities to EPMAC's ISSM.

h. Ensure that all users abide by all proprietary software/licensing agreements.

i. Provide assistance to EPMAC's TSSM, as required.

(Signature of Commanding officer or designated representative)

Figure 1-2

**Sample Terminal Area Security Officer Designation Letter**

From: Name of Command To: Commanding officer, Enlisted Placement  
Management Center(Code 40ITB)

Subj: TERMINAL AREA SECURITY OFFICER (TASO) AND ALTERNATE TERMINAL AREA  
SECURITY OFFICER (ATASO)

Ref: (a) SECNAVINST 5239.3  
(b) OPNAVINST 5239.1B

1. In accordance with references (a) and (b) the following individuals  
are appointed TASO and ATASO:

TASO Name:  
Code:  
E-Mail:  
Phone: DSN: Comm:  
ATASO Name:  
Code:  
E-Mail:  
Phone: DSN: Comm:

2. The TASO and ATASO are responsible for the following  
microcomputer(s) that access the Active Readiness Information System  
(ARIS):

Make/Model	Location	Bldg/Room
------------	----------	-----------

(Signature of Commanding Officer or Designated Representative)

Figure 1-3

**Sample Remote Terminal Security Agreement**

From: Name of Command  
To: Commanding officer, Enlisted Placement Management Center  
(Code 40ITB)

Subj: REMOTE TERMINAL SECURITY AGREEMENT

Ref: (a) SECNAVINST 5239.3  
(b) OPNAVINST 5239.1B

Encl: (1) Terminal Area Security Officer Designation Letter

1. I certify that the installation and management of the microcomputer(s) that access the Active Readiness Information System (ARIS) installed at this activity is/are in compliance with all provisions of references (a) and (b) and that the Information Systems Security (INFOSEC) requirements are implemented for accessing Enlisted Placement Management Center's (EPMAC) sensitive unclassified systems.

2. The designation letter for the Terminal Area Security Officer (TASO) and Alternate Terminal Area Security Officer (ATASO) is forwarded as enclosure (1). Any changes in the designations of the TASO and ATASO will be forwarded to EPMAC's Information Systems Security Manager (ISSM).

(Signature of Commanding Officer or designated representative)