



UNITED STATES MARINE CORPS  
2D MARINE AIRCRAFT WING  
II MARINE EXPEDITIONARY FORCE  
POSTAL SERVICE CENTER BOX 8050  
CHERRY POINT, NC 28533-0050

WgO 5230.15B  
G-6  
JAN 10 2012

WING ORDER 5230.15B

From: Commanding General, 2d Marine Aircraft Wing  
To: Distribution List

Subj: INFORMATION SYSTEMS COORDINATOR (ISC) PROGRAM

Ref: (a) Systems Security Access Request (SAAR)  
(b) TM 4700-15-1H  
(c) MARADMIN 118/11  
(d) WgO 5230.13C  
(e) MARADMIN 162/00  
(f) IRM 5239-04

Encl: (1) Blank SAAR  
(2) Example ISC Appointment Letter  
(3) Blank Unit Garrison ADPE Inventory  
(4) 2d MAW ISC Manual

1. Situation. The current operational environment within 2d Marine Aircraft Wing (2d MAW) requires the ongoing support of established and future garrison Automated Data Processing Equipment (ADPE). Those assets include: desktop computers, laptop computers, multifunction devices, tablets, cellular phones, air cards and Blackberry devices. These ADPE assets need to be maintained in a high level of operational readiness and availability. To ensure this, every group and squadron within 2d MAW will maintain an ISC to ensure proper management of unit garrison network attached ADPE assets. This Order establishes guidelines and procedures for ISCs to maintain accountability for unit garrison network-attached ADPE assets, manage and maintain unit Blackberry Enterprise Services (BES) accounts and provide local and subordinate unit Navy Marine Corps Intranet (NMCI) support liaison.

2. Cancellation. WgO 5230.15A.

DISTRIBUTION STATEMENT A: Approved for public release;  
distribution is unlimited.

3. Mission. Establish guidelines for the formation of ISCs at the group and squadron level within 2d MAW and to define their roles and responsibilities.

4. Execution

a. Commander's Intent. With clear guidance and unambiguous policy, 2d MAW ISCs will manage ADPE assets for absolute accountability as well as to ensure that staff and commanders have the support required to successfully complete their missions.

b. Concept of Operations

(1) ISCs will be assigned in writing down to the Squadron level and will be responsible for implementing the directives established in this Order. Ultimately, unit commanders are responsible for accountability of garrison, network-attached ADPE assets.

(2) The roles and responsibilities of the ISC are separate from that of the unit S-6. All unit ISCs are report to the unit S-6 for coordination and direction.

c. Tasks

(1) Wing G-6 Information Systems Management Office (ISMO)

(a) Conduct ISC training to support the NMCI deployment and operational requirements.

(b) Ensure subordinate ISCs comply with this Order.

(2) Wing Staff Sections and Marine Wing Headquarters Squadron 2 (MWHS-2)

(a) Appoint an ISC in writing and provide a copy of the appointment letter to the Wing G-6.

(b) Ensure the ISC attends training as required.

(c) Ensure ISC conducts routine inventories and provides results to Wing G-6 ISMO In Accordance With (IAW) enclosure (3).

JAN 10 2012

(3) Group S-6

(a) Appoint an ISC in writing and provide a copy of the appointment letter to the Wing G-6.

(b) Scan and upload the ISC appointment letters to the G-6 ISMO SharePoint at the following location: <https://intranet.2dmaw.usmc.mil/G6/ismo/ISC%20Letter%20Repository/Forms/AllItems.aspx>. The file name will be in the following format: Unit (No Dashes) Last Name Rank FIMI.pdf (i.e. Marine Wing Support Squadron 274 (MWSS-274) Smith Cpl IM.pdf). Contact G-6 ISMO if you are unable to upload to that location.

(c) Ensure the ISC attends training as required.

(d) Ensure ISC conducts routine inventories and provides results to Wing G-6 ISMO IAW enclosure (3).

(e) Consolidate and forward all squadron inventories to Wing G-6 ISMO IAW enclosure (3).

c. Coordinating Instructions

(1) The Wing G-6 ISMO will act as the central point of contact for all Wing Staff ISC and Information Technology/Information Assurance (IT/IA) related issues.

(2) Any recommended changes to this Order and Manual should be submitted to the 2d MAW G-6 ISMO via the appropriate chain of command.

(3) In order to ensure stability and maintain continuity, ISCs should be selected on their ability to perform the ISC duties for a minimum of one year.

(4) There is no prescribed rank for an ISC; however, due to the importance of the position and the level of responsibility, it is recommended that units appoint a sergeant or above.

5. Administration and Logistics. The point of contact for this Order is the 2d MAW G-6 ISMO at DSN: 582-7072/3551, Commercial: (252) 466-7072/3551.

6. Command and Signal

- a. Command. This Order is applicable to all 2d MAW units.
- b. Signal. This Order is effective the date signed.

  
R. W. REGAN  
Chief of Staff

DISTRIBUTION: A

## SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

### PRIVACY ACT STATEMENT

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.  
**PRINCIPAL PURPOSE:** To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.  
**ROUTINE USES:** None.  
**DISCLOSURE:** Disclosure of this Information is voluntary; however, failure to provide the requested Information may impede, delay or prevent further processing of this request.

<b>TYPE OF REQUEST</b> <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID _____	<b>DATE (YYYYMMDD)</b> _____
---	---------------------------------

<b>SYSTEM NAME (Platform or Applications)</b> _____	<b>LOCATION (Physical Location of System)</b> _____
--	--

**PART I (To be completed by Requestor)**

1. NAME (Last, First, Middle Initial)	2. ORGANIZATION
3. OFFICE SYMBOL/DEPARTMENT	4. PHONE (DSN or Commercial)
5. OFFICIAL E-MAIL ADDRESS	6. JOB TITLE AND GRADE/RANK
7. OFFICIAL MAILING ADDRESS	8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR	
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training.    DATE (YYYYMMDD) _____	
11. USER SIGNATURE	12. DATE (YYYYMMDD)

**PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)**

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:  
 AUTHORIZED     PRIVILEGED

15. USER REQUIRES ACCESS TO:     UNCLASSIFIED     CLASSIFIED (Specify category)  
 OTHER \_\_\_\_\_

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input type="checkbox"/>	16a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.) _____
---	---

17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)
------------------------------------	----------------------------	---------------------

20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
--	----------------------------------	-------------------

21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)
--	-------------------	----------------------

22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)
-----------------------------------	-----------------------------	------------------	---------------------

26. NAME (Last, First, Middle Initial)

27. OPTIONAL INFORMATION (Additional Information)

By signing block 11 I agree to the following rules of behavior:

- I understand that I am providing both implied and expressed consent to allow authorized authorities, to include law enforcement personnel, access to my files and e-mails which reside or were created on Government IT resources.
- I will not conduct any personal use that could intentionally cause congestion, delay, or disruption of service to any Marine Corps system or equipment.
- I will not install or use any Instant Messaging client or peer-to-peer file sharing application, except that which has been installed and configured to perform an authorized and official function.
- I will not use Marine Corps IT systems as a staging ground or platform to gain unauthorized access to other systems.
- I will not create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the subject matter.
- I will not use Government IT Resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- I will not use Government IT resources for personal or commercial gain without commander approval. These activities include solicitation of business services or sale of personal property.
- I will not create, download, view, store, copy, or transmit materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited such as transmitting sexually explicit or sexually oriented materials.
- I will not use Marine Corps IT systems to engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity.
- I will not post Marine Corps information to external newsgroups, bulletin boards or other public forums without proper authorization. This includes any use that could create the perception that the communication was made in ones official capacity as a Marine Corps member, unless appropriate approval has been obtained or uses at odds with the Marine Corps mission or positions.
- I will not use Marine Corps IT resources for the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.
- I will not modify or attempt to disable any anti-virus program running on a Marine Corps IT system without proper authority.
- I will not connect any personally owned computer or computing system to a DoD network without prior proper written approval.

**PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION**

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION (YYYYMMDD)	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III	
29. VERIFIED BY (Print name)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (YYYYMMDD)

**PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION**

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (YYYYMMDD)	PROCESSED BY (Print name and sign)	DATE (YYYYMMDD)
DATE REVALIDATED (YYYYMMDD)	REVALIDATED BY (Print name and sign)	DATE (YYYYMMDD)

DD2875 ADDENDUM  
STANDARD MANDATORY NOTICE AND CONSENT PROVISION  
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

- You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

- You consent to the following conditions:

- o The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- o At any time, the U.S. Government may inspect and seize data stored on this information system.

- o Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

- o This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.

- o Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and

User Initials: \_\_\_\_\_

data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

o In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

o All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

User Initials: \_\_\_\_\_

## INSTRUCTIONS

The prescribing document is as issued by using DoD Component.

**A. PART I:** The following information is provided by the user when establishing or modifying their USER ID.

- (1) Name. The last name, first name, and middle initial of the user.
- (2) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
- (3) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).
- (4) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.
- (5) Official E-mail Address. The user's official e-mail address.
- (6) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.
- (7) Official Mailing Address. The user's official mailing address.
- (8) Citizenship (US, Foreign National, or Other).
- (9) Designation of Person (Military, Civilian, Contractor).
- (10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.
- (11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).
- (12) Date. The date that the user signs the form.

**B. PART II:** The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

- (13) Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.
- (14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)
- (15) User Requires Access To: Place an "X" in the appropriate box. Specify category.
- (16) Verification of Need to Know. To verify that the user requires access as requested.
- (16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.
- (17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.
- (18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.
- (19) Date. Date supervisor signs the form.
- (20) Supervisor's Organization/Department. Supervisor's organization and department.
- (20a) E-mail Address. Supervisor's e-mail address.
- (20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form 2875.

(22) Signature of Information Assurance Officer (IAO) or Appointee. Signature of the IAO or Appointee of the office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form 2875.

(27) Optional Information. This item is intended to add additional information, as required.

**C. PART III:** Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Date of Investigation. Date of last investigation.

(28b) Clearance Level. The user's current security clearance level (Secret or Top Secret).

(28c) IT Level Designation. The user's IT designation (Level I, Level II, or Level III).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number. The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature. The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date. The date that the form was signed by the Security Manager or his/her representative.

**D. PART IV:** This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

### E. DISPOSITION OF FORM:

**TRANSMISSION:** Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

**FILING:** Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.



Unit Letter Head

IN REPLY REFER TO:  
5230  
Unit  
Date

From: Commanding Officer, <unit>  
To: <Rank> <FirstName> <MI> <LastName> <Last4/MOS> USMC  
Subj: APPOINTMENT AS INFORMATION SYSTEMS COORDINATOR (ISC) FOR  
<UNIT>  
Ref: (a) WgO 5230.15B

1. In accordance with the reference, you are hereby appointed as the Information Systems Coordinator for <unit>.
2. You are to familiarize yourself with the reference and will be guided by it in the performance of your duties.
3. Your appointment will remain in effect until written authority, notification, transferred, reassigned or this appointment is superseded.
4. This authority supersedes all previous authorizations.

I. M. COMMANDER

---

Unit  
Date

FIRST ENDORSEMENT

From: <Rank> <FirstName> <MI> <LastName> <Last4/MOS> USMC  
TO: Commanding Officer, <unit>

1. I have read and understand the reference and hereby assume the duties as the ISC for <unit>.

I.M. MARINE

Copy to:  
Commanding Officer, <Unit>  
<Group>, S-6

Enclosure (2)



WgO 5230.15B

JAN 10 2012

**2d Marine Aircraft Wing  
Information Systems Coordinator Manual  
10 November 2011**

Enclosure (4)

**Table of Contents**

Purpose	3
Command Liaison/General Administration	4
Desktop Support	5
Maintenance Administration	5
Prohibited Actions	5
Violation Reporting	6

**Purpose**

1. The purpose of this document is to enable Information Systems Coordinators (ISC) to effectively operate within their unit and understand their roles and responsibilities.
2. This Manual is intended to be a living document and is subject to review and modification. Recommendations for modification should be addressed to the 2d MAW ISMO Section at (252/DSN 582) 466-7072.

1. Command Liaison/General Administration

a. Attend ISC Training provided by 2d MAW G-6 Information Systems Management Office (ISMO) garrison operational support.

b. Act as the unit's single point of contact for all Information Technology (IT) issues. Advise the Commanding Officer (CO), Division Head or Officer in Charge (OIC) on matters pertaining to IT.

c. Respond to all IT related data calls as tasked by higher headquarters.

d. Adhere to an administrative reporting chain through the unit S-6s within the unit (i.e. Section ISC will coordinate actions through Squadron S-6 and Squadron S-6 through Group S-6, etc.). This ensures all levels of responsibility maintain cognizance.

e. Plan, prioritize and coordinate IT support and future requirements (to include hardware and software procurement, Secret Internet Protocol Router Network (SIPRNET), deployment support requirements, etc.). Coordinate with the unit Chain of Command, Squadron, Group S-6 and the 2d MAW G-6 ISMO.

f. Ensure dissemination and compliance of information and directives pertaining to IT.

g. Ensure new unit personnel fill out a SAAR form to enable the transferring of the account to the proper NMCI unit code. Direct the personnel to submit their form to the TISD Helpdesk.

h. Coordinate with Group S-6s and G-6 ISMO to ensure users are placed in appropriate unit distribution lists and have appropriate permissions to access the section, unit or group shared drive(s).

i. When a Marine departs from a unit, the local ISC or S-6 representative will have the Marine removed from the distribution lists and have his permissions revoked from the appropriate shared drive(s) and SharePoint site(s).

j. Direct all personnel departing the command or separating from service to check out with the Station TISD. Inform departing personnel that are joining commands outside of 2d MAW that they must transfer their account to the new command upon arrival.

k. Maintain a current inventory of all Automatic Data Processing Equipment (ADPE) assets (NMCI or government equipment) and applications in use at your command for data call purposes utilizing the blank form included as enclosure (3).

l. Assist the unit S-6 in reviewing the weekly G-6 ISMO shared drive report to ensure proper management of unit space allocation and usage. This report is located at <https://intranet.2dmaw.usmc.mil/G6/ismo/Resource%20Center/Forms/AllItems.aspx>.

m. Assist the unit S-6 in conducting quarterly updates of all unit distribution lists to ensure accuracy of personnel. This should be in conjunction with the NMCI active user account inactivity report.

## 2. Desktop Support

a. Provide local application expertise to personnel within the unit.

b. Refer hardware and software problems to the NMCI Helpdesk.

c. Track all ticket numbers given by the Helpdesk for problem resolution.

d. Refer problems not solved in a timely manner (up to 2 weeks per current service level agreements) through the S-6 chain to the G-6 ISMO - with the appropriate ticket number(s).

## 3. Maintenance Administration

a. Provide local and subordinate NMCI liaison for all garrison network attached ADPE assets.

b. Perform the appropriate level of preventive maintenance for all ADPE assets within the unit.

c. Maintain maintenance record jackets per reference (b) for unit garrison network attached ADPE assets.

4. Prohibited Actions. ISCs will not perform and will ensure that none of the users for whom they are responsible, perform any of the following:

JAN 10 2012

- a. Change, modify or tamper with user accounts and passwords.
- b. Change or tamper with local administrator passwords.
- c. Add additional passwords to any of the computer systems.
- d. Tamper or change any system files (CMOS, BIOS, etc.).
- e. Tamper with Central Processing Unit (CPU) cases (this constitutes improper maintenance and is a chargeable offense).
- f. Manipulate, move, power off or unplug any of the higher network configuration hardware (including lines, hubs and switches).
- g. Per the reference (d), no unauthorized software will be loaded onto any government computer system. If unauthorized software is found on an NMCI or government computer system, the ISC will report the violation through the S-6 chain to the G-6 Cyber Security section.

5. Violation Reporting. Inappropriate use of government owned computer resources is prohibited, per reference (e). ISCs will immediately report violations (inappropriate surfing, chain mail, etc.) through the S-6 chain to the G-6 Cyber Security section.