



UNITED STATES MARINE CORPS
MARINE AIR GROUND TASK FORCE TRAINING COMMAND
MARINE CORPS AIR GROUND COMBAT CENTER
BOX 788100
TWENTYNINE PALMS, CALIFORNIA 92278-8100

CCO 5230.3A

6

OCT 04 2011

COMBAT CENTER ORDER 5230.3A

From: Commanding General
To: Distribution List

Subj: ESTABLISHING AND MAINTAINING SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) COMPUTER NETWORK CONNECTIVITY ABOARD THE MARINE AIR GROUND TASK FORCE TRAINING COMMAND (MAGTFTC), MARINE CORPS AIR GROUND COMBAT CENTER (MCAGCC)

Ref: (a) MCAGCC SIPRNET Authority to Operate (ATO)/Authority to Connect (ATC) (NOTAL)
(b) SECNAV M-5510.36
(c) CCO 5532.1
(d) MARADMIN 590/05
(e) <http://www.marines.mil/unit/29palms/G6/Pages/default.aspx>, Sample Standard Operating Procedures for SIPRNET

1. Situation. The Combat Center's SIPRNET system infrastructure is constantly subjected and endangered by external and internal information technology threats. The references provide Department of Defense, Department of the Navy, and Marine Corps directives, policies, and security measures to operate, maintain, and protect SIPRNET equipment and information against illegal or accidental modification, destruction, disclosure, or denial of service.

2. Cancellation. CCO 5230.3.

3. Mission. Promulgate policy, procedures, and responsibility for commanding officers and directors to establish, maintain, operate, and govern user accessibility to the Combat Center SIPRNET.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All established SIPRNET seats, system administrators, and personnel granted access to the MCAGCC SIPRNET domain will strictly adhere to the policies and procedures set forth in this Order. Failure to do so may create a breach of national security and result in punitive measures.

(2) Concept of Operations. The Combat Center SIPRNET domain is defined as the classified computer network, administered by the MAGTFTC, MCAGCC Assistant Chief of Staff G-6 (AC/S), Communication and Information Systems for communication up to "SECRET" classified information via the Marine Corps Enterprise Network (MCEN).

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

b. Subordinate Element Missions

(1) Chief of Staff. Approve or disapprove restricted area requests.

(2) Assistant Chief of Staff G-6, Communication and Information Systems

(a) Provide contract oversight, customer technical representation, and onsite operational liaison with the Navy Marine Corps Internet (NMCI) SIPRNET contractor aboard the Combat Center.

(b) Identify SIPRNET domain resource requirements for annual budgets and ensure resources are in compliance with higher headquarters directives and policies.

(c) Information Assurance Manager

1. Provide assistance completing the sample standard operating procedures (SOP), reference (e).

2. Coordinate issuance of the ATO and ATC with the designated approving authority when all requirements are met.

(3) Designated Approving Authority

(a) Provide staff cognizance of the MCEN SIPRNET domain, seat certification, and accreditation for all organizations utilizing the Combat Center SIPRNET domain.

(b) Review all SIPRNET seat requests for compliance with component directives and policies.

(c) Maintain all required MCEN SIPRNET domain and seat accreditation documentation for active seats.

(d) Designate the information assurance manager (IAM), certification authority, and all component information assurance officers associated with the MCEN SIPRNET domain in writing.

(4) Unit Security Manager

(a) Ensure all SIPRNET seat requests meet the designated space vault, secure room, or SIPRNET work area requirements per exhibit 10A of reference (b).

(b) Certify SIPRNET work areas. The MAGTFTC security manager will certify MAGTFTC directorate work spaces and the unit security managers will certify respective unit SIPRNET work areas. The spaces cannot be certified until the following documentation is received by the unit security manager:

1. A copy of the Chief of Staff's letter designating the space as a restricted area.

2. Physical Security Survey. Grant or deny waivers as warranted, for deficiencies cited in the physical security survey.

3. SIPRNET SOP. A sample of the SIPRNET SOP is located on the G-6 website, reference (e), and must:

- a. Be signed by the commanding officer or director.
- b. Identify written procedures specifying tasks assigned to specific billet(s) to safeguard classified information, information processing system, and the KG-175.
- c. Provide access control procedures based on a "need to know" basis.
- d. Contain procedures for periodic inspections.
- e. Contain procedures to utilize removable secondary storage media devices per reference (d).
- f. Provide procedures to control security container combinations.
- g. Provide emergency plans with a recall roster, procedures for fire, natural disaster, and emergency removal and destruction of classified material.

(c) Revoke certification letter for security violation(s).

(d) Provide initial and annual access briefings, North Atlantic Treaty Organization (NATO) Secret briefings, maintain command access rosters to record briefings, sign SIPRNET system authorization access requests, and SIPRNET end user agreements.

(5) Assistant Chief of Staff G-7, Mission Assurance

(a) Conduct physical security surveys when requested per reference (c).

(b) Forward the completed physical security survey with cited deficiencies to requestor and a copy to the unit security manager and IAM.

c. Coordinating Instructions

(1) Reference (a) delineates the components and boundaries of the Combat Center SIPRNET.

(2) A computer or other information technology system assigned an internet protocol address that is connected to the Combat Center SIPRNET is defined as a "seat".

(3) As used in this Order, unless specifically stated otherwise, the term security manager refers to the security manager of the requesting unit or the MAGTFTC security manager for MAGTFTC directorates, hereafter collectively referred to as unit security manager.

(4) As used in this Order, unless specifically stated otherwise, the term information assurance manager refers to the MAGTFTC IAM.

(5) Three independent, but related approvals must be obtained to establish a SIPRNET seat aboard the Combat Center.

(a) The seat must be approved and funded by the NMCI contract process. Funding and approval for NMCI SIPRNET seats is controlled and budgeted each fiscal year by the Marine Corps major subordinate commands.

(b) The unit security manager must certify the space in which a SIPRNET seat(s) will be fielded as a vault, secure room, or SIPRNET work area per exhibit 10A of reference (b).

(c) The MCEN must grant ATO the SIPRNET seat and ATC to the Combat Center SIPRNET domain.

(6) Procedures to Obtain Approval for a SIPRNET Seat

(a) Obtain NMCI Seat Approval. The unit or directorate ensures the funding and valid NMCI order for the requested SIPRNET seat is available by having their information system coordinator contact the Customer Technical Representative to initiate a SIPRNET seat order.

(b) Restricted Area Request. The commanding officer or director forwards a written request to the Chief of Staff (COS) to have a specified space, e.g. vault or secure room, be designated as a level two or three restricted area per reference (c) for the purpose of hosting a SIPRNET seat(s).

(c) Physical Security Survey Approval

1. The unit or directorate forwards a letter to the Provost Marshal, Attention: Physical Security Chief requesting a physical security survey. A restricted area designation letter approved by the COS will be included in the request as an enclosure.

2. The physical security chief returns the completed physical security survey to the appropriate unit or directorate and forwards a copy to the unit security manager and IAM.

3. Physical Security Deficiencies. The SIPRNET approval process will not proceed until deficiencies stated in the physical security survey are rectified or a waiver is granted by the unit security manager.

a. Cited Building Deficiencies. The unit or directorate is responsible for initiating work requests to the AC/S G-4, Installation and Logistics, public works division to have cited facility deficiencies corrected.

b. If the deficiencies are minor and projected to be rectified within six months, the unit or directorate may submit a program objectives and milestones (PO&AM) to the designated approving authority (DAA) and unit security manager outlining how and when the deficiencies will be rectified.

(d) Designating the Requested SIPRNET Space as a Vault, Secure Room, or SIPRNET Work Area

1. The unit security manager is responsible for certifying the requested SIPRNET space as a vault, secure room, or SIPRNET work area per

exhibit 10A of reference (b). SIPRNET hardware cannot be installed in the space until it is certified. (A SIPRNET work area is defined as a room with a SIPRNET approved information processing system or protection distribution system outlet.)

2. Prior to certifying a space, the unit security manager must receive a copy of the COS's letter designating the space as a restricted area, the requesters SIPRNET SOP signed by their commanding officer or director, and a completed physical security survey.

(e) Authority to Operate and Authority to Connect

1. When all physical security deficiencies are rectified or granted a waiver, the unit or directorate will complete the SOP, reference (e). The IAM and unit security manager will provide assistance completing the SOP.

2. When the SOP is completed, the unit or directorate will contact the IAM to schedule a SIPRNET seat fielding walk through. The unit security manager, IAM, and NMCI contractor information assurance personnel will conduct a SIPRNET seating field walk through jointly, to ensure all requirements have been met to obtain final approval by the DAA.

a. The IAM will coordinate issuance of the ATO and ATC with the DAA when all requirements are met.

b. If physical security deficiencies still exist, the DAA may issue an interim authority to operate (IATO), for a period not to exceed six months providing a PO&AM was submitted and the unit security manager determines the physical security deficiencies pose an "acceptable risk." The DAA may only issue an IATO if it is determined the physical security deficiencies pose an "acceptable risk." When the DAA determines there is an "acceptable risk" to operate a SIPRNET seat and all security deficiencies are rectified or issued a permanent waiver, the DAA will issue the ATO and ATC.

(1) The SIPRNET ATO and ATC will be valid for a period of three years unless the SIPRNET seat installation or operation changes, which will revoke the DAAs ATO and ATC.

(2) The unit security manager can revoke the certification letter at any time for a security violation.

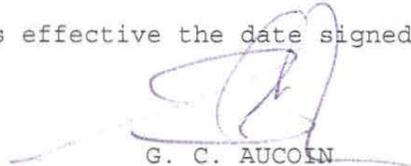
(f) Obtaining and Retaining SIPRNET Access. To obtain and retain SIPRNET access, all SIPRNET users must complete the on-line annual information assurance training and submit appendices G and H of the SOP, reference (e), annually to the AC/S G-6, legacy applications office. Unit security managers are responsible for the initial and annual access briefings, NATO Secret briefings, signing appendices G and H of the SOP, and maintaining command access rosters to record the briefings.

5. Administration and Logistics. Distribution statement A directives issued by the Commanding General are distributed via e-mail upon request and can be viewed at <http://www.29palms.usmc.mil/dirs/manpower/adj/ccotoc.asp>.

6. Command and Signal

a. Command. This Order is applicable to all Combat Center personnel, and organizations requesting and granted access to the Combat Center SIPRNET domain.

b. Signal. This Order is effective the date signed.



G. C. AUCOIN
Chief of Staff