



**DEPARTMENT OF THE NAVY**  
NAVY RECRUITING DISTRICT, NEW ORLEANS  
400 RUSSELL AVE BLDG 192  
NEW ORLEANS, LOUISIANA 70143-5077

NAVCRUITDISTNOLAINST 5239.3E

40

20 Feb 2015

NAVCRUITDISTRICT NEW ORLEANS INSTRUCTION 5239.3E

From: Commanding Officer, Navy Recruiting District New Orleans

Subj: NAVY RECRUITING DISTRICT INFORMATION SYSTEMS (IS)  
TRAINING PLAN

Ref: (a) DoDI 8500.01  
(b) SECNAVINST 5239.3B  
(c) OPNAVINST 5239.1C  
(d) COMNAVCRUITCOMINST 5239.1B  
(e) COMNAVCRUITCOMINST 1500.4R

Encl: (1) Training Schedule  
(2) Training Syllabus (NAVCRUIT Form 1500/2  
(Rev. 03-2012))

1. Purpose. To establish Navy Recruiting District New Orleans' Information System (IS) Training Plan.

2. Cancellation. NAVCRUITDISTINST 5239.3D.

3. Background. As delineated in references (a) through (d) and as directed by reference (e), each person reporting on board will receive formal IS security indoctrination from the command Systems Administrator (SYSAD), as well as follow-on quarterly IS security training and General Military Training (GMT) for the end users in the subject of Information Assurance Training.

4. Scope. This plan provides guidance for implementing a comprehensive automated IS security training program at NRD New Orleans.

5. Policy. The establishment of an effective, well defined IS Training Plan is part of the command's overall IS security awareness posture. All command personnel use computer resources. A thorough understanding of established security safeguards and individual user responsibilities will help protect sensitive data from loss, compromise, or inadvertent disclosure.

6. Procedures.

a. IS Security Training. All personnel must complete or have completed within the last year, cyber awareness training and PII awareness found on NKO. All personnel involved in the use of command IS system will receive IS security training per references (a) through (f). Individual IS security training will be conducted as outlined below.

(1) IS Security Indoctrination. Upon arrival each person will receive a formal IS security indoctrination from the command SYSAD. This will include: identification of key IS security personnel, explanation of each person's responsibility regarding the integrity of command computer systems, instruction in good user practices. Additionally, each person will be required to acknowledge their understanding of established IS security safeguards and will be authorized in writing to operate command IS computer systems.

(2) Quarterly IS Security Training. Quarterly computer security training will be conducted by the command SYSAD. This training will include a review of current information in Standard Operating Procedures, instructions and other sources relating to IS security. Special IS security training will focus on issues which relate directly to command mission and function.

(3) Information Assurance Training. IA Security training for the end users will be a quarterly GMT. This training will cover the following subjects:

(a) IS Security roles and responsibilities.

(b) IS Security organization and special terms.

(c) IS Security safeguards including Mode of Operation and Discretionary/Mandatory access controls.

(d) Specific information on user controls and identification of special countermeasures related to software, hardware, and network security, modem operation, the IS security accreditation process, and downgrading and declassification restrictions.

(e) Virus, prevention, detection, and recovery.

(f) IS security violation, investigation and reporting.

(g) Annual IA training. IA user training will be the latest version of Navy IA Security training available on NKO currently consisting of DoD Cyber Awareness Challenge and Privacy & Personally Identifiable Information (PII) training.

7. Training Documentation.

a. Enclosure (1) provides a schedule of minimum professional training and GMT subjects to be presented throughout the fiscal year. The SYSAD, will formulate and make available the designated training subject(s). Each DIVO/DLCPO/Department Head will ensure that all their personnel complete the required training.

b. Enclosure (2) of reference (e) shall be used to document this training. Certain training media produce a Certificate of Completion once the course is completed. The end user will print this certificate out and deliver the certificate to his/her DIVO/DLCPO/Department Head for entry into his/her training jacket.

/s/  
C. A. STOVER

Distribution List:  
Electronic only, via  
<http://www.cnrc.navy.mil/neworleans/>

**TRAINING SCHEDULE**

1 <sup>ST</sup> QTR		
<u>October</u>	<u>November</u>	<u>December</u>
General Security Awareness	Security Program Planning	Internet Browsing Safety
2 <sup>ND</sup> QTR		
<u>January</u>	<u>February</u>	<u>March</u>
Policies & Procedures	Change Control & Computer Abuse	Software Security
3 <sup>RD</sup> QTR		
<u>April</u>	<u>May</u>	<u>June</u>
Social Networking	Facilities Security	Phishing
4 <sup>TH</sup> QTR		
<u>July</u>	<u>August</u>	<u>September</u>
General Devise Problems and Solutions	Care of Computers, peripheral and equipment	PII & Cyber Awareness

NAVCRUITDISTINST 5239.3E  
20 Feb 2015

TRAINING SYLLABUS					
NAME:				RANK/RATE:	
TRAINING TYPE	TRAINING SUBJECT	DATE	INSTRUCTOR	HOURS	ENTRY BY

  

_____	_____
Trainee	Trainer

NAVCRUIT 1500/2 (Rev. 03-2012)

Enclosure (2)