



DEPARTMENT OF THE NAVY  
NAVY RECRUITING COMMAND  
5722 INTEGRITY DR.  
MILLINGTON, TN 38054-5057

COMNAVCRUITCOMINST 5239.4  
N6  
25 Aug 2011

COMNAVCRUITCOM INSTRUCTION 5239.4

From: Commander, Navy Recruiting Command

Subj: NAVY RECRUITING COMMAND MOBILE RECRUITER INITIATIVE  
POLICY

- Ref:
- (a) COMNAVCRUITCOMINST 5720.11, Releasing Navy Recruiting Command Records to Members of The Public Under The Freedom of Information Act (FOIA)
  - (b) ASN (RD&A) Memo, Department of the Navy Acquisition Policy on Mobile (Cellular) Phone and Data Equipment and Services, of 7 Mar 05
  - (c) DoD Directive 5500.7-R, Section 2-301(a), Use of Federal Government Resources - Communication Systems
  - (d) SECNAVINST 5720.44, Public Affairs Policy and Regulations
  - (e) OPNAVINST 5513.10, Department of the Navy List of Advanced Technology and Miscellaneous Program Guides
  - (f) SECNAV M-5239.1, Department of the Navy Information Assurance Program, Information Assurance Manual
  - (g) SECNAVINST 5200.35, Department of the Navy (DON) Management Control Program
  - (h) SECNAVINST 3850.4, Technical Surveillance Countermeasures (TSCM) Program
  - (i) COMNAVCRUITCOMINST 5211.4, Navy Recruiting Command Privacy Program
  - (j) COMNAVCRUITCOMINST 5239.1A, Navy Recruiting Command Information Assurance program
  - (k) COMNAVCRUITCOMINST 5239.3, Navy Recruiting Command Information Systems Acceptable Use Policy
  - (l) OPNAV5239/14, System Authorization Access Request - Navy (SAAR-N), Jul 2008
  - (m) NAVCIRT, Virus Report
  - (n) COMNAVCRUITCOMINST 5234.2wCH1, Information Technology Configuration Management Policy
  - (o) NMCI.31069.01.D+2.E, Report NMCI Missing, Lost, Stolen or Damaged Equipment Form, 4 June 2009
  - (p) Uniform Code of Military Justice, 64 Stat. 109, 10 U.S.C. Chapter 47 (UCMJ)
  - (q) Naval Network Warfare Command (NNWC), Computer Task Order 08-08 (Update 4)

25 Aug 2011

- (r) Secretary of the Navy (SECNAV), Department of the Navy Policy for Contact of Publicly Accessible World Wide Websites

Encl: (1) Releasable/Non-Releasable Information Using .com Networks  
(2) Definitions

1. Purpose. Set forth policy for acceptable use of mobile computing equipment, peripheral devices and Information Technology (IT) infrastructure instituted under the Mobile Recruiting Initiative (MRI). This instruction is intended to complement, reinforce, and/or strengthen the policies and procedures established under references (a) through (q).

2. Background. Production Recruiters are a mobile sales force. They are expected to devote in excess of fifty percent of their time in the field prospecting for new applicants and processing Future Sailors. This requirement drives a need for IT tools that are highly mobile with ubiquitous access to key Manpower, Personnel, Training and Education (MPT&E) Enterprise systems/networks. MRI is a Next Generation Network (NGEN) program specifically designed to satisfy Production Recruiters' distinct business requirements. The mobility afforded under MRI eliminates the need for physical connections to the Navy Marine Corps Intranet (NMCI) network. It provides Recruiters with tools to fully function in the commercial infrastructure (.com) environment.

### 3. Policy

a. MRI delivers unfettered and ubiquitous access to key business systems/networks. In doing so it creates renewed emphasis on physical and electronic security, Information Assurance, and ethical business practices. Improper use of MRI devices can compromise sensitive data, destroy hardware/software, and negatively impact the public trust in the organization. It is each user's obligation to adhere to strict security, Information Assurance, and ethical business practices as set forth in Ref (a) through (q) and other applicable laws, regulations, and policies. Navy Personnel, Department of Defense (DoD) employees, and contractor personnel working for the Navy are expected to uphold the highest standards of conduct. Personnel that violate these policies will be subject to Uniform Code of Military Justice (UCMJ) and other disciplinary action set forth by applicable laws, regulations, and policies.

25 Aug 2011

b. Careful consideration must be given to overall risk to personnel, information/data, infrastructure, equipment, and reputation when instituting new commercial technologies and best practices. MRI computing systems have undergone rigorous risk analysis and have been configured to DoD/DON guidelines. Commander, Naval Network Warfare Command (COMNAVNETWARCOM) granted an Interim Authority to Operate (IATO) to the program in August 2011 and expects to grant full Authority to Operate (ATO) no later than January 2012. Based on this authority, Navy Recruiting Command (NAVCRUITCOM) is authorized to operate MRI computers over commercial infrastructure. Users are not authorized to make any changes to the security baseline of MRI seats without the expressed written consent of the command's Information Assurance Manager.

c. NAVCRUITCOM, like many institutions with a presence in a .com environment, must address new security issues previously not applicable to Recruiters in the field. Operation in the .com environment exposes machines to real world security threats. Navy Recruiters, as a major component of the first line of security, must be more vigilant in this environment and knowledgeable of latest security policies and intrusion schemes by hackers.

d. MRI provides Production Recruiters the ability to perform business transactions using social media, commercial websites, and/or direct electronic communications with potential applicants. Recruiters are expected to adhere to the policies, acceptable use, license and user agreements set by the owners/governing body of the commercially provided communications channel. In events where commercial policy conflicts with DoD/DON policy and regulations, the DoD/DON policy/regulations will take precedence (unless otherwise directed by competent authority). MRI users are directed to contact Commanding Officers for guidance if/when commercial policies are deemed ambiguous. Users are directed to immediately report any/all violations of DoD/DON policies/procedures to Commanding Officers.

e. The .com environment demands moral discipline and ethical consideration due to the public nature of communication and computer networks. The nature of social networking and the culture of free flowing unstructured text where abbreviations, colloquialism and slang exists as a norm require increased diligence to adhere to high ethical standards in the public domain. Social network pages should be viewed as print media

because web pages may be copied, referenced and disseminated as examples of Navy communication in the public domain.

f. Interactions with groups and individuals may result in requests for information about the Navy. Except for recruiting-related information, requests for information concerning Navy component commands from organizations or private citizens shall be encouraged to use the process established in reference (a) and send their requests to the appropriate command.

g. Usage of web-based Navy Recruiting applications (e.g. Web RTools, CIRIMS, NASIS, PRIDE Mod, etc.) and social networking sites will result in the exchange of a variety of information across the Internet. Navy Recruiters will utilize DoD approved secure HTTPS/SSL communication methods while utilizing DoD or .com applications whenever PII data may be involved. Navy Recruiters shall collect personal information via DoD approved methods. Absolutely no medical information shall be associated with individuals; it is permissible, however, to address qualifying medical conditions as a part of program specifics. Navy Recruiters will allow Personal Identifiable Information (PII) data to be present on MRI computers only as long as necessary before transferring the data to the appropriate application. After transmission to the appropriate application, the Recruiter will immediately delete all PII data.

h. Military members shall protect their privacy information. Navy Recruiters, however, shall identify themselves by official name, rank, and phone number as appropriate during their conversation with potential applicants. Social networking aliases may be used in general conversation; however, Recruiters must identify themselves when discussing Navy-related programs.

i. Navy Recruiters shall never discuss ship and aircraft locations, force structures, casualty figures, past missions or results of operations. Intelligence sources can aggregate data from several Recruiters across websites and glean significant information concerning Navy units, their operations and reactions in support of future operations. Additional information is contained within enclosure (1).

j. The Internet is a powerful information tool for both internal and external use. As per reference (d), the Public Affairs Officers (PAO) is responsible for determining how social

25 Aug 2011

networks will be used and also monitoring their use along with any associated technological tools. The NAVCRUITCOM PAO shall create and maintain a clear process for establishing, reviewing and ensuring ongoing maintenance and accuracy of social networking sites and communications.

k. Some Navy Recruiters may find it appropriate to use music or videos on social network sites or during presentations given via MRI equipment. Navy Recruiters shall not place or reference information that violates copyright laws.

l. Factual statements shall be used in all communications. Navy Recruiters have a responsibility to keep informal communications factually accurate when discussing Navy programs. Social networks are print media and can be copied and passed to Navy and congressional leaders as complaints when potential applicants perceive false information.

m. No personal business shall be conducted via MRI equipment. Contacts generated on social networks shall not be used for a personal business venture, including data mining access for the purpose of selling contacts to marketing firms or individuals.

n. Navy Recruiters shall report attacks or perceived attacks on their social network sites or MRI devices via System Administrator (SYSAD), the NAVCRUITCOM help desk or via incident report per reference (m) on the NAVCRUITCOM Quarterdeck. Attacks against Navy social sites could be an indication of, or associated with, an organized attack targeted against the entire Navy Recruiting Command, the Navy, or the DoD information infrastructure. To identify and respond to such attacks, all Recruiters shall report detection of denial of service, information gathering or phishing schemes.

o. System administrators shall ensure computer firewalls, intrusion detection, Data Encryption at Rest (DAR) and virus software are configured and operational in accordance with DoD/DON Information Assurance Policy. To ensure protection against personal and network attacks, Navy Recruiters shall not alter the configuration of computer firewalls, intrusion detection, DAR and virus software. Navy Recruiters will be responsible for accepting and scheduling software patches and virus definitions in accordance with policies set by monitoring software installed on their MRI computers.

25 Aug 2011

p. All Recruiters shall provide the following upon receipt of MRI equipment: proof of completion of Privacy Act (PA)/PII training; a newly signed OPNAV SAAR-N form/user agreement (see reference (l)); proof of completion of ALCON 025/09 annual IA training; a completed and signed User Acceptance Checklist.

q. MRI devices shall never be connected to the NMCI or other DoD/DON networks via any Local Area Network (LAN) cable or Wireless Fidelity (WiFi) connection. If the MRI computer is plugged into a NMCI managed port, the port will be deactivated and a Move Add Change (MAC) request will be required to reactivate via the Information Assurance (IA) manager at NAVCRUITCOM Headquarters. This process may take up to two weeks to reactivate.

r. In accordance with annual Information Assurance (IA) training and Navy policy, the connection of flash media (e.g., memory cards, USB flash drives) to MRI equipment is prohibited until further notice per reference (q).

s. MRI computers are an NMCI/NGEN managed asset. However, NAVCRUITCOM will have client system administration rights. Therefore, the responsibility of the configuration baseline becomes a shared responsibility between NMCI/NGEN and NAVCRUITCOM. As a result, SYSADs are required to ensure the standardized device configuration as set forth by NMCI/NGEN and NAVCRUITCOM is maintained. All proposed changes to the baseline configuration (hardware or software) must follow NMCI/NGEN and NAVCRUITCOM configuration management policy and processes in accordance with reference (n).

t. The issuance of multiple portable pieces of equipment to be used in public and potentially unsecure locations increases the risk of missing, lost, stolen or damaged (MLSD) equipment. Commanding Officers will establish policy to indicate responsibility for MLSD equipment. The replacement of MLSD MRI computers will be accomplished via reference (o).

4. Oversight and Audit. Navy Recruiters need to be cognizant that the MRI is a government computer asset, and as such will be subject to monitoring by government agencies to include key stroke analysis, website visitation practices and security scans. An N7 inspection team and/or the CO/XO will perform spot checks quarterly (or as directed) on at least 25% of their MRI devices to ensure unauthorized sites are not being accessed, to ensure PII information is being deleted, and to ensure unauthorized data is not being captured or stored. All

25 Aug 2011

personnel must be diligent and alert to avoid lapses in discipline within the open and free conversational environment of the .com arena. Greater freedom requires increased vigilance and discipline to ensure we represent the Navy in a professional manner.

/s/

R. L. GRAF

Distribution:

Electronic only, via

<http://www.cnrc.navy.mil/Publications/directives.htm>