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

CCO 5230.3F
14A
MAR 28 2019

COMBAT CENTER ORDER 5230.3F

From: Commanding General
To: Distribution List

Subj: ESTABLISHING AND MAINTAINING SECRET INTERNET PROTOCOL ROUTER NETWORK COMPUTER NETWORK CONNECTIVITY ABOARD THE COMBAT CENTER

Ref: (a) DoDM 5200.01 Volumes 1-4, "DoD Information Security Program", February 24, 2012
(b) DoD Instruction 8500.1, "Cybersecurity"' March 14, 2014
(c) SECNAV M-5510.36
(d) MCO 5530.14A
(e) MARADMIN 330/16
(f) MARADMIN 590/05
(g) CCO 5532.1E
(h) 29 Palms SIPRNET Authority to Operate (ATO)/Authority to Connect (ATC)

Encl: (1) New SIPRNET Letter Template
(2) SIPRNET Change Request
(3) Flowchart

1. Situation. The Marine Air Ground Task Force Training Command (MAGTFTC), Marine Corps Air Ground Combat Center (MCAGCC) Marine Corps Enterprise Network Secret Internet Protocol Router Network (MCEN-S) system infrastructure is persistently subjected to and threatened by external and internal information technology threats. The references provide guidance and policies on the security measures needed to operate, maintain, and protect MCEN-S equipment and data. Those measures protect against illicit or accidental modification, destruction, disclosure, or denial of service. They further outline the requirements on the handling, storing, labeling, and classification of that data, to include physical and electronic types and their respective containers.

2. Cancellation. CCO 5230.3E.

3. Mission. Establish procedures and responsibility for Commanding Officers (CO), Assistant Chiefs of Staff (ACs/S), Special Staff Officers, and appointed personnel to establish, maintain, operate, and govern user accessibility to the MAGTFTC, MCAGCC MCEN-S.

4. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. All established MCEN-S seats, system administrators, and personnel granted access to the MAGTFTC, MCAGCC

DISTRIBUTION STATEMENT B: Distribution authorized only for MAGTFTC, MCAGCC directorates, special staff sections, and operational forces.

MCEN-S domain will strictly adhere to the procedures set forth in this Order. Failure to do so may create a breach of national security which may result in punitive measures.

(2) Concept of Operations. The MAGTFTC, MCAGCC MCEN-S domain is defined as the classified computer network, administered by the MAGTFTC, MCAGCC AC/S Communications Directorate (CD), for communications of classified information up to "SECRET" via the MCEN. All connections must be obtained and maintained per this Order.

b. Subordinate Element Missions

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

(2) AC/S CD

(a) Review and evaluate customer requests and documentation for ATC.

(b) Provide connectivity for approved Secret Internet Protocol Router Network (SIPRNET) locations.

(c) Provide Tactical Local Area Network Encryption (TACLANE) for circuit encryption.

(d) Provide switch for circuit networking.

(e) SIPRNET Program Manager (PM)

1. Provide Requesting entity with a sample SIPRNET standard operating procedures (SOP) specific to the system, to assist them in processing their MCEN-S connection request.

2. Provide Requesting entity initial Change Request feasibility determination.

3. Ensure the Connection Approval Process is successful.

a. Assign Internet Protocol (IP) addresses to the unit.

b. Ensure a physical network connection to the unit exists.

4. Maintain an appropriate security posture for the mission at hand.

5. Maintain all required MCEN-S domain and seat accreditation documentation for active seats.

6. Maintain a MCEN-S ATO/ATC.

7. Network Diagram. With information provided by the requesting unit, the network diagram must identify all hardware information (make, model, hostname, and IP address) of all devices that are requesting connection to the network.

(f) Information Systems Security Manager (ISSM)

1. Provide oversight of the MCEN-S domain assessment and authorization (A&A) for all organizations utilizing the MAGTFTC, MCAGCC MCEN-S domain.

2. Review all MCEN-S seat requests for compliance with directives and policies.

3. Review all required MCEN-S A&A documentation.

4. Ensure SIPRNET assets are scanned for vulnerabilities to ensure that all Security Technical Implementation Guides and software patches are applied and updated.

5. Ensure that the Host Based Security System is loaded and configured on each server and workstation, including Programs of Record (POR) to detect malicious computer-related activities.

6. Sign as the Information Assurance Officer on the SIPRNET System Authorization Access Requests (SAARs).

(3) Requesting Unit CO or designated representative

(a) CO Request. If this is a new classified area without an existing MCEN-S connection, then a letter, from the CO to the AC/S CD shall be attached; see enclosure (1). The letter can be downloaded from the unit Information Systems Coordinator (ISC) folder located on the MCAGCC Shared drive at \\mcuspndlfs43\MCAGCC\Communications Directorate\Shared\ISC Support.

(b) SIPRNET Change Request. Complete the SIPRNET Change Request, enclosure (2), and attach and submit through the Remedy process via the unit, along with the following documentation:

1. SIPRNET SOP. Develop an SOP that identifies physical security, information security, personnel security, and communications security procedures that shall be signed by the Commanding Officer or Director. The AC/S CD SIPRNET PM will provide a sample SOP. The SOP shall include but is not limited to the following procedures:

a. Tasks assigned to billets to safeguard classified information, information processing systems, and the authorized encryption device.

b. Access control based on "need-to-know".

c. Periodic inspections.

d. Utilization of removable secondary storage media and devices.

e. Control of security container combinations.

f. Emergency removal and destruction of classified material.

2. Designation Letter. A classified area designation letter must be signed by the Security Manager.

(c) Supply Change Request. If a new MCEN-S workstation is required, then the process must go thru the unit supply chain. Other equipment that will be connected to the MCEN-S (i.e.; video telecommunications conference, printer, IP phone) must be processed thru the unit supply chain.

(d) TACLANE. Units should coordinate with the AC/S CD for the procurement of the TACLANE device to connect to the MCEN-S.

(e) POR. In order to connect POR's to the MCEN-S, a current (ATO/ATC) for the POR would be required. Administrative access will be given to each of the POR devices for a Communications Directorate SIPR System Administrator. The process for connecting a POR begins with generating a request thru the Remedy system via the unit ISC. In the event that the POR's ATO lapses, the systems will be disconnected from the network.

(f) Unit Security Manager

1. Validate classified information storage areas by ensuring the SIPRNET requests meet the designated space requirements as a vault, Secure Room (SR), Controlled Access Area (CAA), Restricted Access Area (RAA), or limited Controlled Area (LCA), per references (a) through (d).

2. Create and maintain classified area designation letters and, as required, revoke designations for security violation(s), or when the area is no longer needed.

3. As required, request waivers, as warranted, for deficiencies cited in the physical security survey conducted by the Provost Marshal Office (PMO).

4. Provide initial and annual access briefs, North Atlantic Treaty Organization (NATO) secret briefings, and maintain command access rosters to recorded briefings.

5. Complete and sign Part III of the SIPRNET SAARs.

6. Provide assistance in completing the unit MCEN-S SOP.

7. Maintain copies of users Derivative Classification Training course certificates.

(4) PMO

(a) Conduct physical security surveys, as required, for open Secret storage areas, per references (a), (b), and (c).

(b) Forward the completed physical security survey with cited deficiencies to the requestor and a copy to the unit Security Manager, the Combat Center Security Manager, and the Installation ISSM.

c. Coordinating Instructions

(1) Refer to the flowchart and checklist in enclosures (2) and (3) for the required steps to establish MCEN-S connectivity.

(2) Requirements for Maintaining MCEN-S Services

(a) To retain MCEN-S access, all MCEN-S users shall annually complete the online Cyber Awareness Training on MarineNet or Total Workforce Management System, depending on their status, per reference (e), and complete the Derivative Classification Course as required biennially.

(b) Unit Security Managers are responsible for the initial and annual access briefings, NATO Secret briefings, signing the SAAR, and maintaining command access rosters to record the briefings.

(c) All MCEN-S assets shall be connected to the MCEN-S domain every Monday, Wednesday and Friday, for a minimum of six continuous hours, between the operating hours of 0730-1630, or as directed by the CD. This is to ensure systems receive required updates and system scans. This is a mandatory requirement. Failure to comply with this requirement shall result in the disabling of the MCEN-S connection.

(d) The Requesting Unit is required to keep all POR systems updated to the most current version for the system.

5. Administration and Logistics

a. Directives issued by this Headquarters are published and distributed electronically. Electronic versions of Combat Center directives can be found at https://www.29palms.marines.mil/Staff-Offices/Adjutant-Office/Orders/.

b. Forms. Enclosure (2) is form CC 2620/1 SIPRNET Change Request. This form can be obtained from the Forms Online website at https://forms.documentservices.dla.mil/order/. Enter the form number on the "Search Criteria" box and select "Form Number" from the "Title" drop down box and click on the "Search" button. The forms can also be accessed by the unit ISC thru the MCAGCC shared drive at \\mcuspndlfs43\MCAGCC\Communications Directorate\Shared\ISC Support. All previous editions of the form are obsolete and will not be accepted.

6. Command and Signal

a. Command. This order is applicable to all Combat Center personnel and organizations requesting access to the MAGTFTC, MCAGCC MCEN-S domain.

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

R. MARTINEZ
Chief of Staff

DISTRIBUTION: B

New SIPRNET Letter Template

UNITED STATES MARINE CORPS
Unit Name
BOX 78____
TWENTYNINE PALMS, CALIFORNIA 92278-____

5230
Unit Code
DD Mmm YY

From: Commanding Officer
To: Assistant Chief of Staff, Communications Directorate
Via: Communications Directorate Service Desk

Subj: REQUEST NEW MARINE CORPS ENTERPRISE NETWORK-SECRET INTERNET PROTOCOL ROUTER NETWORK (MCEN-S) CONNECTION

Ref: (a) CCO 5230.3F

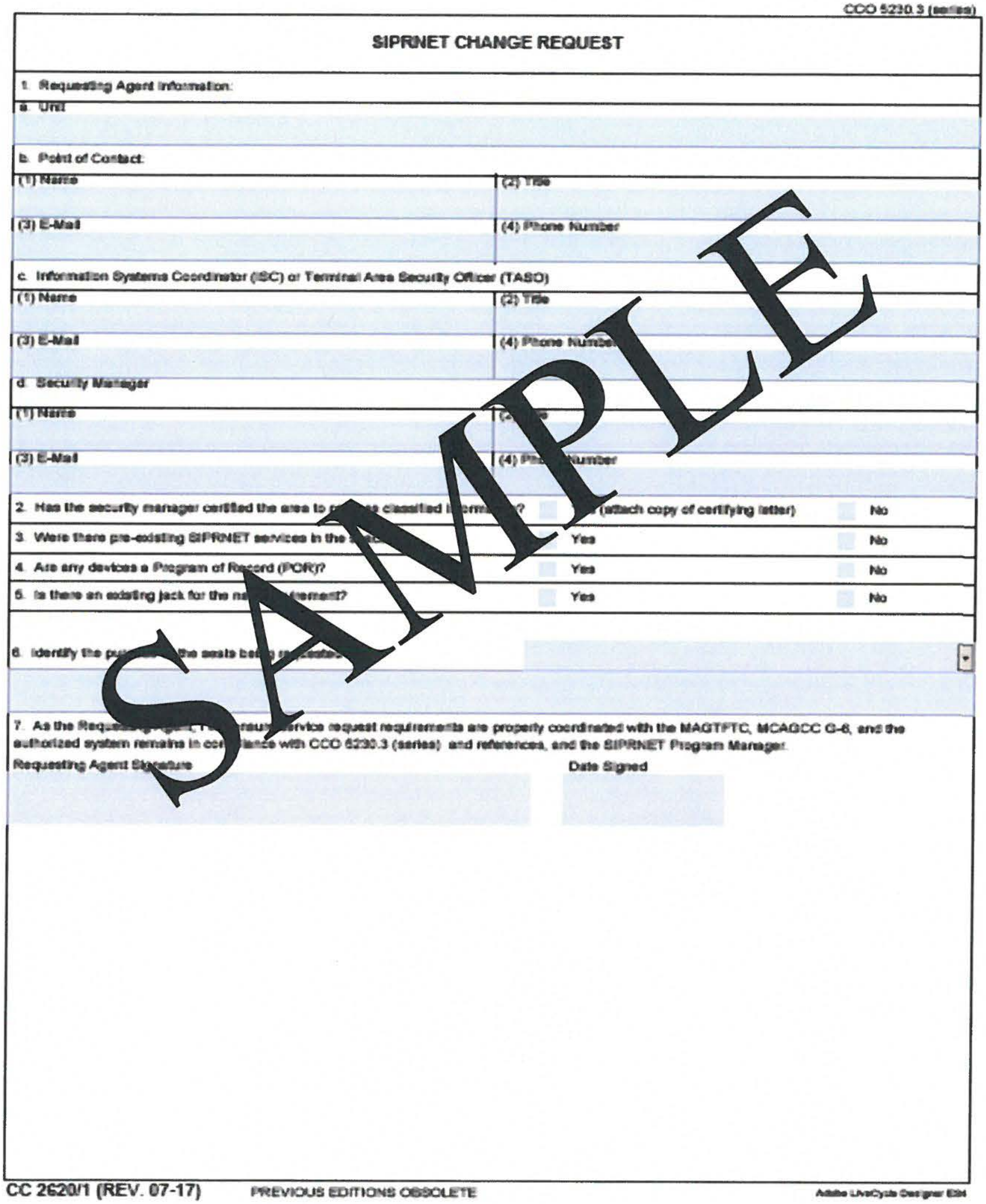
1. Per reference (a), *unit/organization* is requesting a new MCEN-S connection as we currently do not possess one. The proposed location will be in building **####**, room **###** of the **##** floor.

2. The device types and quantities to be connected are;

Device	Model	Quantity

3. *Unit/organization* has reviewed the reference in its entirety and has begun the processes as directed.

C. O. Sign



CCO 5230.3 (series)

SIPRNET CHANGE REQUEST

1. Requesting Agent Information:

a. Unit

b. Point of Contact:

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

c. Information Systems Coordinator (ISC) or Terminal Area Security Officer (TASO)

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

d. Security Manager

(1) Name	(2) Title
(3) E-Mail	(4) Phone Number

2. Has the security manager certified the area to process classified information?	□ Yes (attach copy of certifying letter)	□ No
3. Were there pre-existing SIPRNET services in the space?	□ Yes	□ No
4. Are any devices a Program of Record (POR)?	□ Yes	□ No
5. Is there an existing jack for the new requirement?	□ Yes	□ No

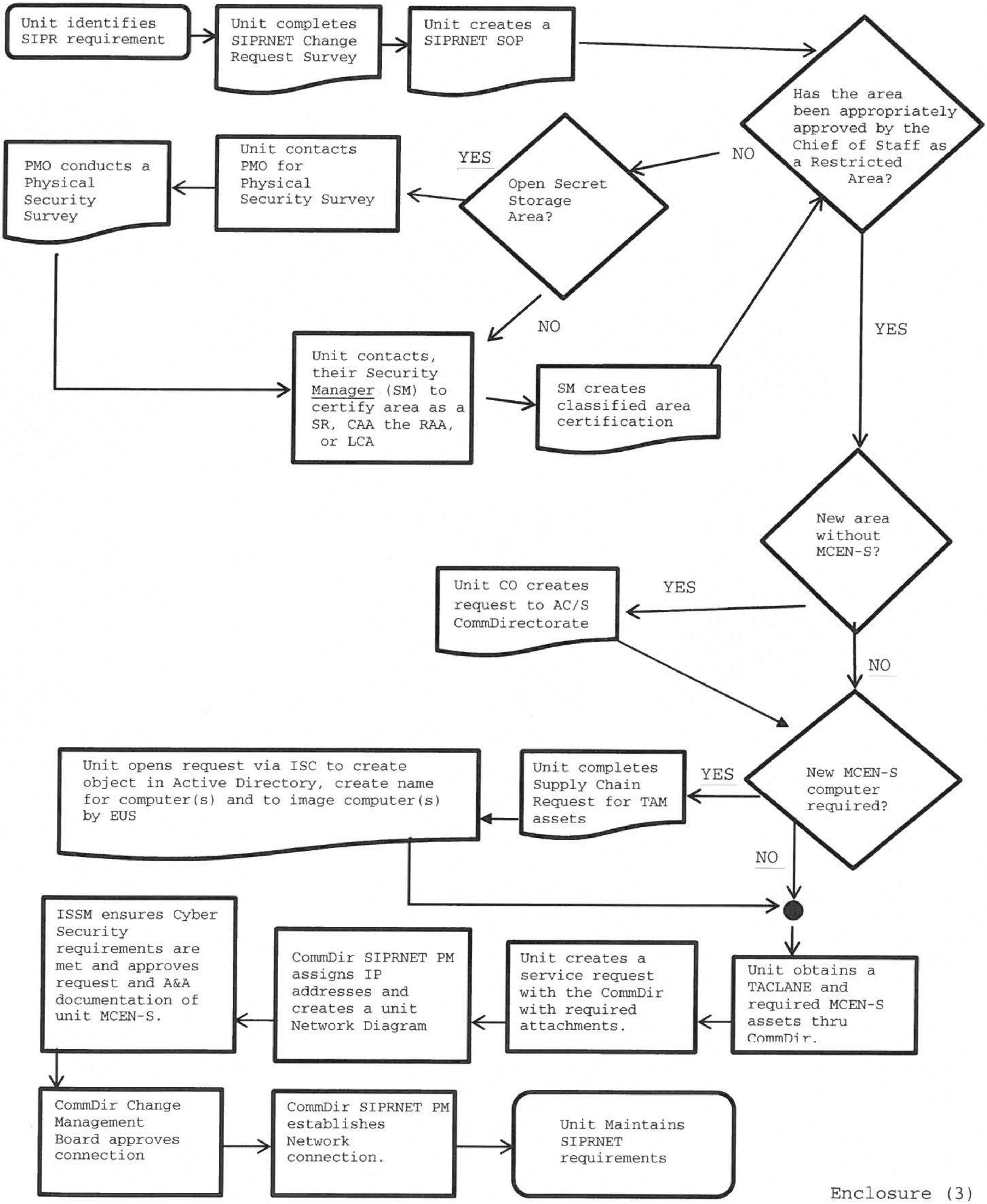
6. Identify the purpose of the seats being requested ▾

7. As the Requesting Agent, I will ensure service request requirements are properly coordinated with the MAGTFTC, MCAGCC G-6, and the authorized system remains in compliance with CCO 5230.3 (series) and references, and the SIPRNET Program Manager.

Requesting Agent Signature   Date Signed

CC 2620/1 (REV. 07-17)   PREVIOUS EDITIONS OBSOLETE   Adobe LiveCycle Designer ES4

Flowchart


Unit identifies SIPR requirement
Unit completes SIPRNET Change Request Survey
Unit creates a SIPRNET SOP
Has the area been appropriately approved by the Chief of Staff as a Restricted Area?
NO
Open Secret Storage Area?
YES
Unit contacts PMO for Physical Security Survey
PMO conducts a Physical Security Survey
NO
Unit contacts, their Security Manager (SM) to certify area as a SR, CAA the RAA, or LCA
SM creates classified area certification
YES
New area without MCEN-S?
YES
Unit CO creates request to AC/S CommDirectorate
NO
New MCEN-S computer required?
YES
Unit completes Supply Chain Request for TAM assets
Unit opens request via ISC to create object in Active Directory, create name for computer(s) and to image computer(s) by EUS
NO
Unit obtains a TACLANE and required MCEN-S assets thru CommDir.
Unit creates a service request with the CommDir with required attachments.
CommDir SIPRNET PM assigns IP addresses and creates a unit Network Diagram
ISSM ensures Cyber Security requirements are met and approves request and A&A documentation of unit MCEN-S.
CommDir Change Management Board approves connection
CommDir SIPRNET PM establishes Network connection.
Unit Maintains SIPRNET requirements