DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, D.C. 20350-3000

NAVMC 3500.56A
C 469
13 May 2011

NAVMC 3500.56A

From: Commandant of the Marine Corps
To: Distribution List

Subj: COMMUNICATIONS (COMM) TRAINING AND READINESS (T&R) MANUAL

Ref: (a) MCO P3500.72A
(b) MCO 1553.3A
(c) MCO 3500.27B W/Erratum
(d) MCRP 3-0A
(e) MCRP 3-0B
(f) MCO 1553.2B

1. Purpose. Per reference (a), this T&R Manual establishes required training standards, regulations, and practices within the communications occupational field. Additionally, it provides tasking for formal schools preparing personnel for service within the communications occupational field.

2. Cancellation. NAVMC DIR 3500.56

3. Scope

a. There are two Core Mission Essential Task Lists (METL) in this Manual. Communication Battalion METL and Communication Squadron METL are used in Defense Readiness Reporting System (DRRS) by all battalions and squadrons for the assessment and reporting of unit readiness. Units achieve training readiness for reporting in DRRS by gaining and sustaining proficiency in the training events in this Manual at both collective unit and individual levels. The Communication Battalion's and Communication Squadron's Mission Essential Tasks (METs) Matrix reflects specific collective event codes and titles and categorizes them directly under the supported MET.

b. Per reference (b), commanders will conduct an internal assessment of the unit's ability to execute its mission and develop long-, mid-, and short-range training plans to sustain proficiency and correct deficiencies. Training plans will incorporate these events to standardize training and provide objective assessment of progress toward attaining combat readiness. Commanders will keep records at the unit and individual levels to record training achievements, identify training gaps and document objective assessments of readiness associated with training Marines. Commanders will use reference (c) to integrate Operational Risk Management (ORM). References (d) and (e) provide amplifying information for effective planning and management of training within the unit.

c. Formal school and training detachment commanders will use references (a) and (f) to ensure program of instruction meet skill training requirements established in this manual, and provides career-progression training in the events designated for initial training in the formal school environment.

4. Information. Commanding General (CG), Training and Education Command (TECOM) will update this T&R Manual as necessary to provide current and relevant training standards to commanders, and to ensure a current Core Capabilities METL is available for use in DRRS. All questions pertaining to the Marine Corps Ground T&R Program and Unit Training Management should be directed to: CG, TECOM (Ground Training Division C 469), 1019 Elliot Road, Quantico, VA 22134.

5. Command. This manual is applicable to the Marine Corps Total Force.

6. Certification. Reviewed and approved this date.

R. C. FOX
By direction

Distribution: PCN 10031977700

Copy to: 7000260 (2)
8145001 (1)

LOCATOR SHEET

Subj: COMMUNICATIONS (COMM) TRAINING AND READINESS (T&R) MANUAL

Location: _____
(Indicate location(s) of copy(ies) of this Manual.)

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Entered	Signature of Person Incorporating Change

COMM T&R MANUAL

TABLE OF CONTENTS

APPENDICES

COMM T&R MANUAL

CHAPTER 1

OVERVIEW

CHAPTER 1

OVERVIEW

1000. INTRODUCTION

1. The T&R Program is the Corps' primary tool for planning, conducting and evaluating training and assessing training readiness. Subject matter experts (SMEs) from the operating forces developed core capability Mission Essential Task Lists (METLs) for ground communities derived from the Marine Corps Task List (MCTL). This T&R Manual is built around these METLs and other related Marine Corps Tasks (MCT). All events contained in the manual relate directly to these METLs and MCTs. This comprehensive T&R Program will help to ensure the Marine Corps continues to improve its combat readiness by training more efficiently and effectively. Ultimately, this will enhance the Marine Corps' ability to accomplish real-world missions.

2. The T&R Manual contains the individual and collective training requirements to prepare units to accomplish their combat mission. The T&R Manual is not intended to be an encyclopedia that contains every minute detail of how to accomplish training. Instead, it identifies the minimum standards that Marines must be able to perform in combat. The T&R Manual is a fundamental tool for commanders to build and maintain unit combat readiness. Using this tool, leaders can construct and execute an effective training plan that supports the unit's METL. More detailed information on the Marine Corps Ground T&R Program is found in reference (a).

3. The T&R Manual is designed for use by curriculum developers to create courses of instruction and unit commanders to determine predeployment training requirements in preparation for training. This directive focuses on individual and collective tasks performed by OPFOR units and supervised by personnel in the performance of unit Mission Essential Tasks (METs).

1001. UNIT TRAINING

1. The training of Marines to perform as an integrated unit in combat lies at the heart of the T&R program. Unit and individual readiness are directly related. Individual training and the mastery of individual core skills serve as the building blocks for unit combat readiness. A Marine's ability to perform critical skills required in combat is essential. However, it is not necessary to have all individuals within a unit fully trained in order for that organization to accomplish its assigned tasks. Manpower shortfalls, temporary assignments, leave, or other factors outside the commander's control, often affect the ability to conduct individual training. During these periods, unit readiness is enhanced if emphasis is placed on the individual training of Marines on-hand. Subsequently, these Marines will be mission ready and capable of executing as part of a team when the full complement of personnel is available.

2. Commanders will ensure that all tactical training is focused on their combat mission. The T&R Manual is a tool to help develop the unit's training plan. In most cases, unit training should focus on achieving unit proficiency in the core METL. However, commanders will adjust their training focus to support METLs associated with a major OPLAN/CONPLAN or named operation as designated by their higher commander and reported accordingly in the Defense Readiness Reporting System (DRRS). Tactical training will support the METL in use by the commander and be tailored to meet T&R standards. Commanders at all levels are responsible for effective combat training. The conduct of training in a professional manner consistent with Marine Corps standards cannot be over emphasized.

3. Commanders will provide personnel the opportunity to attend formal and operational level courses of instruction as required by this manual. Attendance at all formal courses must enhance the warfighting capabilities of the unit as determined by the unit commander.

1002. UNIT TRAINING MANAGEMENT

1. Unit Training Management (UTM) is the application of the Systems Approach to Training (SAT) and the Marine Corps Training Principles. This is accomplished in a manner that maximizes training results and focuses the training priorities of the unit in preparation for the conduct of its wartime mission.

2. UTM techniques, described in references (b) and (d), provide commanders with the requisite tools and techniques to analyze, design, develop, implement, and evaluate the training of their unit. The Marine Corps Training Principles, explained in reference (b), provide sound and proven direction and are flexible enough to accommodate the demands of local conditions. These principles are not inclusive, nor do they guarantee success. They are guides that commanders can use to manage unit-training programs. The Marine Corps training principles are:

- Train as you fight
- Make commanders responsible for training
- Use standards-based training
- Use performance-oriented training
- Use mission-oriented training
- Train the MAGTF to fight as a combined arms team
- Train to sustain proficiency
- Train to challenge

3. To maintain an efficient and effective training program, leaders at every level must understand and implement UTM. Guidance for UTM and the process for establishing effective programs are contained in references (a) through (f).

1003. SUSTAINMENT AND EVALUATION OF TRAINING

1. The evaluation of training is necessary to properly prepare Marines for combat. Evaluations are either formal or informal, and performed by members

of the unit (internal evaluation) or from an external command (external evaluation).

2. Marines are expected to maintain proficiency in the training events for their MOS at the appropriate grade or billet to which assigned. Leaders are responsible for recording the training achievements of their Marines. Whether it involves individual or collective training events, they must ensure proficiency is sustained by requiring retraining of each event at or before expiration of the designated sustainment interval. Performance of the training event, however, is not sufficient to ensure combat readiness. Leaders at all levels must evaluate the performance of their Marines and the unit as they complete training events, and only record successful accomplishment of training based upon the evaluation. The goal of evaluation is to ensure that correct methods are employed to achieve the desired standard, or the Marines understand how they need to improve in order to attain the standard. Leaders must determine whether credit for completing a training event is recorded if the standard was not achieved. While successful accomplishment is desired, debriefing of errors can result in successful learning that will allow ethical recording of training event completion. Evaluation is a continuous process that is integral to training management and is conducted by leaders at every level and during all phases of planning and the conduct of training. To ensure training is efficient and effective, evaluation is an integral part of the training plan. Ultimately, leaders remain responsible for determining if the training was effective.

3. The purpose of formal and informal evaluation is to provide commanders with a process to determine a unit's/Marine's proficiency in the tasks that must be performed in combat. Informal evaluations are conducted during every training evolution. Formal evaluations are often scenario-based, focused on the unit's METs, based on collective training standards, and usually conducted during higher-level collective events. References (a) and (f) provide further guidance on the conduct of informal and formal evaluations using the Marine Corps Ground T&R Program.

1004. ORGANIZATION. The Communications T&R Manual is comprised of 27 chapters. Chapter 2 lists the Communication Battalion's and Communication Squadron's Core METs, which are used as part of the Defense Readiness Reporting System (DRRS). Chapter 3 contains collective events from the Team (3000 level), Section (4000 level), Platoon (5000 level), Company (6000 level) and Battalion / Squadron (7000 level). Chapters 4 through 27 contain individual events for the entire communications occupational field.

1005. T&R EVENT CODING

1. T&R events are coded for ease of reference. Each event has a 4-4-4-digit identifier. The first four digits are referred to as a "community" and represent the MOS. The second four digits represent the functional or duty area (PLAN, OPER, PROT, etc.). The last four digits represent the level, duty area and sequence of the event.

2. The T&R levels are illustrated in Figure 1. An example of the T&R coding used in this Manual is shown in Figure 2.

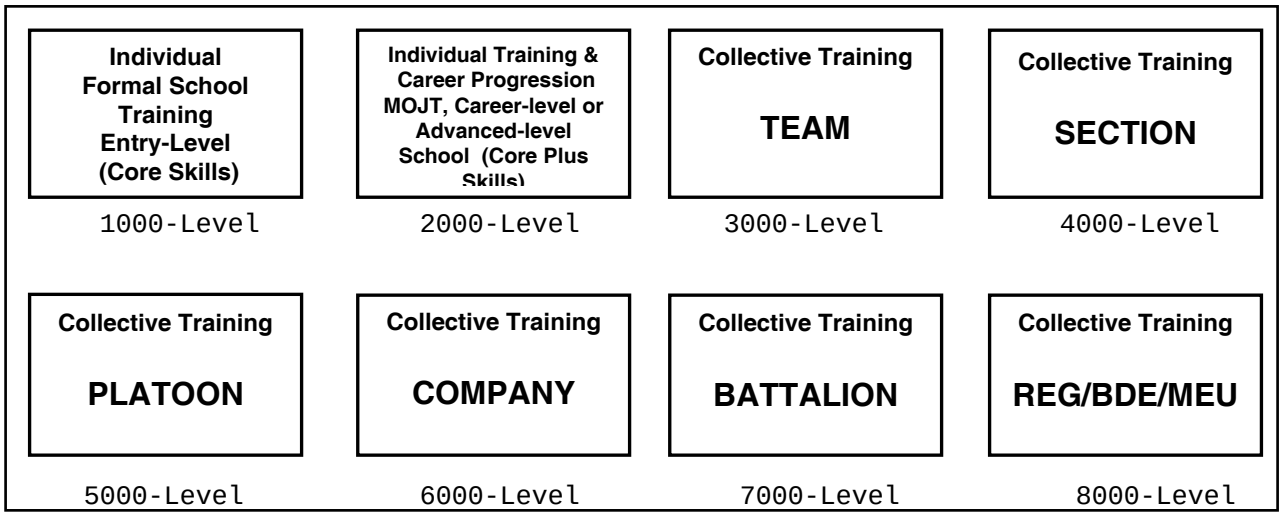

Figure 1: T&R Event Levels

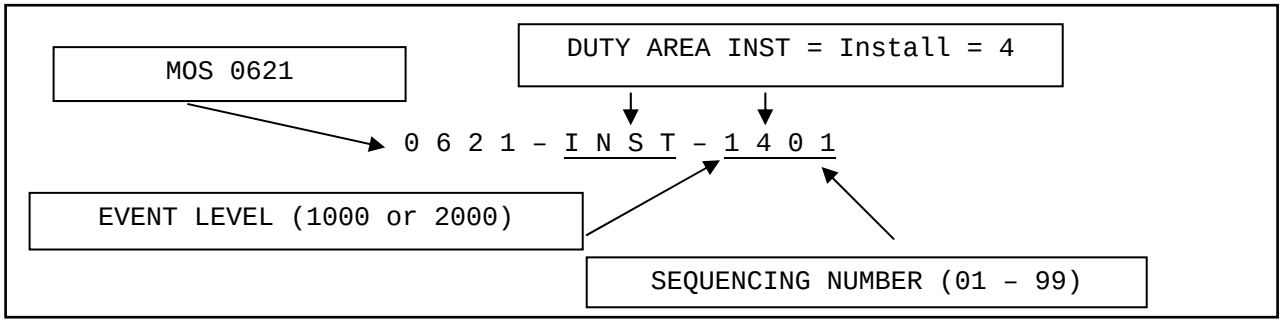

Figure 2: T&R Event Coding

1006. COMBAT READINESS PERCENTAGE

1. The Marine Corps Ground T&R Program includes processes to assess readiness of units and individual Marines. Every unit in the Marine Corps maintains a basic level of readiness based on the training and experience of the Marines in the unit. Even units that never trained together are capable of accomplishing some portion of their missions. Combat readiness assessment does not associate a quantitative value for this baseline of readiness, but uses a "Combat Readiness Percentage", as a method to provide a concise descriptor of the recent training accomplishments of units and Marines.

2. Combat Readiness Percentage (CRP) is the percentage of required training events that a unit or Marine accomplishes within specified sustainment intervals.

3. Unit combat readiness is assessed as a percentage of the successfully completed and current (within sustainment interval) key training events called "Evaluation-Coded" (E-Coded) Events. E-Coded Events and unit CRP calculation are described in follow-on paragraphs. CRP achieved through the

completion of E-Coded Events is directly relevant to readiness assessment in DRRS.

4. Individual combat readiness is assessed as the percentage of required individual events in which a Marine is current. This translates as the percentage of training events for his/her MOS and grade that the Marine successfully completes within the directed sustainment interval. Individual skills are developed through a combination of 1000-level training (entry-level formal school courses), individual on-the-job training in 2000-level events, and follow-on formal school training. Skill proficiency is maintained by retraining in each event per the specified sustainment interval.

1007. EVALUATION-CODED (E-CODED) EVENTS

1. T&R Manuals can contain numerous unit events, some for the whole unit and others for integral parts that serve as building blocks for training. To simplify training management and readiness assessment, only collective events that are critical components of a Mission Essential Task (MET), or key indicators of a unit's readiness, are used to generate CRP for a MET. These critical or key events are designated in the T&R Manual as Evaluation-Coded (E-Coded) events because they directly support a MET on the METL. Formal evaluation of unit performance in these events is recommended because of their value in assessing combat readiness. Only E-Coded events are used to calculate CRP for each MET.

2. The use of a METL-based training program allows the commander discretion in training. This makes the T&R Manual a training tool rather than a prescriptive checklist.

1008. CRP CALCULATION

1. Collective training begins at the 3000 level (team, crew or equivalent). Unit training plans are designed to accomplish the events that support the unit METL while simultaneously sustaining proficiency in individual core skills. E-Coded collective events are the only events that contribute to unit CRP. This is done to assist commanders in prioritizing the training toward the METL, taking into account resource, time, and personnel constraints.

2. Unit CRP increases after the completion of E-Coded events. The number of E-Coded events for the MET determines the value of each E-Coded event. For example, if there are 4 E-Coded events for a MET, each is worth 25% of MET CRP. MET CRP is calculated by adding the percentage of each completed and current (within sustainment interval) E-Coded training event. The percentage for each MET is calculated the same way and all are added together and divided by the number of METS to determine unit CRP. For ease of calculation, we will say that each MET has four E-Coded events, each contributing 25% towards the completion of the MET. If the unit has completed and is current on three of the four E-Coded events for a given MET, then they have completed 75% of the MET. The CRP for each MET is added together and divided by the number of METS to get unit CRP; unit CRP is the average of MET CRP.

For Example:

MET 1: 75% complete (3 of 4 E-Coded events trained)
MET 2: 100% complete (6 of 6 E-Coded events trained)
MET 3: 25% complete (1 of 4 E-Coded events trained)
MET 4: 50% complete (2 of 4 E-Coded events trained)
MET 5: 75% complete (3 of 4 E-Coded events trained)

To get unit CRP, simply add the CRP for each MET and divide by the number of METS:

MET CRP: 75 + 100 + 25 + 50 + 75 = 325

Unit CRP: 325 (total MET CRP)/5 (total number of METS) = 65%

1009. T&R EVENT COMPOSITION

1. This section explains each of the components of a T&R event. Some of the components listed below are not included in the events within this T&R manual.

a. Event Code (see Sect 1005). The event code is an up to 4-4-4 character set. For individual training events, the first four characters indicate the occupational function. The second up to four characters indicate functional area (PLAN = 1, OPER = 5, PROT = 8, etc.). The third four characters are simply a numerical designator / sequence for the event.

b. Event Title. The event title is the name of the event.

c. E-Coded. This is a "yes/no" category to indicate whether the event is E-Coded. If yes, the event contributes toward the CRP of the associated MET. The value of each E-Coded event is based on number of E-Coded events for that MET. Refer to paragraph 1008 for detailed explanation of E-Coded events.

d. Supported MET(s). List all METs that are supported by the training event.

e. Sustainment Interval. This is the period, expressed in number of months, between evaluation or retraining requirements. Skills and capabilities acquired through the accomplishment of training events are refreshed at pre-determined intervals. It is essential that these intervals are adhered to in order to ensure Marines maintain proficiency.

f. Billet. Individual training events may contain a list of billets within the community that are responsible for performing that event. This ensures that the billets expected tasks are clearly articulated and a Marine's readiness to perform in that billet is measured.

g. Grade. Each individual training event will list the rank(s) at which Marines are required to learn and sustain the training event.

h. Initial Training Setting. Specifies the location for initial instruction of the training event in one of three categories (formal school,

managed on-the-job training, distance learning). Regardless of the specified Initial Training Setting, any T&R event may be introduced and evaluated during managed on-the-job training.

(1) "Formal" – When the Initial Training Setting of an event is identified as "FORMAL" (formal school), the appropriate formal school or training detachment is required to provide initial training in the event. Conversely, formal schools and training detachments are not authorized to provide training in events designated as Initial Training Setting "MOJT" or "DL." Since the duration of formal school training must be constrained to optimize Operating Forces' manning, this element provides the mechanism for Operating Forces' prioritization of training requirements. For formal schools and training detachments, this element defines the requirements for content of courses.

(2) "DL" – Identifies the training event as a candidate for initial training via a Distance Learning product (correspondence course or MarineNet course).

(3) "MOJT" – Events specified for Managed On-the-Job Training are to be introduced to Marines as part of training within a unit by supervisory personnel.

i. Event Description. Provide a description of the event purpose, objectives, goals, and requirements. It is a general description of an action requiring learned skills and knowledge (e.g. Camouflage the M1A1 Tank).

j. Condition. Describe the condition(s), under which tasks are performed. Conditions are based on a "real world" operational environment. They indicate what is provided (equipment, materials, manuals, aids, etc.), environmental constraints, conditions under which the task is performed, and any specific cues or indicators to which the performer must respond. When resources or safety requirements limit the conditions, this is stated.

k. Standard. The standard indicates the basis for judging effectiveness of the performance. It consists of a carefully worded statement that identifies the proficiency level expected when the task is performed. The standard provides the minimum acceptable performance parameters and is strictly adhered to. The standard for collective events is general, describing the desired end-state or purpose of the event. While the standard for individual events specifically describe to what proficiency level in terms of accuracy, speed, sequencing, quality of performance, adherence to procedural guidelines, etc., the event is accomplished.

l. Event Components. Describe the actions composing the event and help the user determine what must be accomplished to properly plan for the event.

m. Prerequisite Events. Prerequisites are academic training or other T&R events that must be completed prior to attempting the task. They are lower-level events or tasks that give the individual/unit the skills required to accomplish the event. They can also be planning steps, administrative requirements, or specific parameters that build toward mission accomplishment.

n. Chained Events. Collective T&R events are supported by lower-level collective and individual T&R events. This enables unit leaders to effectively identify subordinate T&R events that ultimately support specific mission essential tasks. When the accomplishment of any upper-level events, by their nature, result in the performance of certain subordinate and related events, the events are "chained." The completion of chained events will update sustainment interval credit (and CRP for E-Coded events) for the related subordinate level events.

o. Related Events. Provide a list of all Individual Training Standards that support the event.

p. References. The training references are utilized to determine task performance steps, grading criteria, and ensure standardization of training procedures. They assist the trainee in satisfying the performance standards, or the trainer in evaluating the effectiveness of task completion. References are also important to the development of detailed training plans.

q. Distance Learning Products (IMI, CBT, MCI, etc.). Include this component when the event can be taught via one of these media methods vice attending a formal course of instruction or receiving MOJT.

r. Support Requirements. This is a list of the external and internal support the unit and Marines will need to complete the event. The list includes, but is not limited to:

- •Range(s)/Training Area
- •Ordnance
- •Equipment
- •Materials
- •Other Units/Personnel
- •Other Support Requirements

s. Miscellaneous. Provide any additional information that assists in the planning and execution of the event. Miscellaneous information may include, but is not limited to:

- •Admin Instructions
- •Special Personnel Certifications
- •Equipment Operating Hours
- •Road Miles

1010. CBRNE TRAINING

1. All personnel assigned to the operating force must be trained in Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) incident defense, in order to survive and continue their mission in this environment. Individual proficiency standards are defined as survival and basic operating standards. Survival standards are those that the individual must master in order to survive CBRNE attacks. Basic operating standards are those that the individual, and collectively the unit, must perform to continue operations in a CBRNE environment.

2. Units should train under CBRNE conditions whenever possible. Per reference (c), all units must be capable of accomplishing their assigned mission in a contaminated environment.

1011. NIGHT TRAINING

1. While it is understood that all personnel and units of the operating force are capable of performing their assigned mission in "every climate and place," current doctrine emphasizes the requirement to perform assigned missions at night and during periods of limited visibility. Basic skills are significantly more difficult when visibility is limited.

2. To ensure units are capable of accomplishing their mission they must train under the conditions of limited visibility. Units should strive to conduct all events in this T&R Manual during both day and night/limited visibility conditions. When there is limited training time available, night training should take precedence over daylight training, contingent on the availability of equipment and personnel.

1012. OPERATIONAL RISK MANAGEMENT (ORM)

1. ORM is a process that enables commanders to plan for and minimize risk while still accomplishing the mission. It is a decision making tool used by Marines at all levels to increase operational effectiveness by anticipating hazards and reducing the potential for loss, thereby increasing the probability of a successful mission. ORM minimizes risks to acceptable levels, commensurate with mission accomplishment.

2. Commanders, leaders, maintainers, planners, and schedulers will integrate risk assessment in the decision-making process and implement hazard controls to reduce risk to acceptable levels. Applying the ORM process will reduce mishaps, lower costs, and provide for more efficient use of resources. ORM assists the commander in conserving lives and resources and avoiding unnecessary risk, making an informed decision to implement a Course Of Action (COA), identifying feasible and effective control measures where specific measures do not exist, and providing reasonable alternatives for mission accomplishment. Most importantly, ORM assists the commander in determining the balance between training realism and unnecessary risks in training, the impact of training operations on the environment, and the adjustment of training plans to fit the level of proficiency and experience of Sailors/Marines and leaders. Further guidance for ORM is found in references (b) and (d).

1013. APPLICATION OF SIMULATION

1. Simulations/Simulators and other training devices shall be used when they are capable of effectively and economically supplementing training on the identified training task. Particular emphasis shall be placed on simulators that provide training that might be limited by safety considerations or constraints on training space, time, or other resources. When deciding on simulation issues, the primary consideration shall be improving the quality of training and consequently the state of readiness. Potential savings in

operating and support costs normally shall be an important secondary consideration.

2. Each training event contains information relating to the applicability of simulation. If simulator training applies to the event, then the applicable simulator(s) is/are listed in the “Simulation” section and the CRP for simulation training is given. This simulation training can either be used in place of live training, at the reduced CRP indicated; or can be used as a precursor training for the live event, i.e., weapons simulators, convoy trainers, observed fire trainers, etc. It is recommended that tasks be performed by simulation prior to being performed in a live-fire environment. However, in the case where simulation is used as a precursor for the live event, then the unit will receive credit for the live event CRP only. If a tactical situation develops that precludes performing the live event, the unit would then receive credit for the simulation CRP.

1014. MARINE CORPS GROUND T&R PROGRAM

1. The Marine Corps Ground T&R Program continues to evolve. The vision for Ground T&R Program is to publish a T&R Manual for every readiness-reporting unit so that core capability METs are clearly defined with supporting collective training standards, and to publish community-based T&R Manuals for all occupational fields whose personnel augment other units to increase their combat and/or logistic capabilities. The vision for this program includes plans to provide a Marine Corps training management information system that enables tracking of unit and individual training accomplishments by unit commanders and small unit leaders, automatically computing CRP for both units and individual Marines based upon MOS and rank (or billet). Linkage of T&R Events to the Marine Corps Task List (MCTL), through the core capability METs, has enabled objective assessment of training readiness in the DRRS.

2. DRRS measures and reports on the readiness of military forces and the supporting infrastructure to meet missions and goals assigned by the Secretary of Defense. With unit CRP based on the unit’s training toward its METs, the CRP will provide a more accurate picture of a unit’s readiness. This will give fidelity to future funding requests and factor into the allocation of resources. Additionally, the Ground T&R Program will help to ensure training remains focused on mission accomplishment and that training readiness reporting is tied to units’ METLs.

COMM T&R MANUAL

CHAPTER 2

MISSION ESSENTIAL TASKS MATRIX

CHAPTER 2

MISSION ESSENTIAL TASKS MATRIX

2000. COMMUNICATIONS BATTALION CORE MISSION ESSENTIAL TASK LIST. The Communications Battalion Mission Essential Task List (METL) Table lists the Standardized Core Mission Essential Task list, derived from the Marine Corps Task List, for the Communications Battalion. This METL is used for readiness reporting in the Defense Readiness Reporting System (DRRS) and is reflected in the T&R METL.

COMM BN CORE MISSION ESSENTIAL TASK

MARINE CORPS TASK LIST	COMM BN CORE METL
MCT 1.1	Provide Forces
MCT 5.1.1.1	Provide Single Channel Radio Communications
MCT 5.1.1.2	Provide Wide Area Networks (WAN)/Local Area Networ (LAN)Communications
MCT 5.1.1.3	Provide Electronic Message Communications
MCT 5.1.1.4	Provide Telephone Communications
MCT 5.1.1.5	Provide Digital Backbone
MCT 5.1.2.6	Provide Communications Control

2001. MARINE WING COMMUNICATIONS SQUADRON CORE MISSION ESSENTIAL TASK LIST. The Marine Wing Communications Squadron Mission Essential Task List (METL) Table lists the Standardized Core Mission Essential Task list, derived from the Marine Corps Task List, for the Marine Wing Communications Squadron. This METL is used for readiness reporting in the Defense Readiness Reporting System (DRRS) and is reflected in the T&R METL.

MWCS CORE MISSION ESSENTIAL TASK

MARINE CORPS TASK LIST	MWCS CORE METL
MCT 1.1.2	Provide Forces
MCT 5.1.1.1	Provide Single Channel Radio Communications
MCT 5.1.1.2	Provide Wide Area Networks (WAN)/Local Area Network (LAN)Communications
MCT 5.1.1.3	Provide Electronic Message Communications
MCT 5.1.1.4	Provide Telephone Communications
MCT 5.1.1.5	Provide Digital Backbone
MCT 5.1.2.6	Provide Communications Control

2002. COMMUNICATIONS BATTALTION AND SQUADRON MISSION ESSENTIAL TASKS MATRIX. The Communications Battalion and Squadron T&R Mission Essential Task List (METL) reflect the tasks in the Comm Bn and MWCS Core METL. The Communications Battalion and Squadron METL Table includes the designated MET number. The following event codes are the linked evaluation coded (E- Coded) events that support the MET.

2003. MET# / MISSION ESSENTIAL TASK / E-CODE MATRIX

MET 1. PROVIDE FORCES		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
MET 2. PROVIDE SINGLE CHANNEL RADIO COMMUNICATIONS		
EVENTY	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3001	Establish a single channel radio site	No
COMM-PIOM-3002	Employ a satellite terminal	No
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5001	Provide single channel radio services	No
COMM-PIOM-5031	Execute a cabling plan	No
COMM-PIOM-5040	Provide data network services	No
COMM-PIOM-5050	Operate an EoIP communications system	No
COMM-PIOM-5060	Provide a communications network in support of a command element	Yes
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6050	Operate an EoIP communications system	No
COMM-PIOM-6060	Provide a communications network in support of a command element	Yes
COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7050	Operate an EoIP communications system	No
COMM-PIOM-7060	Provide a communications network in support of a command element.	Yes
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes
MET 3. Provide Wide Area Networks (WAN)/Local Area Networks(LAN)Communications		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3020	Establish Video Teleconferencing services	No
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4040	Establish data network services	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No

COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5031	Execute a cabling plan	No
COMM-PIOM-5040	Provide data network services	No
COMM-PIOM-5050	Operate an EoIP communications system	No
COMM-PIOM-5060	Provide a communications network in support of a command element	Yes
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6050	Operate an EoIP communications system	No
COMM-PIOM-6060	Provide a communications network in support of a command element	Yes
COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7050	Operate an EoIP communications system	No
COMM-PIOM-7060	Provide a communications network in support of a command element.	Yes
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes
COMM-PIOM-7064	Provide Defense Information Systems Network (DISN) services	Yes
MET 4. PROVIDE ELECTRONIC MESSAGE COMMUNICATIONS		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4040	Establish data network services	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5031	Execute a cabling plan	No
COMM-PIOM-5040	Provide data network services	No
COMM-PIOM-5050	Operate an EoIP communications system	No
COMM-PIOM-5060	Provide a communications network in support of a command element	Yes
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6050	Operate an EoIP communications system	No
COMM-PIOM-6051	Provide classified/unclassified defense messaging services	No
COMM-PIOM-6060	Provide a communications network in support of a command element	Yes
COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7050	Operate an EoIP communications system	No
COMM-PIOM-7060	Provide a communications network in support of a command element	Yes
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes
COMM-PIOM-7064	Provide Defense Information Systems Network (DISN) services	Yes

MET 5. PROVIDE TELEPHONE COMMUNICATIONS		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3020	Establish Video Teleconferencing services	No
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4030	Install trunked telephony services	No
COMM-PIOM-4040	Establish data network services	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5030	Provide telephony services	No
COMM-PIOM-5031	Execute a cabling plan	No
COMM-PIOM-5040	Provide data network services	No
COMM-PIOM-5050	Operate an EoIP communications system	No
COMM-PIOM-5060	Provide a communications network in support of a command element	Yes
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6050	Operate an EoIP communications system	No
COMM-PIOM-6060	Provide a communications network in support of a command element	Yes
COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7050	Operate an EoIP communications system	No
COMM-PIOM-7060	Provide a communications network in support of a command element	Yes
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes
COMM-PIOM-7064	Provide Defense Information Systems Network (DISN) services	Yes
MET 6. PROVIDE DIGITAL BACKBONE		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-3002	Employ a satellite terminal	No
COMM-PIOM-3003	Establish a multi-channel radio site	No
COMM-PIOM-3010	Establish a multiplexed architecture	No
COMM-PIOM-3060	Provide communications services for rapid response	No
COMM-PIOM-4003	Establish a terrestrial multi-channel UHF radio link	No
COMM-PIOM-4004	Establish a terrestrial multi-channel SHF radio link	No
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5002	Establish a hybrid meshed/nodal satellite network	No
COMM-PIOM-5031	Execute a cabling plan	No
COMM-PIOM-5040	Provide data network services	No
COMM-PIOM-5060	Provide a communications network in support of a command element	Yes
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6060	Provide a communications network in support of a command element	Yes

COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7060	Provide a communications network in support of a command element	Yes
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes
COMM-PIOM-7064	Provide Defense Information Systems Network (DISN) services	Yes
MET 7. PROVIDE COMMUNICATIONS CONTROL		
EVENT	**EVENT TITLE**	**E-CODED**
COMM-PIOM-4060	Provide communications for a MEU Command Element	No
COMM-PIOM-4061	Provide initial communications for a Joint Task Force (JTF) Command Element	No
COMM-PIOM-5061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-5062	Perform communications control	No
COMM-PIOM-6061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-6062	Perform communications control	No
COMM-PIOM-7061	Establish communications with higher, adjacent and subordinate units	Yes
COMM-PIOM-7062	Perform communications control	Yes
COMM-PIOM-7063	Facilitate information exchange across the MAGTF	Yes

COMM T&R MANUAL

CHAPTER 3

COLLECTIVE EVENTS

COMM T&R MANUAL

CHAPTER 3

COLLECTIVE EVENTS

3000. PURPOSE. This chapter illustrates the relationship between unit competencies [Mission Essential Tasks (METS)] and unit training (Collective Events). Unit training managers can isolate all training relevant to each MET and devise training to support their competencies as needed. Collective training provides a base for comparison of units as well as defines the training requirements to be met by reporting units.

3001. COLLECTIVE EVENT LEVELS

1. 3000-Level Events: Team
2. 4000-Level Events: Section
3. 5000-Level Events: Platoon
4. 6000-Level Events: Company
5. 7000-Level Events: Battalion / Squadron

3002. EVENT CODING. Events in the T&R Manual are depicted with a 12 field alphanumeric system, i.e. COMM-PIOM-7060. All collective events in this manual use the following methodology:

a. Field one – Each event starts with “COMM”, indicating that the event is for units within the communications occupational field.

b. Field two – This field is alpha characters indicating a functional area. The collective event functional area is Plan, Install, Operate, Maintain (PIOM) for all collective events.

c. Field three – This field provides numerical sequencing as well as represents the level of the event. The first digit of this field indicates the level 3000 to 7000. The second digit is a place holder to allow for sequential numbering in the case the allocated 10 digit (last two digits) numbering scheme is exceeded. The third and fourth digits are associated with a specific function and sequence (ie. 01 – 09 are associated with radio communications, 30 - 39 with telephony, and 40 – 40 with data services etc… For example, 5002 indicates that this is a five thousand level event and that it is the second task within the radio functional area. More information on event levels and sequencing can be found in paragraph 1005 of chapter one.

Functional Area	Field Name	Example
Plan Install Operate Maintain	PIOM	COMM-PIOM-7060

3003. 7000-LEVEL EVENTS

COMM-PIOM-7064: Provide Defense Information Systems Network (DISN) services

SUPPORTED MET(S): 3, 4, 5, 6

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will establish DISN STEP access and IOM all required communication and support assets IOT provide secure/non-secure voice, video, data and real-time services in support of end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, all equipment and personnel, the Satellite Access Authorization (SAA) and Gateway Access Authorization (GAA).

STANDARD: Within 48 hours to satisfy the commander's information exchange requirements.

EVENT COMPONENTS:
1. Establish satellite connectivity.
2. Establish STEP/TELEPORT connectivity.
3. Establish multiplexer connectivity.
4. Terminate voice circuits as required.
5. Terminate VTC circuits as required.
6. Terminate DMS circuits as required.
7. Distributed DISN services.
8. Terminate special circuits as required.
9. Terminate data network circuits as required.

CHAINED EVENTS:

COMM-PIOM-5001	COMM-PIOM-5031	COMM-PIOM-5040
COMM-PIOM-5030	COMM-PIOM-5002	

RELATED EVENTS:

COMM-PIOM-7060	COMM-PIOM-5050	COMM-PIOM-7062
COMM-PIOM-6050	COMM-PIOM-6051	COMM-PIOM-6060
COMM-PIOM-6061	COMM-PIOM-6062	COMM-PIOM-7050
COMM-PIOM-5061	COMM-PIOM-5062	COMM-PIOM-5060
COMM-PIOM-4061	COMM-PIOM-7063	COMM-PIOM-4060
COMM-PIOM-7061		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-7063: Facilitate information exchange across the MAGTF

SUPPORTED MET(S): 2, 3, 4, 5, 6, 7

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will IOM all required communication and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data, and real-time services in support of MAGTF information exchange requirements with higher, adjacent, and subordinate units.

CONDITION: Given a command's mission, communications plan, all equipment and personnel.

STANDARD: To enable command and control.

EVENT COMPONENTS:
1. Establish communication services with higher unit.
2. Establish communication services with adjacent units.
3. Establish communication services with subordinate units.

CHAINED EVENTS:

COMM-PIOM-5031	COMM-PIOM-5040	COMM-PIOM-5030
COMM-PIOM-5002	COMM-PIOM-5001	

RELATED EVENTS:

COMM-PIOM-7060	COMM-PIOM-6050	COMM-PIOM-7061
COMM-PIOM-7062	COMM-PIOM-7064	COMM-PIOM-5061
COMM-PIOM-4060	COMM-PIOM-6051	COMM-PIOM-6062
COMM-PIOM-6060	COMM-PIOM-6061	COMM-PIOM-5060
COMM-PIOM-4061	COMM-PIOM-5050	COMM-PIOM-5062
COMM-PIOM-7050		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-7062: Perform communications control

SUPPORTED MET(S): 7

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will exercise communications control (COMCON) through the organization, direction, coordination, planning, decentralized execution, and employment of resources to engineer, install, operate, and maintain a communications network responsive to operational requirements. COMMCON consists of three functional areas: systems planning and engineering, operational systems control, and technical control and is exerted through the arrangement of communication elements throughout the chain of command to ensure MAGTF interoperability.

CONDITION: Given a command's mission, communications plan, all equipment and personnel.

STANDARD: To mitigate risks to information exchange and minimize service interruptions.

EVENT COMPONENTS:
1. Establish a COMCON hierarchy.
2. Establish a SYSCON.
3. Establish a TECHCON.
4. Establish a helpdesk as required.
5. Submit reports as required.
6. Coordinate network modifications.

RELATED EVENTS:

COMM-PIOM-5062	COMM-PIOM-7063	COMM-PIOM-5050
COMM-PIOM-5060	COMM-PIOM-5061	COMM-PIOM-6050
COMM-PIOM-6051	COMM-PIOM-6060	COMM-PIOM-6061
COMM-PIOM-7050	COMM-PIOM-7061	COMM-PIOM-7064
COMM-PIOM-6062	COMM-PIOM-7060	COMM-PIOM-4060
COMM-PIOM-4061		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-7061: Establish communications with higher, adjacent and subordinate units

SUPPORTED MET(S): 2, 3, 4, 5, 6, 7

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will IOM all required communications and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services that support end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, all equipment and personnel, and having established DISN services.

STANDARD: Within 48 hours of arrival at the area of operation, meet the commander's information exchange requirements.

EVENT COMPONENTS:
1. Establish single channel radio networks.
2. Establish terrestrial multi-channel radio networks.
3. Establish satellite networks.
4. Establish a multiplexed architecture.
5. Establish telephony services.
6. Establish data network services.

CHAINED EVENTS:

COMM-PIOM-5001	COMM-PIOM-5002	COMM-PIOM-5040
COMM-PIOM-5031	COMM-PIOM-5030	

RELATED EVENTS:

COMM-PIOM-5050	COMM-PIOM-6050	COMM-PIOM-7062
COMM-PIOM-7064	COMM-PIOM-7063	COMM-PIOM-7060
COMM-PIOM-5062	COMM-PIOM-6061	COMM-PIOM-4060
COMM-PIOM-4061	COMM-PIOM-5060	COMM-PIOM-5061
COMM-PIOM-6060	COMM-PIOM-6062	COMM-PIOM-6051

REFERENCES:

1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-7060: Provide a communications network in support of a command element

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will IOM all required communication and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services in support of end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within a time allotted by the commander, to satisfy information exchange requirements.

EVENT COMPONENTS:

1. Establish multi-channel radio networks.
2. Establish a nodal satellite network.
3. Establish a systems control facility.
4. Establish single channel radio networks.
5. Establish a technical control facility.
6. Establish a cabling plant.
7. Establish a multiplexed architecture.
8. Establish telephone networks.
9. Establish data networks.
10. Establish special circuits as required.
11. Implement COMSEC policies established by higher headquarters.
12. Implement information assurance policies.
13. Distribute services to end users.

CHAINED EVENTS:

COMM-PIOM-5031	COMM-PIOM-5001	COMM-PIOM-5040
COMM-PIOM-5030	COMM-PIOM-5002	

RELATED EVENTS:

COMM-PIOM-7050	COMM-PIOM-6062	COMM-PIOM-7064
COMM-PIOM-5050	COMM-PIOM-5062	COMM-PIOM-4060
COMM-PIOM-5060	COMM-PIOM-5061	COMM-PIOM-4061
COMM-PIOM-6060	COMM-PIOM-6061	COMM-PIOM-7061
COMM-PIOM-7063	COMM-PIOM-6050	COMM-PIOM-6051
COMM-PIOM-7062		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-7050: Operate an EoIP communications system

SUPPORTED MET(S): 2, 3, 4, 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Battalion/Squadron will provide an everything over Internet Protocol (EoIP) converged network solution to enable command and control. The term "converged" describes communications equipment that integrates voice, video, data and real-time services into one system (see reference #1).

CONDITION: Given a communications plan, all required equipment and personnel, SAA, and approved certification and accreditation package.

STANDARD: To provide a converged network solution that satisfies the commander's information exchange requirements.

EVENT COMPONENTS:
1. Review the communications plan.
2. Install the EoIP communications system.
3. Extend voice, video, data, and real-time services to end users.

CHAINED EVENTS:

COMM-PIOM-5031	COMM-PIOM-5040

RELATED EVENTS:

COMM-PIOM-7062	COMM-PIOM-6051	COMM-PIOM-7064
COMM-PIOM-5061	COMM-PIOM-4060	COMM-PIOM-4061
COMM-PIOM-7060	COMM-PIOM-6060	COMM-PIOM-6061
COMM-PIOM-6062	COMM-PIOM-5060	COMM-PIOM-5062
COMM-PIOM-6050	COMM-PIOM-5050	COMM-PIOM-7061
COMM-PIOM-7063		

REFERENCES:
1. CISCO Exploration LAN Switching and Wireless Text Book
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

3004. 6000-LEVEL EVENTS

COMM-PIOM-6062: Perform communications control

SUPPORTED MET(S): 7

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Company will exercise communications control (COMCON) through the organization, direction, coordination, planning, decentralized execution, and employment of resources to engineer, install, operate, and maintain a communications network responsive to operational requirements. COMCON consists of three functional areas: systems planning and engineering, operational systems control, and technical control and is exerted through the arrangement of communication elements throughout the chain of command to ensure MAGTF interoperability.

CONDITION: Given a command's mission, communications plan, all equipment and personnel.

STANDARD: To mitigate risks to information exchange and minimize service interruptions.

EVENT COMPONENTS:
1. Establish a COMCON hierarchy.
2. Establish a SYSCON.
3. Establish a TECHCON.
4. Establish a helpdesk as required.
5. Submit reports as required.
6. Coordinate network modifications.

RELATED EVENTS:

COMM-PIOM-4060	COMM-PIOM-5061	COMM-PIOM-7063
COMM-PIOM-6050	COMM-PIOM-6051	COMM-PIOM-6060
COMM-PIOM-7050	COMM-PIOM-7060	COMM-PIOM-7061
COMM-PIOM-7062	COMM-PIOM-7064	COMM-PIOM-5062
COMM-PIOM-6061	COMM-PIOM-5050	COMM-PIOM-5060
COMM-PIOM-4061		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-6061: Establish communications with higher, adjacent and subordinate units

SUPPORTED MET(S): 2, 3, 4, 5, 6, 7

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Company will IOM all required communications and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services that support end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, all equipment and personnel, and having established DISN services.

STANDARD: Within 48 hours of arrival at the area of operation, meet the commander's information exchange requirements.

EVENT COMPONENTS:
1. Establish single channel radio networks.
2. Establish terrestrial multi-channel radio networks.
3. Establish satellite networks.
4. Establish data network services.
5. Establish a multiplexed architecture.
6. Establish telephony services.

CHAINED EVENTS:

COMM-PIOM-5001	COMM-PIOM-5002	COMM-PIOM-5030
COMM-PIOM-5031	COMM-PIOM-5040	

RELATED EVENTS:

COMM-PIOM-6060	COMM-PIOM-7050	COMM-PIOM-7064
COMM-PIOM-7060	COMM-PIOM-7061	COMM-PIOM-7063
COMM-PIOM-5050	COMM-PIOM-5062	COMM-PIOM-5060
COMM-PIOM-4060	COMM-PIOM-4061	COMM-PIOM-6050
COMM-PIOM-6051	COMM-PIOM-6060	COMM-PIOM-6062
COMM-PIOM-7062	COMM-PIOM-5061	

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-6060: Provide a communications network in support of a command element

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Company will IOM all required communication and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services in support of end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within a time allotted by the commander, to satisfy information

exchange requirements.

EVENT COMPONENTS:
1. Establish multi-channel radio networks.
2. Establish a nodal satellite network.
3. Establish a systems control facility.
4. Establish single channel radio networks.
5. Establish a technical control facility.
6. Establish a cabling plant.
7. Establish a multiplexed architecture.
8. Establish telephone networks.
9. Establish data networks.
10. Establish special circuits as required.
11. Implement COMSEC policies established by higher headquarters.
12. Implement information assurance policies.
13. Distribute services to end users.

CHAINED EVENTS:

COMM-PIOM-5001	COMM-PIOM-5002	COMM-PIOM-5030
COMM-PIOM-5031	COMM-PIOM-5040	

RELATED EVENTS:

COMM-PIOM-5060	COMM-PIOM-5050	COMM-PIOM-4060
COMM-PIOM-4061	COMM-PIOM-7060	COMM-PIOM-7063
COMM-PIOM-6050	COMM-PIOM-6051	COMM-PIOM-6061
COMM-PIOM-6062	COMM-PIOM-7064	COMM-PIOM-5062
COMM-PIOM-7050	COMM-PIOM-7061	COMM-PIOM-7062
COMM-PIOM-5061		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-6051: Provide classified/unclassified defense messaging services

SUPPORTED MET(S): 4

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Company will IOM the Defense Message System (DMS) in support of higher and subordinate headquarters. The DMS consists of all required hardware, software, procedures, standards, facilities, and personnel and provides a secure, timely, reliable messaging service across strategic and deployed environments. Examples of successful tasks include exchanging classified/unclassified messages electronically between organizations and individuals within the DoD.

CONDITION: Given a command's mission, Defense Messaging plan, all equipment and personnel, and established DISN data networking services.

STANDARD: Within 24 hours to satisfy the commander's information exchange

requirements.

EVENT COMPONENTS:
1. Coordinate for continued defense messaging capability.
2. Install a defense messaging system.
3. Provide classified/unclassified messaging service.

RELATED EVENTS:

COMM-PIOM-5061	COMM-PIOM-7063	COMM-PIOM-6061
COMM-PIOM-6062	COMM-PIOM-5050	COMM-PIOM-5060
COMM-PIOM-5062	COMM-PIOM-7061	COMM-PIOM-7062
COMM-PIOM-7064	COMM-PIOM-6050	COMM-PIOM-4060
COMM-PIOM-4061	COMM-PIOM-7060	COMM-PIOM-7050
COMM-PIOM-6060		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP 2-01.2 Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-6050: Operate an EoIP communications system

SUPPORTED MET(S): 2, 3, 4, 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The Company will provide an everything over Internet Protocol (EoIP) converged network solution to enable command and control. The term "converged" describes communications equipment that integrates voice, video, data and real-time services into one system (see reference #1).

CONDITION: Given a communications plan, all required equipment and personnel, SAA, and approved certification and accreditation package.

STANDARD: To provide a converged network solution that satisfies the commander's information exchange requirements.

EVENT COMPONENTS:
1. Review the communications plan.
2. Install the EoIP communications system.
3. Extend voice, video, data, and real-time services to end users.

CHAINED EVENTS:

COMM-PIOM-5031	COMM-PIOM-5040

RELATED EVENTS:

COMM-PIOM-7063	COMM-PIOM-7064	COMM-PIOM-6060
COMM-PIOM-6061	COMM-PIOM-6062	COMM-PIOM-7062
COMM-PIOM-5060	COMM-PIOM-5061	COMM-PIOM-5062
COMM-PIOM-4060	COMM-PIOM-4061	COMM-PIOM-5050

COMM-PIOM-7050 COMM-PIOM-7060 COMM-PIOM-7061
COMM-PIOM-6051

REFERENCES:

1. CISCO Exploration LAN Switching and Wireless Text Book
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

3005. 5000-LEVEL EVETNS

COMM-PIOM-5062: Perform communications control

SUPPORTED MET(S): 7

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will exercise communications control (COMCON) through the organization, direction, coordination, planning, decentralized execution, and employment of resources to engineer, install, operate, and maintain a communications network responsive to operational requirements. COMMCON consists of three functional areas: systems planning and engineering, operational systems control, and technical control and is exerted through the arrangement of communication elements throughout the chain of command to ensure MAGTF interoperability.

CONDITION: Given a command's mission, communications plan, all equipment and personnel.

STANDARD: To mitigate risks to information exchange and minimize service interruptions.

EVENT COMPONENTS:
1. Establish a COMCON hierarchy.
2. Establish a SYSCON.
3. Establish a TECHCON.
4. Establish a helpdesk as required.
5. Submit reports as required.
6. Coordinate network modifications.

RELATED EVENTS:

COMM-PIOM-4060	COMM-PIOM-6050	COMM-PIOM-5060
COMM-PIOM-6051	COMM-PIOM-6060	COMM-PIOM-6062
COMM-PIOM-7050	COMM-PIOM-7060	COMM-PIOM-7061
COMM-PIOM-7062	COMM-PIOM-7063	COMM-PIOM-7064
COMM-PIOM-6061	COMM-PIOM-5050	COMM-PIOM-5061
COMM-PIOM-4061		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-5061: Establish communications with higher, adjacent and subordinate units

SUPPORTED MET(S): 2, 3, 4, 5, 6, 7

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will IOM all required communications and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services that support end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, all equipment and personnel, and having established DISN services.

STANDARD: Within 48 hours of arrival at the area of operation, meet the commander's information exchange requirements.

EVENT COMPONENTS:
1. Establish single channel radio networks.
2. Establish terrestrial multi-channel radio networks.
3. Establish satellite networks.
4. Establish data network services.
5. Establish a multiplexed architecture.
6. Establish telephony services.

CHAINED EVENTS:

COMM-PIOM-5001	COMM-PIOM-5002	COMM-PIOM-5030
COMM-PIOM-5031	COMM-PIOM-5040	

RELATED EVENTS:

COMM-PIOM-4060	COMM-PIOM-4061	COMM-PIOM-6060
COMM-PIOM-6050	COMM-PIOM-6061	COMM-PIOM-6062
COMM-PIOM-5050	COMM-PIOM-5060	COMM-PIOM-5062
COMM-PIOM-7050	COMM-PIOM-7060	COMM-PIOM-7061
COMM-PIOM-7062	COMM-PIOM-7063	COMM-PIOM-7064
COMM-PIOM-6051		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5060: Provide a communications network in support of a command element

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will IOM all required communication and support assets IOT provide secure/non-secure voice (e.g. radio and telephony), video, data and real-time services in support of end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within a time allotted by the commander, to satisfy information

exchange requirements.

EVENT COMPONENTS:
1. Establish multi-channel radio networks.
2. Establish single channel radio networks.
3. Establish a technical control facility.
4. Establish a cabling plant.
5. Establish a multiplexed architecture.
6. Establish telephone networks.
7. Establish data networks.
8. Establish special circuits as required.
9. Implement COMSEC policies established by higher headquarters.
10. Implement information assurance policies.
11. Distribute services to end users.
12. Establish a nodal satellite network.
13. Establish a systems control facility.

RELATED EVENTS:

COMM-PIOM-7050	COMM-PIOM-6062	COMM-PIOM-7064
COMM-PIOM-7061	COMM-PIOM-7063	COMM-PIOM-5062
COMM-PIOM-6060	COMM-PIOM-6061	COMM-PIOM-4060
COMM-PIOM-4061	COMM-PIOM-5061	COMM-PIOM-5050
COMM-PIOM-7060	COMM-PIOM-6050	COMM-PIOM-6051
COMM-PIOM-7062		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JP6-0 Joint Communications System
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5050: Operate an EoIP communications system

SUPPORTED MET(S): 2, 3, 4, 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will provide an everything over Internet Protocol (EoIP) converged network solution to enable command and control. The term "converged" describes communications equipment that integrates voice, video, data and real-time services into one system (see reference #1).

CONDITION: Given a communications plan, all required equipment and personnel, SAA, and approved certification and accreditation package.

STANDARD: To provide a converged network solution that satisfies the commander's information exchange requirements.

EVENT COMPONENTS:
1. Review the communications plan.
2. Install the EoIP communications system.
3. Extend voice, video, data, and real-time services to end users.

CHAINED EVENTS:
COMM-PIOM-5031 COMM-PIOM-5040

RELATED EVENTS:

COMM-PIOM-4060	COMM-PIOM-6051	COMM-PIOM-6060
COMM-PIOM-6061	COMM-PIOM-6062	COMM-PIOM-7060
COMM-PIOM-7062	COMM-PIOM-7063	COMM-PIOM-7064
COMM-PIOM-7050	COMM-PIOM-7061	COMM-PIOM-5060
COMM-PIOM-5061	COMM-PIOM-5062	COMM-PIOM-6050
COMM-PIOM-4061		

REFERENCES:
1. CISCO Exploration LAN Switching and Wireless Text Book
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5040: Provide data network services

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will employ data network resources IAW the Data Network Plan utilizing all necessary support assets. Examples of successful tasks include the installation of switches, routers, servers and boundary protection devices to provide access to secure/non-secure email, web browsing and other required data network services.

CONDITION: Given a command's mission, a Data Network Plan, all equipment and personnel, an approved certification and accreditation package, and an existing digital backbone.

STANDARD: Within 48 hours to satisfy the commander's information exchange requirements.

EVENT COMPONENTS:
1. Install network architecture.
2. Install boundary protection devices.
3. Install data network services.
4. Conduct computer network defense.
5. Enforce information assurance policies.
6. Provide end user support.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5031: Execute a cabling plan

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will IOM all required cable runs to provide connectivity between transmission mediums, multiplexing systems, and switching systems including inside and outside plant installation.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within the time allotted by the commander and with signal quality levels appropriate to the medium.

EVENT COMPONENTS:
1. Validate cut sheets and CCSD/SLD.
2. Validate line route map.
3. Install cable runs.
4. Establish inside plant.
5. Establish outside plant.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5030: Provide telephony services

SUPPORTED MET(S): 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will IOM all terminal devices IAW the Telephone Network Plan utilizing all necessary support assets. Examples of successful tasks include establishing secure and non-secure call processing according to Multi-Level Precedence and Preemption directives in a stand alone, tandem or gateway architecture, and any special requirements such as conference calling or other features.

CONDITION: Given a command's mission, Telephone network plan, all equipment and personnel, and an existing trunk.

STANDARD: Within 3 hours to satisfy the command's circuit switching requirements.

EVENT COMPONENTS:
1. Validate cut sheets and diagrams.
2. Establish loops.
3. Install terminal devices.
4. Provide input for ISD.
5. Validate input for ISD.
6. Provide end user support.

CHAINED EVENTS: COMM-PIOM-4030

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5002: Establish a hybrid meshed/nodal satellite network

SUPPORTED MET(S): 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The platoon will IOM a hybrid meshed satellite network IAW the Radio Network Plan utilizing all necessary support assets. A hybrid meshed/nodal configuration is multiple nodal and non-nodal terminals communicating in a single topology. Platoon members will ensure site survey guidelines and Satellite Access Authorization (SAA) parameters are enforced. An example of a successful task is a satellite network that provides signal quality levels capable of supporting data exchange.

CONDITION: Given a command's mission, a Radio Network Plan, all equipment and personnel, and an SAA.

STANDARD: Within 12 hours of arrival at the designated site, with appropriate signal quality levels.

EVENT COMPONENTS:
1. Coordinate with external agencies for satellite access.
2. Establish link(s).
3. Verify signal quality levels.

CHAINED EVENTS:
COMM-PIOM-4003 COMM-PIOM-4004

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-5001: Provide single channel radio services

SUPPORTED MET(S): 2

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: The platoon will provide single channel radio services IAW the Radio Network Plan utilizing all necessary support assets. An example of a successful task includes the physical layout and the configuration of all single channel radio assets that meet all functional and safety parameters.

CONDITION: Provided a commands mission, a Radio Network Plan, SAA, and all required equipment and personnel.

STANDARD: Within 1 hour to satisfy the commander's information exchange requirements.

EVENT COMPONENTS:
1. Conduct deliberate ORM.
2. Establish single channel radio networks by frequency band.
3. Extend radio services to end users.
4. Establish a radio watch.

CHAINED EVENTS:
COMM-PIOM-3002 COMM-PIOM-3001

RELATED EVENTS:
COMM-PIOM-3001 COMM-PIOM-3002

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. JP6-0 Joint Communications System
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. UNIT SOP Unit's Standing Operating Procedures

3006. 4000-LEVEL EVENTS

COMM-PIOM-4061: Provide initial communications for a Joint Task Force (JTF) Command Element.

SUPPORTED MET(S): 1, 2, 3, 4, 5, 6, 7

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The section will IOM all required communication and support assets IOT provide secure/non-secure voice, video, data and real-time services that support end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within 12 hours of arrival at the area of operation, meet the commanders information exchange requirements.

EVENT COMPONENTS:
1. Establish a Systems Control facility.
2. Establish Single Channel Radio Communications.
3. Establish a Technical Control facility.
4. Coordinate with the STEP/TELEPORT sites as required.
5. Establish communication with the STEP/TELEPORT sites as required.
6. Establish adjacent links as required.
7. Terminate the signal at the multiplexer as required.
8. Distribute services to end users.

RELATED EVENTS:

COMM-PIOM-6050	COMM-PIOM-5050	COMM-PIOM-5061
COMM-PIOM-5060	COMM-PIOM-6062	COMM-PIOM-6051
COMM-PIOM-4060	COMM-PIOM-6060	COMM-PIOM-6061
COMM-PIOM-7064	COMM-PIOM-7062	COMM-PIOM-7050
COMM-PIOM-7061	COMM-PIOM-7060	COMM-PIOM-5062
COMM-PIOM-7063		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-4060: Provide communications for a MEU Command Element

SUPPORTED MET(S): 1, 2, 3, 4, 5, 6, 7

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: The section will IOM all required communication and support assets IOT provide secure/non-secure voice, video, data and real-time

services in support of end user information exchange enabling command and control.

CONDITION: Given a command's mission, communications plan, and all equipment and personnel.

STANDARD: Within 12 hours of arrival at the area of operation, meet the commanders information exchange requirements.

EVENT COMPONENTS:
1. Establish a Systems Control facility.
2. Establish Single Channel Radio Communications.
3. Establish a Technical Control facility.
4. Coordinate with the STEP/TELEPORT sites as required.
5. Establish communication with the STEP/TELEPORT sites as required.
6. Establish adjacent links as required.
7. Terminate the signal at the multiplexer as required.
8. Distribute services to end users.

RELATED EVENTS:

COMM-PIOM-5060	COMM-PIOM-7063	COMM-PIOM-7062
COMM-PIOM-7064	COMM-PIOM-4061	COMM-PIOM-5050
COMM-PIOM-5062	COMM-PIOM-7061	COMM-PIOM-7060
COMM-PIOM-6060	COMM-PIOM-6061	COMM-PIOM-5061
COMM-PIOM-6050	COMM-PIOM-6051	COMM-PIOM-6062
COMM-PIOM-7050		

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-4040: Establish data network services

SUPPORTED MET(S): 3, 4, 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: The Section will employ data network resources IAW the Data Network Plan utilizing all necessary support assets. Examples of successful tasks include the installation of switches, routers, servers and boundary protection devices to provide access to secure/non-secure email, web browsing and other required data network services.

CONDITION: Given a command's mission, a data network plan, all equipment and personnel, an approved certification and accreditation package, and an existing digital backbone.

STANDARD: Within 48 hours to satisfy the commanders information exchange requirements.

EVENT COMPONENTS:

1. Install network architecture.
2. Implement computer network defense.
3. Install network services.
4. Provide end user support.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-4030: Install trunked telephony services.

SUPPORTED MET(S): 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: The section will IOM all telephony services IAW the telephone network plan utilizing all necessary support assets. Examples of successful tasks are establishing secure and non-secure call processing in a stand alone or stacked architecture.

CONDITION: Given a command's mission, telephone network plan, all equipment and personnel.

STANDARD: Within 4 hours of establishment of an integrated network that satisfies the commanders information exchange requirements.

EVENT COMPONENTS:
1. Validate cutsheets.
2. Program switchboard trunk.
3. Configure media gateway.
4. Configure multiplexing device or router.
5. Verify trunk connectivity.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-4004: Establish a terrestrial multi-channel SHF radio link

SUPPORTED MET(S): 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: The section will IOM terrestrial multi-channel SHF radio links IAW the radio network plan utilizing all necessary support assets. Examples of successful tasks include multi-channel order wire communications and transmission systems signal quality levels that support data exchange.

CONDITION: Given a command's mission, radio network plan, and all equipment and personnel.

STANDARD: Within 2 hours at a signal quality level sufficient to support data exchange.

EVENT COMPONENTS:
1. Validate cutsheets.
2. Establish terrestrial multi-channel radio site.
3. Engineer radio link.
4. Verify received signal level.
5. Verify bit error rate.

CHAINED EVENTS:
COMM-PIOM-3003

REFERENCES:
1. CEOI Communications-Electronic Operating Instructions
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. Joint Pub 6-0 Joint Communications System, 10 June 2010.
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-4003: Establish a terrestrial multi-channel UHF radio link.

SUPPORTED MET(S): 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: The section will IOM terrestrial multi-channel UHF radio links IAW the radio network plan utilizing all necessary support assets. Examples of successful tasks include multi-channel order wire communications and transmission systems signal quality levels that support data exchange.

CONDITION: Given a command's mission, radio network plan, and all equipment and personnel.

STANDARD: Within 2 hours at a signal quality level sufficient to support data exchange.

EVENT COMPONENTS:
1. Validate cutsheets.
2. Establish terrestrial multi-channel radio site.
3. Engineer radio link.
4. Verify received signal level.
5. Verify bit error rate.

CHAINED EVENTS: COMM-PIOM-3003

REFERENCES:
1. CEOI Communications-Electronic Operating Instructions
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. Joint Pub 6-0 Joint Communications System, 10 June 2010.
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

3007. 3000-LEVEL EVENTS

COMM-PIOM-3060: Provide communications services for rapid response

SUPPORTED MET(S): 2, 3, 4, 5, 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: The teams will IOM all required communication and support assets IOT provide secure/non-secure voice, video, data and real-time services that support general officer, crisis response, and assessment team communications requirements.

CONDITION: Given a mission and required equipment and personnel.

STANDARD: Within a timeline allotted by the commander to satisfy information exchange requirements.

EVENT COMPONENTS:
1. Receive warning order.
2. Embark equipment.
3. Deploy
4. Provide voice, video, data and real-time communications services.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-3020: Establish Video Teleconferencing services

SUPPORTED MET(S): 3, 5

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: VTC is considered a real-time service and is employed to support the commanders information exchange requirements. VTC suites are not standardized. Examples of successful tasks include a secure/non-secure ISDN dial-up, serial port, and IP based capability depending upon the planned network.

CONDITION: Given a Real-time Services Plan, required equipment and personnel, and an existing transmission path.

STANDARD: Within 24 hours, with the Quality of Service required to satisfy the commanders information exchange requirements.

EVENT COMPONENTS:
1. Coordinate VTC protocol with service provider.
2. Install VTC terminal
3. Establish secure VTC services.

4. Establish non-secure VTC services.
5. Establish call.
6. Provide end user support.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-3010: Establish a multiplexed architecture

SUPPORTED MET(S): 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: The team will IOM all multiplexed networks utilizing all necessary support assets. Examples of successful tasks are link synchronization of point-to-point and multi-point multiplexed circuits.

CONDITION: Given a Multiplexing Plan, all required equipment and personnel, an approved timing source, and a transmission path.

STANDARD: Within 12 hours, to extend communications circuits and satisfy the commanders information exchange requirements.

EVENT COMPONENTS:
1. Establish a point-to-point multiplexing network.
2. Establish a point-to-multi-point multiplexing network.
3. Distribute circuits to appropriate network devices.
4. Validate network timing scheme.
5. Validate cut sheets.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

COMM-PIOM-3003: Establish a multi-channel radio site

SUPPORTED MET(S): 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: The Team will install a multi-channel radio site IAW the Radio Network Plan utilizing all necessary support assets. A multi-channel radio site includes the physical layout and the initial configuration of the multi-channel radio. Team members will ensure site survey guidelines are enforced. An example of a successful task includes a multi-channel radio site that meets all functional and safety parameters.

CONDITION: Provided a command's mission, a Radio Network Plan, and all required equipment and personnel.

STANDARD: In the time allotted by the commander.

EVENT COMPONENTS:
1. Configure equipment.
2. Execute mission.
3. Conduct time critical ORM.
4. Validate the site plan.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. Joint Pub 6-02 Joint Doctrine for the Employment of Operational/Tactical Command, Control, Communications and Computer Systems
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-3002: Employ a satellite terminal

SUPPORTED MET(S): 2, 6

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: The Team will install a satellite terminal IAW the Radio Network Plan utilizing all necessary support assets. Team members will ensure site survey guidelines and SAA parameters are enforced. An example of a successful task is a site includes the physical layout, the initial configuration of the terminal satellite terminal, establishment of links (e.g. point to point, point to multi-point, hub-spoke, hybrid-mesh) site that meets all functional and safety parameters.

CONDITION: Provided a command's mission, Radio Network Plan, Satellite Access Authorization (SAA), cut sheets, and all required equipment and personnel.

STANDARD: Within 2 hours, with signal quality level that supports data exchange.

EVENT COMPONENTS:
1. Conduct time critical ORM.
2. Validate the site plan.
3. Coordinate with service provider.
4. Configure terminal.
5. Establish link(s).
6. Verify signal quality.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM-PIOM-3001: Establish a single channel radio site

SUPPORTED MET(S): 2

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 2 months

DESCRIPTION: The Team will install a single channel radio site IAW the Radio Network Plan utilizing all necessary support assets. A single channel radio site includes the physical layout and the initial configuration of all single channel radio and retransmission assets. Team members will ensure site survey guidelines are enforced. An example of a successful task includes a single channel radio site that meets all functional and safety parameters.

CONDITION: Provided a commands mission, a Radio Network Plan, and all required equipment and personnel.

STANDARD: In the time allotted by the commander.

EVENT COMPONENTS:
1. Conduct time critical ORM.
2. Validate the site plan.
3. Configure equipment.
4. Execute mission.

CHAINED EVENTS:
0621-OPER-2501 0621-INST-2401

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. Joint Pub 6-0 Joint Communications System, 10 June 2010.
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. UNIT SOP Unit's Standing Operating Procedures

COMM T&R MANUAL

CHAPTER 4

INDIVIDUAL EVENTS

CHAPTER 4

INDIVIDUAL EVENTS

4000. PURPOSE. The purpose of 1000-Level individual training is to provide the knowledge and skills necessary to perform the basic skills of any MOS. 2000-Level training is received either MOJT or at advanced level and career progression schools.

4001. INDIVIDUAL SKILLS

1. Core Skills are basic individual skills that make a Marine and qualify them for an MOS. They are the 1000 level skills introduced in the entry level training in the formal schools and refined in operational units.

2. Core Plus Skills are advance individual skills that are environment, mission, rank, or billet specific. They are the 2000 level skills introduced in the entry level managed on the job training in operational units and advanced formal schools training.

4002. EVENT CODING. Events in the T&R Manual are depicted with an up to 12 field alphanumeric system, i.e. XXXX-XXXX-XXXX. All individual events use the following methodology:

a. Field one – Each event starts with 06XX. 0600 indicates that the event is a core capability for all Marines within the occupational field. 0659 indicates that the event is for a Data Chief, etc.

b. Field two – This field is alpha characters indicating a functional area. The individual event functional areas are listed below:

Functional Area	Field Name	Example
Plan	PLAN	0699-PLAN-1101
Design	DSGN	0620-DSGN-1207
Engineer	ENGR	0610-ENGR-2304
Install	INST	0651-INST-1401
Operate	OPER	0621-OPER-2505
Maintain	MANT	0611-MANT-2608
Manage	MNGT	0629-MNGT-1703
Protect	PROT	0689-PROT-1802

c. Field three – This field provides numerical sequencing as well as represents the level of the event. All individual events are either 1000-level events that are taught at MOS-producing formal schools or 2000-level events that are taught at advanced-level schools or are MOJT. The first digit of this field indicates whether it is a core (1) or core plus (2) event. The second digit indicates the associated functional area, and the last two digits indicate the task number. For example, 2305 indicates that this is a core plus task and it is the fifth task within the Engineer

functional area for that MOS. More information on event levels and sequencing can be found in paragraph 1005 of chapter one.

4003. ADMINISTRATIVE NOTES. Each event may contain a paragraph that describes support requirements Marines will need to complete the event. Such support requirements could include equipment, materials, ammunition, or any other external or internal support that may be required to complete the event.

COMM T&R MANUAL

CHAPTER 5

MOS 0600 INDIVIDUAL EVENTS

CHAPTER 5

MOS 0600 INDIVIDUAL EVENTS

5000. INDEX OF INDIVIDUAL EVENTS

5001. 1000-LEVEL EVENTS

0600-INST-1401: Install a power source

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0600, 0612, 0613, 0621, 0622, 0623, 0627, 0651, 0652, 0653, 0689

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided power source, equipment, and references.

STANDARD: Ensuring the equipment is properly powered and grounded, and per MIL-HDBK-419.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify applicable power source.
3. Execute Installation.
4. Ground equipment.
5. Turn on equipment.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MIL-HDBK 419_ Grounding Techniques

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Power source

0600-MANT-1601: Maintain Communications Equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0600, 0612, 0613, 0621, 0622, 0623, 0627, 0651, 0652, 0653

GRADES: PVT, PFC, LCPL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided preventive maintenance documents, equipment, and technical manuals (TM).

STANDARD: Ensuring the equipment is clean, rust free, SL-3 complete, and operational.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Conduct Stock List-3 (SL-3) inventory.

3. Inspect equipment.
4. Execute PM checklist.
5. Conduct an operational check.
6. Complete equipment records.
7. Report discrepancies.
8. Document authorized maintenance.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MCO P4790.1B Marine Corps Integrated Maintenance Management System (MIMMS) Introduction Manual (Mar 89)
3. MCO P4790.2_ MIMMS Field Procedures Manual
4. TM 4700-15/1_ Ground Equipment Record Procedures

0600-PROT-1801: Perform Information Assurance Technician (IAT) level I duties.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Technician Level I personnel make the CE less vulnerable by correcting flaws and implementing IAT controls in the hardware or software installed within their operational systems. The CE is defined as local area network(s) server host and its operating system, peripherals and applications.

BILLETS: Information Assurance Technician (IAT) level I

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a computing environment and IA directives.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of information, information systems, and information infrastructures.

PERFORMANCE STEPS:
1. Recognize a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact.
2. Apply instructions and pre-established guidelines to perform IA tasks within CE.
3. Provide end user IA support for all CE operating systems, peripherals, and applications.
4. Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to their CE.
5. Apply CE specific IA program requirements to identify areas of weakness.
6. Apply appropriate CE access controls.
7. Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.

8. Conduct tests of IA safeguards in accordance with established test plans and procedures.
9. Implement and monitor IA safeguards for CE system(s) in accordance with implementation plans and standard operating procedures.
10. Apply established IA security procedures and safeguards and comply with responsibilities of assignment.
11. Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.
12. Implement online warnings to inform users of access rules for CE systems.
13. Implement applicable patches including IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for the CE operating system(s).
14. Understand and implement technical vulnerability corrections.
15. Enter assets in a vulnerability management system.
16. Apply system security laws and regulations relevant to the CE being supported.
17. Implement DoD and DoD Component password policy.
18. Implement specific IA security countermeasures.
19. Obtain and maintain IA certification appropriate to position.

REFERENCES:

1. DoD 8570.01-M Information Assurance Workforce Improvement Program Incorporating Change 2,April 20, 2010
2. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
3. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES). Appropriate certification must be obtained within 6 months of assuming IAT billet.

SPECIAL PERSONNEL CERTS: One of the following: 1. Computing Technology Industry Association (CompTIA) A+ Certification. 2. Computing Technology Industry Association (CompTIA) Network+ Certification. 3. International Information Systems Security Certifications Consortium (ISC)2 System Security Certified Practitioner (SSCP). 4. Appropriate operating systems cert (CHECK 8570).

5002. 2000-LEVEL EVENTS

0600-PLAN-2101: Supervise embarkation of communications assets.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT, MAJ

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, equipment, personnel, and references.

STANDARD: Ensuring equipment is properly marked, stored, and accounted for during all phases of the embarkation and debarkation of equipment.

PERFORMANCE STEPS:
1. Identify equipment requirements.
2. Prioritize equipment to be embarked and debarked.
3. Identify embark method.
4. Maintain equipment accountability.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. MCO P4600.7C USMC Transportation Manual
3. NWP 22-26 Communications Planning - Embarkation

0600-OPER-2501: Implement a communications equipment embarkation plan.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612, 0613, 0621, 0622, 0623, 0627, 0651, 0681, 0689

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided embarkation documents, equipment, and references.

STANDARD: Ensuring the items on the Equipment Density List (EDL) are properly marked and prepared for embarkation, per the references.

PERFORMANCE STEPS:
1. Adhere to all safety precautions.
2. Review unit embarkation SOP.
3. Ensure manifests are correct.
4. Submit data to Embarkation Officer.
5. Ensure equipment, boxes, pallets, and vehicles are marked and waterproofed.
6. Conduct safety and load inspections of all vehicles.
7. Ensure arrangements have been made to store classified material.
8. Ensure hazardous materials are packaged, marked, and documented.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

0600-OPER-2502: Implement an emergency action plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0602, 0610, 0612, 0613, 0619, 0620, 0621, 0622, 0623, 0627, 0629, 0640, 0648, 0650, 0651, 0652, 0653, 0659, 0681, 0689, 0699

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT, MSGT, WO-1, CWO-2, 2NDLT, 1STLT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided equipment, references, and given the order to execute.

STANDARD: To destroy or safeguard all COMSEC material depending on the situation, per the references.

PERFORMANCE STEPS:
1. Adhere to all safety precautions.
2. Receive the instructions.
3. Review the plan.
4. Execute the plan.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. MCO 3500.27_ Operational Risk Management (ORM)
3. UNIT SOP Unit's Standing Operating Procedures

0600-OPER-2503: Operate a Command and Control (C2) streaming information system.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: This task encompasses the operation of assets that disseminate real time streaming video services.

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: In order to receive streaming video that supports C2 requirements.

PERFORMANCE STEPS:
1. Perform equipment setup procedures.

2. Operate a receive terminal.
3. Operate a receive broadcast manager.
4. Execute the plan.

0600-OPER-2504: Operate a High Mobility Multipurpose Wheeled Vehicle (HMMWV).

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

DESCRIPTION: This event is designed for communications Marines that are required to operate a HMMWV.

MOS PERFORMING: 0612, 0621, 0622, 0623, 0627, 0651

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided with applicable references, operational motor transport assets (M-Series Vehicle), forms and required tools and equipment.

STANDARD: Demonstrating a working knowledge and familiarization of the vehicle's mechanical operation while observing safe driving procedures.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Prepare operational forms and records.
3. Inventory vehicle.
4. Conduct Preventive Maintenance Checks and Services (PMCS).
5. Attach trailer to vehicle as applicable.
6. Start the engine.
7. Drive the vehicle under normal conditions as applicable.
8. Drive the vehicle off-road as applicable.
9. Drive the vehicle under administrative conditions as applicable.
10. Drive the vehicle under limited vision conditions as applicable.
11. Drive the vehicle under unusual conditions as applicable.
12. Drive the vehicle with towed load as applicable.
13. Park the vehicle.
14. Employ the emergency brake.
15. Turn off the engine.
16. Complete operational forms and records.

REFERENCES:
1. FM 21-305 Manual for Wheeled Vehicle Driver
2. FM 55-30 Army Motor Transport Units and Operations
3. FMFM 4-9 Motor Transport
4. MCO 3500.27_ Operational Risk Management (ORM)

0600-MANT-2601: Induct communications equipment into the maintenance cycle

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0612, 0613, 0621, 0622, 0623, 0627, 0651, 0689

GRADES: LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment and references.

STANDARD: In accordance with Units Maintenance SOP.

PERFORMANCE STEPS:
1. Identify faulty equipment.
2. Perform operational check.
3. Record suspected defect.
4. Ensure an Equipment Record Order (ERO) is properly filled in and opened.
5. Induct equipment into maintenance cycle.
6. File the ERO in the equipment record jacket.
7. Track maintenance process.
8. Close the ERO when maintenance is completed.
9. Place a copy of the closed-out ERO in the Equipment Record Jacket.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MCO P4400.150_ Consumer Level Supply Policy Manual
3. MCO P4790.1B Marine Corps Integrated Maintenance Management System (MIMMS) Introduction Manual (Mar 89)
4. UNIT SOP Unit's Standing Operating Procedures

0600-MNGT-2701: Manage Resource Readiness

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0619, 0629, 0659, 0681, 0689, 0699

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's Mission Essential Task List, Training Exercise and Employment Plan, Table of Organization and Equipment, resource readiness documents, and mission.

STANDARD: To ensure resource availability to satisfy the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine equipment resources.
2. Organize equipment resources.
3. Determine logistical requirements.
4. Determine equipment readiness.
5. Supervise equipment maintenance.
6. Maintain equipment accountability.

7. Identify personnel resources.
8. Organize personnel resources.

REFERENCES:
1. MCO P4790.2_ MIMMS Field Procedures Manual
2. MCRP 3-0A Unit Training Management Guide
3. MCWP 4-11 Combat Service Support

0600-MNGT-2702: Manage a training program

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 1 month

GRADES: SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, Commander's guidance, and references.

STANDARD: To ensure all required training is completed to maintain unit readiness.

PERFORMANCE STEPS:
1. Use a T&R Manual.
2. Conduct a Training Assessment.
3. Determine a Training Strategy.
4. Develop a Short Range Training Plan.
5. Develop Training Schedules.
6. Develop a Training Scenario.
7. Coordinate Unit Training.
8. Conduct Operational Risk Assessment.
9. Create a Performance Evaluation Checklist.
10. Prepare for Training.
11. Conduct Training.
12. Evaluate Training.
13. Conduct After Action Reviews.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MCRP 3-0A Unit Training Management Guide
3. MCRP 3-0B How to Conduct Training

0600-MNGT-2703: Manage a Communications Network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Systems Control (SYSCON) represents current operations and day-to-day management of the operational communications network. The SYSCON serves as the focal point for information regarding the health of the current network, maximizes the effectiveness of communications resources to meet operational demands, and remedies deficiencies and outages.

MOS PERFORMING: 0619, 0629, 0659

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To support secure and non-secure voice, data and special circuits.

PERFORMANCE STEPS:
1. Maintain situational awareness of the communications network.
2. Monitor system performance.
3. Analyze traffic data to gauge network viability.
4. Conduct quality tests to gauge network viability.
5. Comply with direction from higher Communications Control agencies.
6. Supervise the execution of communications plans.
7. Supervise the execution of technical directives.
8. Supervise the execution of operational directives.
9. Provide direction to the local and the subordinate Communications Control agencies.
10. Coordinate with external Communications Control agencies as required.
11. Coordinate actions for service installation.
12. Coordinate actions for service restoration.
13. Supervise emergency adjustments to the communications network as required.
14. Maintain information management products related to the communications network.
15. Distribute information management products related to the communications network.
16. Manage reporting from subordinate Communications Control agencies.
17. Manage reporting to higher Communications Control agencies.
18. Recommend corrective actions for network adjustments.
19. Ensure network-wide compliance with applicable security directives.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. CJCSM 6231.01C Manual for Employing Joint Tactical Communications (Joint Systems Management)
3. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
4. CJCSM 6231.03B Manual for the Employment of Joint Tactical Communications (Joint Data Systems)
5. CJCSM 6231.04A Manual for the Employment of Joint Tactical Communications (Joint Transmission Systems)
6. CJCSM 6231.05B Manual for the Employment of Joint Tactical Communications (Joint Communications Security)
7. CJCSM 6231.06B Manual for the Employment of Joint Tactical Communications (Joint Technical Control Procedures and Systems)
8. CJCSM 6231.07D Manual for the Employment of Joint Tactical Communications (JOINT NETWORK Management and CONTROL)
9. MCO 3500.27_ Operational Risk Management (ORM)
10. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
11. UNIT SOP Unit's Standing Operating Procedures

0600-PROT-2801: Safeguard Communications Security (COMSEC) Material

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided CMS documents, equipment, and security measures.

STANDARD: Ensuring 100% accountability and proper handling of COMSEC material and equipment.

PERFORMANCE STEPS:
1. Identify COMSEC material.
2. Receive COMSEC material.
3. Know and adhere to the minimum control requirements for COMSEC material.
4. Know and adhere to the access requirements for keyed and unkeyed Controlled Cryptographic Items (CCI), to include access by U.S. and Non-U.S. citizens and Contractors.
5. Know the modes of transportation authorized for shipping and transporting COMSEC material.
6. Know the inventory/accounting requirements associated with COMSEC material held.
7. Issue COMSEC material as applicable (Local Element Issuing only).
8. Store COMSEC material.
9. Destroy COMSEC material.
10. Report a COMSEC incident.

REFERENCES:
1. CJCSM 6231.05B Manual for the Employment of Joint Tactical Communications (Joint Communications Security)
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. EKMS-3 (series) EKMS Inspection Manual
4. EKMS-5A Cryptographic Equipment Information/Guidance Manual
5. NAG-14_ Safeguarding COMSEC Material and Facilities
6. OPNAVINST 2201.3 COMSEC Monitoring
7. SECNAVINST 5510.30_ Dept of Navy Personnel Security Program
8. SECNAVINST 5510.36_ Dept of the Navy Information and Personnel Security Program Regulations

SUPPORT REQUIREMENTS:

EQUIPMENT: GSA approved security container or High Security Padlock

MATERIAL: SF-700, Security Container Information Envelope

0600-PROT-2802: Perform Information Assurance Technician (IAT) level II duties.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Technician Level II personnel provide NE and advanced level CE support. They pay special attention to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. These positions focus on threats and vulnerabilities and improve the security of systems. IAT Level II personnel have mastery of the functions of the IAT Level I position. The NE is defined as the constituent element of an enclave responsible for connecting CE by providing short haul data transport capabilities, such as local or campus area networks, or long haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks that provides for the application of IA controls.

BILLETS: Information Assurance Technician (IAT) level II

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a Networking environment and IA directives.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Demonstrate expertise in IAT Level I CE knowledge and skills.
2. Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence.
3. Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the NE.
4. Recommend and schedule IA related repairs in the NE.
5. Perform IA related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE.
6. Provide end user support for all IA related applications for the NE.
7. Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.
8. Manage accounts, network rights, and access to NE systems and equipment.
9. Analyze system performance for potential security problems.
10. Assess the performance of IA security controls within the NE.
11. Identify IA vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing.
12. Provide leadership and direction to IA operations personnel.
13. Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
14. Install, test, maintain, and upgrade network operating systems software and hardware to comply with IA requirements.
15. Evaluate potential IA security risks and take appropriate corrective and recovery action.
16. Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
17. Diagnose and resolve IA problems in response to reported incidents.

18. Research, evaluate, and provide feedback on problematic IA trends and patterns in customer support requirements.
19. Ensure IAT Level I personnel are properly trained and have met OJT program requirements.
20. Perform system audits to assess security related factors within the NE.
21. Develop and implement access control lists on routers, firewalls, and other network devices.
22. Install perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
23. Work with other privileged users to jointly solve IA problems.
24. Write and maintain scripts for the NE.
25. Demonstrate proficiency in applying security requirements to an operating system for the NE or CE used in their current position.
26. Implement applicable patches including IAVAs, IAVBs, and TAs for their NE.
27. Adhere to IS security laws and regulations to support functional operations for the NE.
28. Implement response actions in reaction to security incidents.
29. Support the design and execution of exercise scenarios.
30. Support Security Test and Evaluations (Part of Certification and Accreditation(C&A) Process).
31. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
2. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
3. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES). Appropriate certification must be obtained within 6 months of assuming IAT billet.

SPECIAL PERSONNEL CERTS: One of the following: 1. Computing Technology Industry Association (CompTIA) Security + Certification. 2. Security Certified Program Security Certified Network Professional (SCNP). 3. International Information Systems Security Certifications Consortium (ISC) 2 System Security Certified Practitioner (SSCP). 4. Global Information Assurance Certification (GIAC) GIAC Security Essentials Certification (GSEC). 5. Appropriate operating systems cert

---

0600-PROT-2803: Perform Information Assurance Technician (IAT) level III duties.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Technician Level III personnel focus on the enclave environment and support, monitor, test, and

troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments. IAT Level III personnel have mastery of the functions of both the IAT Level I and Level II positions. An enclave is defined as a collection of CE connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems. Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

BILLETS: Information Assurance Technician (IAT) level III

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a enclave environment and IA directives.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Mastery of IAT Level I and IAT Level II CE/NE knowledge and skills.
2. Recommend and schedule IA related repairs within the enclave environment.
3. Coordinate and ensure end user support for all enclave applications and operations.
4. Lead teams to quickly and completely solve IA problems for the enclave environment.
5. Formulate or provide input to the enclave's IA/IT budget.
6. Plan and schedule the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave.
7. Determine whether a security incident is indicative of a violation of law that requires specific legal action.
8. Direct the implementation of appropriate operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
9. Provide direction to system developers regarding correction of security problems identified during testing.
10. Evaluate functional operation and performance in light of test results and make recommendations regarding C&A.
11. Examine enclave vulnerabilities and determine actions to mitigate them.
12. Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards.
13. Analyze IA security incidents and patterns to determine remedial actions to correct vulnerabilities.
14. Develop the enclave termination plan to ensure that IA security incidents are avoided during shutdown and long term protection of archived resources is achieved.

15. Develop and apply effective vulnerability countermeasures for the enclave.
16. Develop and manage IA customer service performance requirements.
17. Develop IA related customer support policies, procedures, and standards.
18. Write and maintain scripts required to ensure security of the enclave environment.
19. Design perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., enhance rule sets to block sources of malicious traffic, and establish a protective net of layered filters to prevent, detect, and eradicate viruses.
20. Schedule and perform regular and special backups on all enclave systems.
21. Establish enclave logging procedures to include: important enclave events; services and proxies; log archiving facility.
22. Provide OJT for IAT Level I and II DoD personnel.
23. Analyze IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and take or recommend appropriate action.
24. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
2. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
3. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: One of the following: 1. Information Systems Audit and Control Association (ISACA) Certified Information Security Auditor (CISA) Certification. 2. Security Certified Program Security Certified Network Architect (SCNA). 3. Global Information Assurance Certification (GIAC) GIAC Security Expert (GSE). 4. International Information Systems Security Certifications Consortium (ISC) 2 Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience) Certification.

0600-PROT-2804: Perform Information Assurance Manager (IAM) Level I duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Management Level I personnel are responsible for the implementation and operation of a DoD IS or system DoD Component within their CE regardless of their occupational title. Incumbents ensure that IA related IS are functional and secure within the CE. The CE is defined as local area network(s) server host and its operating system, peripherals and applications.

BILLETS: Information Assurance Manager (IAM) Level I

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5, 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a computing environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of information, information systems, and information infrastructures.

PERFORMANCE STEPS:
1. Adhere to HQMC C4 IA Directives.
2. Provide system related input on IA security requirements.
3. Ensure data retention and recovery within the CE.
4. Coordinate with higher headquarters IAM in the development or modification of the computer environment IA security program plans and requirements.
5. Ensure CE users meet systems authorization access requirements.
6. Recognize security violations.
7. Report security violations.
8. Supervise corrective measures to IA vulnerabilities.
9. Supervise the adherence of system security configuration guidelines.
10. Comply with IA security requirements in a CE.
11. Coordinate IA inspections, tests, and reviews.
12. Participate in the Certification and Accreditation process.
13. Collect data for IA reporting requirements.
14. Within six months of being assigned to an IAM Level I billet, obtain IA certification appropriate to position.
15. Maintain IA Certification appropriate to position.

REFERENCES:
1. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
2. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
3. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or The Marine Corps Communications Electronics School (MCCES). Appropriate certification must be obtained within 6 months of assuming IAM billet.

SPECIAL PERSONNEL CERTS: One of the following: 1. Computing Technology Industry Association (CompTIA) Security + Certification. 2. Global Information Assurance Certification (GIAC) GIAC Security Leadership Certificate (GSLC) Certification. 3. Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM) Certification. International Information Systems Security Certifications Consortium (ISC) 2

0600-PROT-2805: Perform Information Assurance Manager (IAM) Level II duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Management Level II personnel are responsible for the IA program of an IS within the NE. Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the NE. The NE is defined as the constituent element of an enclave responsible for connecting CE by providing short haul data transport capabilities, such as local or campus area networks, or long haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks that provides for the application of IA controls.

BILLETS: Information Assurance Manager (IAM) Level II

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a networking environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:
1. Adhere to HQMC C4 IA Directives.
2. Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for the NE.
3. Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
4. Develop NE security requirements specific to an IT acquisition for inclusion in procurement documents.
5. Recommend resource allocations required to securely operate and maintain an organizations NE IA requirements.
6. Participate in an IS risk assessment during the C&A process.
7. Develop security requirements for hardware, software, and services acquisitions specific to NE IA security programs.
8. Ensure that IA and IA enabled software, hardware, and firmware comply with appropriate NE security configuration guidelines, policies, and procedures.
9. Assist in the gathering and preservation of evidence used in the prosecution of computer crimes.
10. Ensure that NE IS recovery processes are monitored and that IA features and procedures are properly restored.
11. Review IA security plans for the NE.
12. Ensure that all IAM review items are tracked and reported.
13. Identify alternative functional IA security strategies to address organizational NE security concerns.
14. Ensure that IA inspections, tests, and reviews are coordinated for the NE.

15. Review the selected security safeguards to determine that security concerns identified in the approved plan have been fully addressed.
16. Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
17. Monitor contract performance and periodically review deliverables for conformance with contract requirements related to NE IA, security, and privacy.
18. Provide leadership and direction to NE personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.
19. Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow NE and IA policies and procedures.
20. Advise the DAA of any changes affecting the NE IA posture.
21. Conduct an NE physical security assessment and correct physical security weaknesses.
22. Help prepare IA certification and accreditation documentation.
23. Ensure that compliance monitoring occurs, and review results of such monitoring across the NE.
24. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
2. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
3. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: One of the following: 1. Global Information Assurance Certification (GIAC) GIAC Security Leadership Certificate (GSLC) Certification. 2. Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM) Certification. International Information Systems Security Certifications Consortium (ISC) 3. Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience) Certification.

0600-PROT-2806: Perform Information Assurance Manager (IAM) Level III duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Management Level III personnel are responsible for ensuring that all enclave IS are functional and secure. They determine the enclaves long term IA systems needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through

the DoD certification and accreditation process. An enclave is defined as a collection of CE connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in OMB A-130 (Reference (il)). Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

BILLETS: Information Assurance Manager (IAM) Level III

GRADES: GYSGT, MSGT, MGYSGT, CWO-3, CWO-4, CWO-5, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a enclave environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enclave.
2. Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with DoD Component level IA architecture.
3. Ensure IAT Levels I, II, and III, IAM Levels I and II, and anyone with privileged access performing IA functions receive the necessary initial and sustaining IA training and certification(s) to carry out their IA duties.
4. Prepare or oversee the preparation of IA certification and accreditation documentation.
5. Participate in an IS risk assessment during the C&A process.
6. Ensure information ownership responsibilities are established for each DoD IS and implement a role based access scheme.
7. Analyze, develop, approve, and issue enclave IA policies.
8. Evaluate proposals to determine if proposed security solutions effectively address enclave requirements, as detailed in solicitation documents.
9. Identify IT security program implications of new technologies or technology upgrades.
10. Evaluate cost benefit, economic and risk analysis in decision making process.
11. Interpret and/or approve security requirements relative to the capabilities of new information technologies.
12. Interpret patterns of non compliance to determine their impact on levels of risk and/or overall effectiveness of the enclave's IA program.
13. Analyze identified security strategies and select the best approach or practice for the enclave.
14. Ensure that security related provisions of the system acquisition documents meet all identified security needs.

15. Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
16. Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
17. Take action as needed to ensure that accepted products meet Common Criteria requirements as stated in Reference DoDD 8500.2
18. Monitor and evaluate the effectiveness of the enclaves IA security procedures and safeguards to ensure they provide the intended level of protection.
19. Provide enclave IA guidance for development of the COOP.
20. Ensure all IAM review items are tracked and reported.
21. Advise the DAA of changes affecting the enclave's IA posture.
22. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
2. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
3. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
4. DoDI 8500.2 Information Assurance (IA) Implementation

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: One of the following: 1. Global Information Assurance Certification (GIAC) GIAC Security Leadership Certificate (GSLC) Certification. 2. Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM) Certification. International Information Systems Security Certifications Consortium (ISC) 2. 3. Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience) Certification.

0600-PROT-2807: Perform Information Assurance System Architect and Engineer (IASAE) level I duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, IASAE Level I personnel are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within their CE. Incumbents ensure that IA related IS will be functional and secure within the CE.

MOS PERFORMING: 0610, 0620, 0650, 0689

BILLETS: System Architect and Engineer (IASAE) Level I

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a computing environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Identify information protection needs for CE system(s) and network(s).
2. Define CE security requirements in accordance with applicable IA requirements (e.g., DoDD 8500.2, DCID 6/3), and organizational security policies).
3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
4. Design security architectures for CE system(s) and network(s).
5. Design and develop IA or IA-enabled products for use within a CE.
6. Integrate and/or implement Cross Domain Solutions (CDS) for use within a CE.
7. Design, develop, and implement security designs for new or existing CE system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the CE.
8. Design, develop, and implement system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
9. Develop and implement specific IA countermeasures for the CE.
10. Develop interface specifications for CE system(s).
11. Develop approaches to mitigate CE vulnerabilities, recommend changes to system or system components as needed.
12. Ensure that system designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
13. Develop IA architectures and designs for DoD IS with basic integrity and availability requirements, to include MAC III systems as defined in DoDI 8500.2 and DoDD 8500.1; systems with a Basic Level-of-Concern for availability or integrity in accordance with DCID 6/3; and other DAA designated systems.
14. Develop IA architectures and designs for systems processing Sensitive Compartmented Information (SCI) that will operate at Protection Level 1 or 2 as defined in DCID 6/3.
15. Assess threats to and vulnerabilities of CE system(s).
16. Identify, assess, and recommend IA or IA-enabled products for use within a CE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of DoDI 8500.2 and DoDD 8500.1.
17. Ensure that the implementation of security designs properly mitigate identified threats.
18. Assess the effectiveness of information protection measures utilized by CE system(s).
19. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
20. Provide input to IA C&A process activities and related documentation (system life-cycle support plans, concept of operations, operational procedures and maintenance training materials, etc.).

21. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
22. Provide engineering support to security/certification test and evaluation activities.
23. Document system security design features and provide input to implementation plans and standard operating procedures.
24. Recognize a possible security violation and take appropriate action to report the incident.
25. Implement and/or integrate security measures for use in CE system(s) and ensure that system designs incorporate security configuration guidelines.
26. Ensure the implementation of CE IA policies into system architectures.
27. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. Director of Central Intelligence Directive (DCID) 6/3 Protecting Sensitive Compartmented Information within Information Systems.
2. DoDD 8500.1 Information Assurance (IA)
3. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
4. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
5. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
6. DoDI 8500.2 Information Assurance (IA) Implementation

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: 1. International Information Systems Security Certifications Consortium (ISC)2 Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience) Certification.

0600-PROT-2808: Perform Information Assurance System Architect and Engineer (IASAE) Level II duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, IASAE Level II positions are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within the NE. Incumbents ensure that IA related IS will be functional and secure within the NE.

MOS PERFORMING: 0610, 0620, 0650, 0689

BILLETS: System Architect and Engineer (IASAE) Level II

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a Network environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Identify information protection needs for the NE.
2. Define NE security requirements in accordance with applicable IA requirements (DoDI 8500.2 and DCID 6/3 and organizational security policies).
3. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
4. Design security architectures for use within the NE.
5. Design and develop IA or IA-enabled products for use within a NE.
6. Integrate and/or implement CDS for use within a CE or NE.
7. Develop and implement security designs for new or existing network system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the NE.
8. Design, develop, and implement network security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.
9. Design, develop, and implement specific IA countermeasures for the NE.
10. Develop interface specifications for the NE.
11. Develop approaches to mitigate NE vulnerabilities and recommend changes to network or network system components as needed.
12. Ensure that network system(s) designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
13. Develop IA architectures and designs for DoD IS with medium integrity and availability requirements, to include MAC II systems as defined in DoDI 8500.2 and DoDD 8500.1, systems with a medium Level-of-Concern for availability or integrity in accordance with DCID 6/3, and other DAA designated systems.
14. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 1 or 2 as defined in DCID 6/3.
15. Assess threats to and vulnerabilities of the NE.
16. Identify, assess, and recommend IA or IA-enabled products for use within an NE; ensure recommended products are in compliance with the DoD evaluation and validation requirements of DoDI 8500.2 and DoDD 8500.1.
17. Ensure that the implementation of security designs properly mitigate identified threats.
18. Assess the effectiveness of information protection measures used by the NE.
19. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.
20. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.

21. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
22. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
23. Provide engineering support to security/certification test and evaluation activities.
24. Document system security design features and provide input to implementation plans and standard operating procedures.
25. Recognize a possible security violation and take appropriate action to report the incident.
26. Implement and/or integrate security measures for use in network system(s) and ensure that system designs incorporate security configuration guidelines.
27. Ensure the implementation of NE IA policies into system architectures.
28. Ensure the implementation of subordinate CE IA policies is integrated into the NE system architecture.
29. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. Director of Central Intelligence Directive (DCID) 6/3 Protecting Sensitive Compartmented Information within Information Systems.
2. DoDD 8500.1 Information Assurance (IA)
3. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
4. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
5. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
6. DoDI 8500.2 Information Assurance (IA) Implementation

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: 1. International Information Systems Security Certifications Consortium (ISC) 2 Certified Information Systems Security Professional (CISSP) (or Associate - this means the individual has qualified for the certification except for the number of years experience) Certification.

0600-PROT-2809: Perform Information Assurance System Architect and Engineer (IASAE) Level III Duties

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, IASAE Level III positions are responsible for the design, development, implementation, and/or integration of a DoD IA architecture, system, or system component for use within CE, NE, and enclave environments. They ensure that the architecture and design of DoD IS are functional and secure. This may include designs for program of record systems

and special purpose environments with platform IT interconnectivity. Incumbents may also be responsible for system or network designs that encompass multiple CE and/or NE to include those with differing data protection/classification requirements.

MOS PERFORMING: 0610, 0620, 0650, 0689

BILLETS: System Architect and Engineer (IASAE) Level III

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT, WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Enclave environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:

1. Identify information protection needs for the enclave environment.
2. Define enclave security requirements in accordance with applicable IA policies (e.g., DoDI 8500.2 and DCID 6/3 and organizational security policies).
3. Provide input on IA security requirements to be included in statements of work and other appropriate procurement documents.
4. Support Program Managers responsible for the acquisition of DoD IS to ensure IA architecture and systems engineering requirements are properly addressed throughout the acquisition life-cycle.
5. Design security architectures for use within the enclave environment.
6. Design and develop IA or IA-enabled products for use within the enclave.
7. Design and develop CDS for use within CE, NE, or enclave environments.
8. Develop and implement security designs for new or existing enclave system(s). Ensure that the design of hardware, operating systems, and software applications adequately address IA security requirements for the enclave.
9. Design, develop, and implement security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation for the enclave environment.
10. Design, develop, and implement specific IA countermeasures for the enclave.
11. Develop interface specifications for use within the enclave environment.
12. Develop approaches to mitigate enclave vulnerabilities and recommend changes to system or system components as needed.
13. Ensure that enclave system(s) and network(s) designs support the incorporation of DoD-directed IA vulnerability solutions, e.g., IAVAs.
14. Develop IA architectures and designs for DoD IS with high integrity and availability requirements, to include MAC I systems as defined in DoDI 8500.2 and DoDD 8500.1, systems with a high Level-of-Concern for availability or integrity in accordance with DCID 6/3, and other DAA designated systems.
15. Develop IA architectures and designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data (e.g., UNCLASSIFIED, SECRET, and

TOP SECRET).
16. Develop IA architectures and designs for systems processing SCI that will operate at Protection Level 3, 4, or 5 as defined in DCID 6/3.
17. Develop IA architectures and designs for DoD IS to include automated IS applications, enclaves (which include networks), and special purpose environments with platform IT interconnectivity, e.g., weapons systems, sensors, medical technologies, or distribution systems.
18. Ensure that acquired or developed system(s) and network(s) employ Information Systems Security Engineering and are consistent with DoD Component level IA architecture.
19. Assess threats to and vulnerabilities of the enclave.
20. Identify, assess, and recommend IA or IA-enabled products for use within an enclave and ensure recommended products are in compliance with the DoD evaluation and validation requirements of DoDI 8500.2 and DoDD 8500.1.
21. Ensure that the implementation of security designs properly mitigate identified threats.
22. Assess the effectiveness of information protection measures utilized by the enclave.
23. Evaluate security architectures and designs and provide input as to the adequacy of security designs and architectures proposed or provided in response to requirements contained in acquisition documents.
24. Ensure security deficiencies identified during security/certification testing have been mitigated, corrected, or a risk acceptance has been obtained by the appropriate DAA or authorized representative.
25. Provide input to IA C&A process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
26. Participate in an IS risk assessment during the C&A process and design security countermeasures to mitigate identified risks.
27. Provide engineering support to security/certification test and evaluation activities.
28. Document system security design features and provide input to implementation plans and standard operating procedures.
29. Recognize a possible security violation and take appropriate action to report the incident.
30. Implement and/or integrate security measures for use in the enclave and ensure that enclave designs incorporate security configuration guidelines
31. Ensure the implementation of enclave IA policies into system architectures.
32. Ensure the implementation of subordinate CE and NE IA policies are integrated into the enclave system architecture.
33. Oversee and provide technical guidance to IASAE Level I and II personnel.
34. Obtain and maintain IA certification appropriate to position.

REFERENCES:
1. Director of Central Intelligence Directive (DCID) 6/3 Protecting Sensitive Compartmented Information within Information Systems.
2. DoDD 8500.1 Information Assurance (IA)
3. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
4. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
5. DoDD 8570.01M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
6. DoDI 8500.2 Information Assurance (IA) Implementation

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or the Marine Corps Communications Electronics School (MCCES).

SPECIAL PERSONNEL CERTS: 1. International Information Systems Security Certifications Consortium (ISC)2 Information Systems Security Architecture Professional (ISSAP). 2. International Information Systems Security Certifications Consortium (ISC)2 Information Systems Security Engineering Professional (ISSEP).

COMM T&R MANUAL

CHAPTER 6

MOS 0602 INDIVIDUAL EVENTS

CHAPTER 6

MOS 0602 INDIVIDUAL EVENTS

6000. INDEX OF INDIVIDUAL EVENTS

6001. 1000-LEVEL EVENTS

0602-PLAN-1101: Develop a communications estimate

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: This event is conducted during the Mission Analysis Phase of the Marine Corps Planning Process.

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, task organization, table of equipment, constraints, restraints, commander’s battlespace area evaluation, initial planning guidance, intelligence preparation of the battlespace (IPB) products, and higher headquarters Annex K.

STANDARD: Within a timeline provided by the commander that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Analyze higher headquarters' Annex K.
2. Analyze intelligence preparation of the battlespace (IPB) products.
3. Determine enemy electronic warfare capabilities.
4. Analyze the commander's battlespace area evaluation.
5. Determine battlespace conditions affect on communications.
6. Analyze the commander's intent.
7. Analyze the command's mission.
8. Analyze friendly force task organization.
9. Identify purpose of the operation.
10. Identify tasks of the operation.
11. Analyze centers of gravity.
12. Determine communication center of gravity.
13. Determine the command's communications system requirements.
14. Coordinate staff information exchange requirements with the Command's Information Management Officer (IMO).
15. Determine communication resources available.
16. Determine communication constraints.
17. Determine communication restraints.
18. Recommend commander's critical information requirements.
19. Identify requests for information.
20. Determine assumptions affecting communication.
21. Draft a communication mission statement.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-PLAN-1102: Refine a communications estimate

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: This event is conducted within the Course of Action (COA) Development, COA Wargame and COA Comparison/Decision Phases of the Marine Corps Planning Process.

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's approved mission statement, tasks, task organization, table of equipment, constraints, restraints, commanders battlespace area evaluation, commanders planning guidance, intelligence preparation of the battlespace (IPB) products, higher headquarters Annex K, and initial communications estimate.

STANDARD: Within a timeline provided by the commander that satisfies the commanders communications system requirements for command and control.

PERFORMANCE STEPS:
1. Analyze higher headquarters Annex K.
2. Evaluate battlefield conditions affects on communication.
3. Determine current communication situation.
4. Analyze course(s) of action.
5. Determine communication resource capabilities.
6. Determine communication resource requirements.
7. Allocate communication resources.
8. Develop communication concept(s) of operation(s).
9. Conduct course of action wargame of communication concept(s) of operation(s).
10. Conduct course of action comparison of communication concept(s) of operation(s).
11. Determine preferred communication concept of operation.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-PLAN-1103: Determine a command's radio network requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, approved course of action, task organization, table of equipment, higher headquarters Annex K.

STANDARD: Within a timeline provided by the commander that satisfies the commanders communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine High Frequency (HF) requirements.
2. Determine Very High Frequency (VHF) requirements.
3. Determine Ultra High Frequency (UHF) requirements.
4. Determine Super High Frequency (SHF) requirements.
5. Determine Extra High Frequency (EHF) requirements.
6. Determine satellite access requirements.
7. Determine disaster recovery requirements.
8. Compile a command's radio network requirements.
9. Submit a command's radio network requirements to higher headquarters.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-PLAN-1104: Determine a command's circuit switching requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, approved course of action, task organization, table of equipment, higher headquarters Annex K.

STANDARD: Within a timeline provided by the commander that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine subscriber requirements.
2. Determine specific switching mission requirements.
3. Determine quantities of trunk interfaces.
4. Determine types of trunk interfaces.
5. Identify call routing planning considerations.
6. Determine trunk signaling requirements.
7. Determine disaster recovery requirements.
8. Compile a commands circuit switching requirements.
9. Submit a commands circuit switching requirements to higher headquarters.

0602-PLAN-1105: Determine a command's packet switching network requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, approved course of action, task organization, table of equipment, higher headquarters Annex K.

STANDARD: Within a timeline provided by the commander that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine network user requirements.
2. Determine enterprise network bandwidth.
3. Determine enterprise network operating system requirements.
4. Determine information assurance data network requirements.
5. Determine disaster recovery requirements.
6. Identify organizational messaging requirements.
7. Identify real-time service requirements.
8. Compile a command’s packet switching network requirements.
9. Submit a commands packet switched network requirements to higher headquarters.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-PLAN-1106: Develop a communications plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Per the MCWP 3-40.3 (DRAFT) MAGTF Communications System, as the tactical COA is converted into the overall CONOPS and the command's OPORD is crafted, the communications planner translates the communication concept of support into the communications CONOPS and develops the communication plan. While the formal, deliberate manifestation of a communications plan is annex K, time available size of unit, and mission dictate the extent to which a plan is documented. The purpose of any order--whether delivered in a 200-page document or verbally--is to provide clarity and promote shared understanding. Once the order is issued, a communication organization can then transition to briefing the plan and conducting rehearsals.

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, approved course of action, task organization, table of equipment, higher headquarters Annex K and communication concept of support.

STANDARD: Within a timeline provided by the commander that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Develop a radio network plan.
2. Determine satellite access requirements.
3. Determine multiplexing network requirements.
4. Develop a circuit switching plan.
5. Develop a packet switching network plan.
6. Determine information assurance requirements.
7. Determine communication security requirements.
8. Submit communications system requirements to higher headquarters.
9. Integrate communications system architecture within higher headquarters communications system architecture.
10. Prepare a communications plan.
11. Disseminate the communications plan.
12. Conduct Transition.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-MNGT-1701: Manage a communications system architecture

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, operational conditions, operational plans, and communications systems architecture.

STANDARD: That satisfies the commander's communications system requirements for command and control during a given operation.

PERFORMANCE STEPS:
1. Supervise the execution of a communications plan.
2. Supervise communications control functions and procedures.
3. Supervise communication security functions and procedures.
4. Supervise information assurance functions and procedures.
5. Evaluate communications system architecture performance.
6. Determine communications system architecture modifications.
7. Direct communications system architecture modifications.
8. Supervise communications system architecture.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. MCWP 5-1 Marine Corps Planning Process (MCPP)

0602-MNGT-1702: Manage communication resources

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's Mission Essential Task List, Training Exercise and Employment Plan, Table of Organization, Table of Equipment, resource readiness documents, and mission.

STANDARD: To ensure resource availability to satisfy the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine equipment resources to satisfy mission requirements.
2. Organize equipment resources to satisfy mission requirements.
3. Determine logistical requirements to satisfy mission requirements.
4. Determine logistical requirements that facilitate equipment readiness.
5. Determine equipment readiness.
6. Supervise equipment maintenance.
7. Maintain equipment accountability.
8. Identify personnel resources to satisfy mission requirements.
9. Organize personnel resources to satisfy mission requirements.
10. Determine mission-specific individual readiness qualification requirements.
11. Plan training.
12. Supervise training.

REFERENCES:
1. MCO P4790.2_ MIMMS Field Procedures Manual
2. MCRP 3-0A Unit Training Management Guide
3. MCWP 4-11 Combat Service Support

0602-PROT-1801: Manage Information Assurance (IA) in a computing environment (CE)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Per DoD 8570.01, Information Assurance Management Level I personnel are responsible for the implementation and operation of a DoD IS or system DoD Component within their CE regardless of their occupational title. Incumbents ensure that IA related IS are fu8nctional and secure within the CE. The CE is defined as local area network(s) server host and its operating system, peripherals and applications.

MOS PERFORMING: 0602

GRADES: 2NDLT, 1STLT, CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a computing environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of Marine Corps information, information systems, and information infrastructures.

PERFORMANCE STEPS:
1. Adhere to HQMC C4 IA Directives.
2. Provide system related input on IA security requirements.
3. Ensure data retention and recovery within the CE.
4. Coordinate with higher headquarters IAM in the development or modification of the computer environment IA security program plans and requirements.
5. Ensure CE users meet systems authorization access requirements.
6. Recognize security violations.
7. Report security violations.
8. Supervise corrective measures to IA vulnerabilities.
9. Supervise the adherence of system security configuration guidelines.
10. Comply with IA security requirements in a CE.
11. Coordinate IA inspections, tests, and reviews.
12. Participate in the Certification and Accreditation process.
13. Collect data for IA reporting requirements.
14. Within six months of being assigned to an IAM Level I billet, obtain IA certification appropriate to position.
15. Maintain IA Certification appropriate to position.

REFERENCES:
1. DoD 8570.01-M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
2. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or Communication Training Centers.

SPECIAL PERSONNEL CERTS: COMP TIA SY0-101 Security + Certification.

COMM T&R MANUAL

CHAPTER 7

MOS 0603 INDIVIDUAL EVENTS

CHAPTER 7

MOS 0603 INDIVIDUAL EVENTS

7000. INDEX OF INDIVIDUAL EVENTS

7001. 2000-LEVEL INDIVIDUAL EVENTS

0603-PLAN-2101: Develop a Major Subordinate Command (MSC) communications concept

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, task organization, table of equipment, constraints, restraints, commander's battlespace area evaluation, initial planning guidance, intelligence preparation of the battlespace (IPB) products, and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Analyze higher headquarters communication plan.
2. Interpret the Commander's guidance.
3. Identify the communications critical vulnerability.
4. Identify the communications mission constraints.
5. Identify the communications mission restraints.
6. Apply planning considerations for Radio Network systems.
7. Apply planning considerations for multiplexing Networks.
8. Apply planning considerations for Circuit Switching Network systems.
9. Apply planning considerations of DISA STEP.
10. Apply planning considerations for end-user terminal equipment.
11. Apply planning considerations for packet switching network equipment.
12. Apply communications resources to the operational scheme of maneuver.
13. Associate using unit's requirements with the communications capabilities.
14. Draft a communications concept.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2102: Develop a Radio Network Plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a communications concept and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine High Frequency (HF) requirements.
2. Determine Very High Frequency (VHF) requirements.
3. Determine Ultra High Frequency (UHF) requirements.
4. Determine Super High Frequency (SHF) requirements.
5. Determine Extra High Frequency (EHF) requirements.
6. Develop a Single Channel Radio Guard Chart.
7. Develop a Multi-Channel Radio Guard Chart.
8. Develop a Single Channel Radio System diagram.
9. Develop a Multi-Channel Radio System diagram.
10. Develop a Satellite Access Request (SAR).
11. Submit a Satellite Access Request (SAR).
12. Draft a Radio Network Appendix for an Annex-K.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2103: Develop a Multiplexing Network Plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a communications concept and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine Time Division multiplexing requirements.
2. Determine Frequency Division multiplexing requirements.
3. Determine Time Division Multiple Access (TDMA) requirements.
4. Determine Frequency Division Multiple Access (FDMA) requirements.
5. Develop Level 1 Time Division Multiplexing Diagram.
6. Develop Level 2 Time Division Multiplexing Diagram.
7. Develop Frequency Division Multiplexing Diagram.
8. Develop Master Transmission System Link Designators.
9. Develop Master Circuit Listing Designators.
10. Develop a Gateway Access Request (GAR).
11. Submit Gateway Access Request (GAR) as required.
12. Draft a Multiplexing Network Appendix for an Annex-K.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2104: Develop a Telephone Network Plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a communications concept and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine subscriber requirements.
2. Determine trunk requirements.
3. Develop a Tactical Circuit Switching diagram.
4. Develop a Commercial Circuit Switching diagram.
5. Develop an IP-based Voice Systems diagram.
6. Develop a Defense Switch Network diagram.
7. Develop a Defense Red Switch Network diagram.
8. Draft a Telephone Network appendix for an Annex-K.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2105: Develop Packet Switching Network Plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a communications concept and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Identify data network bandwidth requirements.
2. Identify network operating system requirements.
3. Identify Information Assurance requirements.
4. Identify organizational messaging requirements.
5. Identify Quality of Service (QoS) requirements.
6. Identify Virtual Private Network (VPN) requirements.
7. Identify Internet Protocol Security (IPSEC) requirements.
8. Identify Internet Protocol routing requirements.
9. Identify data replication requirements.
10. Identify data network time requirements.
11. Identify Disaster Recovery requirements.
12. Develop a SIPRNET WAN diagram.
13. Develop a NIPRNET WAN diagram.
14. Develop a SIPRNET LAN diagram.
15. Develop a NIPRNET LAN diagram.
16. Develop an Active Directory diagram.
17. Develop an Exchange Messaging diagram.
18. Develop a Messaging diagram.
19. Develop a Disaster Recovery diagram.
20. Draft a Data Network appendix for an Annex-K.

REFERENCES:
1. CJCSI 6215.01 Policy for the Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2106: Develop a Network Timing Scheme

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a communications concept and higher headquarters Annex K.

STANDARD: Within the Marine Corps Planning Process that satisfies the commanders communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine Stratum 1 system requirements.
2. Determine Stratum 2 system requirements.
3. Develop a Network Timing diagram.
4. Draft a Network Timing diagram tab for appendix 6 of an Annex-K.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications

3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0603-PLAN-2107: Develop a Major Subordinate Command (MSC) Communications Plan.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0603

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, task organization, table of equipment, constraints, restraints, commander's battlespace area evaluation, initial planning guidance, intelligence preparation of the battlespace (IPB) products, and higher headquarters Annex K.

STANDARD: Within the orders development phase of the Marine Corps planning process that satisfies the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Analyze higher headquarters Annex K.
2. Develop communications concept.
3. Determine COMSEC requirements.
4. Determine radio frequency requirements.
5. Determine voice connectivity requirements.
6. Determine data network requirements.
7. Determine multiplexing requirements.
8. Determine Information Assurance requirements.
9. Integrate the communications architecture with higher and adjacent in accordance with an Annex K.
10. Develop a Radio Network Appendix.
11. Develop a Multiplexing Network Appendix.
12. Develop a Gateway Access Request (GAR) to a Multiplexing Appendix.
13. Develop a Voice Network Appendix.
14. Develop a Data Network Appendix.
15. Develop a network timing scheme.
16. Draft an Annex K in support of an Operations Order.
17. Conduct Transition.

REFERENCES:
1. CJCSI 6215.01 Policy For The Defense Switched Network
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

CHAPTER 8

MOS 0610 INDIVIDUAL EVENTS

CHAPTER 8

MOS 0610 INDIVIDUAL EVENTS

8000. INDEX OF INDIVIDUAL EVENTS

8001. 2000-LEVEL EVENTS

0610-PLAN-2101: Develop telephony services estimate of supportability for a Major Subordinate Command (MSC)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: An estimate of supportability will reconcile mission requirements with MSC resources and identify specific deficiencies.

MOS PERFORMING: 0610

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To identify the MSCs capability to support the telephone services plan.

PERFORMANCE STEPS:
1. Conduct a mission analysis.
2. Review initial planning products.
3. Conduct estimate of supportability.
4. Submit estimates of supportability.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-PLAN-2102: Develop a telephony services estimate of supportability for a Marine Expeditionary Force (MEF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: An estimate of supportability will reconcile mission requirements with MAGTF resources and identify specific deficiencies.

MOS PERFORMING: 0610

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To identify the MEF's capability to support the telephone services plan.

PERFORMANCE STEPS:
1. Conduct a mission analysis.
2. Review initial planning products.
3. Conduct estimate of supportability.
4. Submit estimate of supportability.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-DSGN-2201: Design telephony services architecture for a Major Subordinate Command (MSC)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: The telephony services architecture is the result of COA development, war-gaming, and decision.

MOS PERFORMING: 0610

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To support the commander's chosen course of action and concept of operations.

PERFORMANCE STEPS:
1. Design Circuit Switchboard architecture.
2. Design Cable Plant architecture.
3. Design Voice over Internet Protocol (VoIP) architecture.
4. Design telephony architecture gateway services.
5. Develop Telephony services tabs.
6. Review estimate of supportability.
7. Conduct telephony services COA development.
8. Conduct telephony services COA war-gaming.
9. Obtain COA decision.
10. Identify subscriber clusters.
11. Provision for subscriber clusters.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. DISA STIGS DISA Security Technical Implementation Guides

3. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
4. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-DSGN-2202: Design telephony systems architecture for a Marine Expeditionary Force

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: The telephony systems architecture is the result of COA development, war-gaming, and decision.

MOS PERFORMING: 0610

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To support the commander's chosen course of action and concept of operations.

PERFORMANCE STEPS:
1. Design Circuit Switchboard architecture.
2. Design Cable Plant architecture.
3. Design Voice over Internet Protocol (VoIP) architecture.
4. Design telephony architecture gateway services.
5. Develop Telephony services tabs.
6. Review estimate of supportability.
7. Conduct telephony services COA development.
8. Conduct telephony services COA war-gaming.
9. Obtain telephony services COA decision.
10. Identify subscriber clusters.
11. Provision for subscriber clusters.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-ENGR-2301: Create telephony services engineering documents for a Major Subordinate Command

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineering documents should contain signaling protocols, frame formatting, line coding, trunk specifications, codecs, routing information, IP allocations, equipment rack maps, port identification, device naming/numbering schemes, switch code allocations, dialing instructions, and subscriber listings. The installed architecture will provide the ability to process originating, tandem, and terminating secure and non-secure telephony services.

MOS PERFORMING: 0610

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a basic network design, the commander's intent, the concept of operations, and references.

STANDARD: To provide sufficient technical details required per Standard Operating Procedures to execute the telephony services plan.

PERFORMANCE STEPS:
1. Identify transport media
2. Identify bandwidth availability
3. Establish trunk methodologies
4. Establish trunk quantities required to facilitate TDM and IP traffic density.
5. Allocate IP network addresses
6. Establish Quality of Service (QoS) Tactics Techniques Procedures (TTP) for IP telephony services
7. Establish IP telephone registration TTPs
8. Establish telephony services gateway configurations.
9. Establish signaling protocols
10. Coordinate IP address requirements in support of telephony services
11. Establish telephony services call routing procedures.
12. Specify traffic encryption requirements.
13. Establish subscriber classes of service
14. Draft telephony services engineering documents.
15. Consolidate telephony services engineering documents for incorporation to the Annex K, Appendices 7 and 9.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-ENGR-2302: Create telephony services engineering documents for a Marine Expeditionary Force

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineering documents should contain signaling protocols, frame formatting, line coding, trunk specifications, codecs, routing information, IP allocations, equipment rack maps, port identification, device naming/numbering schemes, switch code allocations, dialing instructions, and subscriber listings. The installed architecture will provide the ability to process originating, tandem, and terminating secure and non-secure telephony services.

MOS PERFORMING: 0610

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided telephony services design documents, the commander's intent, the concept of operations, and references.

STANDARD: To provide sufficient technical details required per Standard Operating Procedures to execute the telephony services plan.

PERFORMANCE STEPS:
1. Identify transport media.
2. Identify bandwidth availability.
3. Establish trunk methodologies.
4. Establish trunk quantities required to facilitate TDM and IP traffic density.
5. Allocate IP network addresses.
6. Establish Quality of Service (QoS) Tactics Techniques Procedures (TTP) for IP telephony services.
7. Establish IP telephone registration TTPs.
8. Establish telephony services gateway configurations.
9. Establish signaling protocols.
10. Coordinate IP address requirements in support of telephony services.
11. Establish telephony services call routing procedures.
12. Specify traffic encryption requirements.
13. Establish subscriber classes of service.
14. Draft telephony services engineering documents.
15. Consolidate telephony services engineering documents for incorporation to the Annex K, Appendices 7 and 9.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. MCWP 5-1 Marine Corps Planning Process (MCPP)

0610-MNGT-2701: Write telephone services commodity section Standing Operating Procedures (SOP)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided commander's guidance, T/O&E, and references.

STANDARD: To establish written guidance to the commodity section.

PERFORMANCE STEPS:
1. Analyze planning documents and existing SOP.
2. Identify mission specific requirements.
3. Draft SOP.
4. Staff SOP.
5. Rehearse SOP.
6. Finalize SOP.
7. Update SOP.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 Communications and Information Systems
3. MCWP 5-1 Marine Corps Planning Process

0610-MNGT-2702: Manage telephony services commodity section

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: This task is billet specific. Section will provide scalable expeditionary telephony services in support of operating forces as defined in the unit mission statement. MOJT initial training settings due to experience gained from prerequisite feeder MOS.

MOS PERFORMING: 0610

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided commander's guidance, personnel, facilities, equipment, funding, and references.

STANDARD: To satisfy telephony services requirements.

PERFORMANCE STEPS:
1. Review unit mission statement and commander's guidance.
2. Maintain accountability of personnel.
3. Maintain operational readiness of personnel.
4. Maintain accountability of equipment.
5. Maintain operational readiness of equipment.

6. Inspect commodity area Turnover Folders or Desktop Procedures.
7. Develop training schedule.
8. Conduct training.
9. Assess equipment readiness.
10. Prepare for deployment of commodity section.
11. Supervise deployment of commodity section.

REFERENCES:
1. MCBUL 3000 Marine Corps Automated Readiness Evaluation System (MARES) Equipment
2. MCO P4790.2_ MIMMS Field Procedures Manual
3. MCRP 3-0A Unit Training Management Guide
4. MCRP 3-0B How to Conduct Training

0610-MNGT-2703: Develop an installation telephone office budget

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Provides a budget that supports the operations and maintenance of inside plant/outside plant management.

MOS PERFORMING: 0610

GRADES: CWO-2, CWO-3, CWO-4

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided budget documents, commander's guidance, and references.

STANDARD: To operate within approved funding authorizations.

PERFORMANCE STEPS:
1. Determine recurring Operational and Maintenance (O&M) costs.
2. Estimate recurring reimbursable allocations.
3. Estimate variable costs.
4. Determine projects costs.
5. Submit required initial authorization.
6. Determine Procurement Marine Corps (PMC) funding requirements.
7. Develop Projected O&M (POM) funding requirements.
8. Submit midyear review.
9. Submit end of year review.

REFERENCES:
1. MCO 2305.13 Unofficial Telephone Service at Department of Defense Activities
2. MCO P4400.150_ Consumer Level Supply Policy Manual
3. DoD Financial Management Regulation
4. Navy Comptroller Manual

0610-MNGT-2704: Manage an installation telephone office

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Provides supervision of installation telephone office functions.

MOS PERFORMING: 0610

GRADES: CWO-2, CWO-3, CWO-4

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: That provides defense switched network and commercial access telephony services to a base, post, or station.

PERFORMANCE STEPS:
1. Establish Inside Plant Standard Operating Procedures.
2. Establish Outside Plant Standard Operating Procedures.
3. Supervise personnel.
4. Account for equipment.
5. Organize personnel resources to satisfy mission requirements.
6. Supervise equipment maintenance.
7. Inspect Turnover Folders or Desktop Procedures.
8. Identify training deficiencies.
9. Ensure completion of mission-specific individual qualification requirements.
10. Conduct training.

REFERENCES:
1. MCO 2305.13 Unofficial Telephone Service at Department of Defense Activities
2. MCO P2066.1 Marine Corps Installation Telephone System
3. OPNAV 2060.8 Management and Business Administration of Department of Defense (DOD) Telephone Systems and Base Telecommunications Services within the Department of the Navy

COMM T&R MANUAL

CHAPTER 9

MOS 0612 INDIVIDUAL EVENTS

CHAPTER 9

MOS 0612 INDIVIDUAL EVENTS

9000. INDEX OF INDIVIDUAL EVENTS

9001. 1000-LEVEL EVENTS

0612-INST-1401: Install cable/wire

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching and data systems, termination points, and transmission mediums.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate cable/wire.
3. Test cable/wire.
4. Inventory cable/wire.
5. Mount cable/wire reel.
6. Run cable/wire.
7. Splice wire when applicable.
8. Tip end of wire.
9. Connect cable/wire to equipment.
10. Label cable/wire.
11. Report changes of plant records to site chief.

REFERENCES:
1. CX-13295/G (300m) and CX-13295/G (1000m) Operator's Manual
2. FM 11-372-2 Outside Plant Cable Placement
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
6. TIA/EIA Telecommunications Industry Association/Electronics Industry Association 568 wiring standard
7. TM 11-5995-208-24&P Cable Assembly, Special Purpose Cx-11230/G
8. TM-11-5805-574-24P Cable Assemblies, Assault, Communications CX-4566 (25, 50, 100, 250, 500 ft lengths)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cables/Wire. 3. Reel. 4. Cable payout device. 5. Telephony switching equipment. 6. Telephone Set.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-INST-1402: Install a distribution device

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching and data systems and termination points.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate distribution device.
3. Test distribution device.
4. Inventory distribution device.
5. Select a suitable surface.
6. Mount the distribution device.
7. Ground the distribution device, if applicable.
8. Terminate cable(s) to the distribution device.
9. Connect wire to the distribution device.
10. Label wires and cables.
11. Report changes of plant records to site chief.

REFERENCES:
1. FM 11-372-2 Outside Plant Cable Placement
2. MCO 3500.27_ Operational Risk Management (ORM)
3. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
4. TM 11-6110-201-12P Operator and Organizational Maintenance Manual with Repair Parts and Special Tools List for Distribution Boxes, J-1077/U AND J-1077A/U
5. TM 11-6110-243-14P Operator's, Organizational, Direct Support, and General Support Maintenance Repair Parts and Special Tools Lists For Distribution Box J-2317/U AND J-2317A/U
6. TM 11332A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
7. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Distribution Device. 3. Cable/Wire. 4. Telephony switching equipment.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-INST-1403: Install a patch panel

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching and data systems.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate patch panel.
3. Test patch panel.
4. Inventory patch panel.
5. Select a suitable surface.
6. Ground equipment.
7. Connect cable(s) to the patch panel.
8. Label cables.
9. Install patch cords.
10. Label Patch Panel.
11. Perform function check.
12. Report changes of plant records to site chief.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 08228A-14/1 Panel, Patching, Communications SB-3659 A/U
3. TM 08229A-14/1 Patch Panel Comm SB-4097/U
4. TM 11332A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
5. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Patch Panel. 3. Cable/Wire. 4. Telephony system.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-INST-1404: Install a Telephony switching system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure reliable telephony services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate telephony system.
3. Select a suitable surface.
4. Ground equipment.
5. Configure the system hardware.
6. Connect required cables.
7. Apply power.
8. Configure system software.
9. Perform system operational checks.

REFERENCES:
1. Data, Voice and Video Cabling, 2nd Edition Author Jim Hayes, Paul Rossenberg, pub. 2005 Delmar Learning
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. TM 11332A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
7. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62
8. The Irwin Handbook of Telecommunications, Fifth Edition Author James Harry Green, 2006 Pantel Inc.

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cable/Wire. 3. Telephony system. 4. Telephone set. 5. Power Source.

MATERIAL: 1. Switching network diagram. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-INST-1405: Install a telephone set

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure reliable telephony services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate telephone set.
3. Test phone.
4. Inventory phones.
5. Select a suitable surface.
6. Configure a telephone set.
7. Connect wire for operation.
8. Install applicable COMSEC.
9. Conduct line/circuit check.
10. Label telephone set.
11. Report changes of plant records to site chief.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. O&T STE User Manual 2.0
3. OMNI User Manual Release 3.0
4. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
5. TIA/EIA Telecommunications Industry Association/Electronics Industry Association 568 wiring standard
6. TM 11-5805-201-12 Operational Manual, TA-312/PT
7. TM 11-5805-693-12P Telephone Set TA-938A/G

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cable/wire. 3. Telephony switching equipment. 4. Telephone set. 5. Power source.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-INST-1406: Install ancillary equipment.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching, data, multiplexing systems, terminating points, and transmission mediums.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate ancillary equipment.
3. Test ancillary equipment.
4. Inventory ancillary equipment.
5. Select a suitable surface.
6. Ground equipment.
7. Configure the ancillary equipment (hardware).
8. Connect interface cables.
9. Apply power.
10. Configure the ancillary equipment (software).
11. Perform system operational checks.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 09006A-10/1 Operation Instructions for Converter Set, Fiber Optic AN/GSC-54
3. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
4. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cable/Wire. 3. Switch. 4. Ancillary/supporting equipment. 5. Power source.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-OPER-1501: Operate a telephony system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, commanders guidance and references.

STANDARD: To ensure reliable telephony services to subscribers.

PERFORMANCE STEPS:
1. Conduct move add changes.
2. Generate meter reports.
3. Conduct database backups.
4. Perform network optimization.
5. Maintain log books.
6. Maintain electrical grounds.
7. Conduct line checks.

REFERENCES:
1. Fifth Edition The Irwin Handbook of Telecommunications, Author James Harry Green, 2006 Pantel Inc.
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. Pub 2005 Delmar Learning Data, Voice and Video Cabling, 2nd Edition Author Jim Hayes, Paul Rossenberg.
7. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
8. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Telephony system. 2. Power source. 3. Computer.

MATERIAL: 1. Switching network diagrams. 2. Cut sheets. 3. Operational Risk Assessment Worksheet (ORAW).

0612-MANT-1601: Maintain a telephony system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided faulty equipment, planning documents, commander's guidance, and references.

STANDARD: To ensure reliable services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Perform operational check to identify problem.
3. Conduct troubleshooting procedures.
4. Isolate problem.
5. Perform corrective action.
6. Restore services.
7. Report as required.
8. Document actions taken.
9. Document authorized maintenance.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63

3. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Telephony system. 2. Power source. 3. Computer.

MATERIAL: 1. Cut sheets. 2. Operational Risk Assessment Worksheet (ORAW).

0612-MANT-1602: Maintain ancillary equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided faulty equipment, planning documents, commanders guidance, and references.

STANDARD: To ensure reliable services to subscribers.

PERFORMANCE STEPS:
1. Review changes to planning documents.
2. Perform operational check to identify problem.
3. Conduct troubleshooting procedures.
4. Isolate problem.
5. Perform corrective action.
6. Restore services.
7. Report as required.
8. Document actions taken
9. Document authorized maintenance.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 11332A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
3. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Ancillary equipment. 2. Power source. 3. Computer.

MATERIAL: 1. Cut sheets. 2. Operational Risk Assessment Worksheet (ORAW).

9002. 2000-LEVEL EVENTS

0612-MANT-2601: Maintain telephony networks

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure reliable services to subscribers.

PERFORMANCE STEPS:
1. Review planning documents.
2. Review traffic metering reports.
3. Recommend network changes.
4. Ensure configuration changes are made properly.
5. Ensure configuration changes are documented.
6. Submit documents for review.

CHAINED EVENTS:
0612-MANT-1601 0612-OPER-1501 0612-MANT-1602

REFERENCES:
1. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
2. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Switching network diagrams.

0612-MNGT-2701: Supervise cable plant installation

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure reliable telephony services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Review all planning documents.
3. Identify priorities of work.
4. Supervise cable installation.
5. Modify cable route as required.
6. Document changes.
7. Submit documents for review.

CHAINED EVENTS: 0612-INST-1401

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Computer with appropriate software for documentation.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Switching network diagram. 4. Operational Risk Assessment Worksheet (ORAW).

0612-MNGT-2702: Supervise installation of telephone sets

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure reliable services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Review all planning documents.
3. Confirm precedence settings for users.
4. Confirm COMSEC requirements are met.
5. Supervise tag installation.
6. Document changes.
7. Submit documents for review.

CHAINED EVENTS: 0612-INST-1405

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. O&T STE User Manual 2.0
3. OMNI User Manual Release 3.0
4. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES

5. TM 11-5805-201-12 Operational Manual, TA-312/PT
6. TM 11-5805-693-12P Telephone Set TA-938A/G

0612-MNGT-2703: Supervise the installation of distribution devices

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure reliable telephony services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Review planning documents.
3. Supervise grounding of equipment.
4. Supervise tag installation.
5. Document changes.
6. Submit documents for review.

CHAINED EVENTS: 0612-INST-1402

REFERENCES:
1. FM 11-372-2 Outside Plant Cable Placement
2. MCO 3500.27_ Operational Risk Management (ORM)
3. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
4. TM 11-6110-201-12P Operator and Organizational Maintenance Manual with Repair Parts and Special Tools List for Distribution Boxes, J-1077/U AND J-1077A/U
5. TM 11-6110-243-14P Operator's, Organizational, Direct Support, and General Support Maintenance Repair Parts and Special Tools Lists For Distribution Box J-2317/U AND J-2317A/U
6. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
7. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Distribution device. 3. Tags. 4. Markers.

MATERIAL: 1. Cable route map. 2. Cut sheets. 3. Switching network diagram. 4. Operational Risk Assessment Worksheet (ORAW).

0612-MNGT-2704: Supervise the installation of telephony systems

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure reliable services to subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Review planning documents.
3. Supervise proper installation of telephony switching systems.
4. Ensure proper telephony system administration is conducted.
5. Supervise grounding of equipment.
6. Ensure proper troubleshooting procedures are followed.

CHAINED EVENTS:
0612-INST-1404 0612-INST-1403

REFERENCES:
1. Data, Voice and Video Cabling, 2nd Edition Author Jim Hayes, Paul Rossenberg, pub. 2005 Delmar Learning
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
7. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62
8. The Irwin Handbook of Telecommunications, Fifth Edition Author James Harry Green, 2006 Pantel Inc.

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cable/wire. 3. Switch. 4. Power source.

MATERIAL: 1. Cut sheets. 2. Switching network diagram. 3. Operational Risk Assessment Worksheet (ORAW).

0612-MNGT-2705: Supervise installation of ancillary equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0612

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To ensure connectivity between switching, data, multiplexing systems, terminating points, transmission mediums, and subscribers.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select appropriate ancillary equipment.
3. Supervise the testing of ancillary equipment.
4. Supervise the inventorying of ancillary equipment.
5. Supervise the selection of suitable surface.
6. Supervise grounding of equipment.
7. Supervise the configuration of ancillary equipment (hardware).
8. Ensure interface cables are connected.
9. Supervise power application.
10. Supervise the configuration of ancillary equipment (software).
11. Ensure a function check is conducted.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
3. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62
4. Unit SOP Unit SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tools. 2. Cable/wire. 3. Ancillary/supporting equipment.

MATERIAL: 1. Cut sheets. 2. Switching network diagrams. 3. Operational Risk Assessment Worksheet (ORAW).

COMM T&R MANUAL

CHAPTER 10

MOS 0613 INDIVIDUAL EVENTS

CHAPTER 10

MOS 0613 INDIVIDUAL EVENTS

10000. INDEX OF INDIVIDUAL EVENTS

10001. 1000-LEVEL EVENTS

0613-INST-1401: Negotiate an unstepped pole

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0613

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided appropriate tools, safety equipment, pole/tree, and reference.

STANDARD: To demonstrate proficiency in pole climbing techniques.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Inventory equipment.
3. Select correct gaffs for pole/tree.
4. Check gaffs for thickness, width, and length with appropriate gauge.
5. Adjust LC-240.
6. Inspect pole/tree.
7. Climb pole/tree.
8. Fasten safety strap around tree/pole.
9. Unfasten safety strap.
10. Descend pole/tree.

REFERENCES:
1. FM 24-20 Tactical Wire and Cable Techniques
2. MCO 3500.27_ Operational Risk Management (ORM)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. LC-240. 2. Poles/trees to climb. 3. Personal protective equipment (PPE).

0613-INST-1402: Install aerial cable

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0613

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided tools, equipment, materials, existing aerial span, a given height requirement, and references.

STANDARD: At the required height to establish connectivity between end points.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Ascend to installation location.
3. Lay cable.
4. Prepare lashing machine, as required.
5. Lash cable to existing span.
6. Descend from installation location.

REFERENCES:
1. FM 11-372-2 Outside Plant Cable Placement
2. MCO 3500.27_ Operational Risk Management (ORM)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Lashing machine. 2. Existing aerial span. 3. PPE 4. Equipment lifting capability.

0613-INST-1403: Install direct-buried cable

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided tools, ditching equipment, materials, and reference.

STANDARD: A minimum of 36 inches beneath the surface to establish connectivity between end points.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Select a cable route.
3. Prepare ditching equipment.
4. Determine correct digging depth.
5. Prepare cable.
6. Dig trench.
7. Lay cable in trench.
8. Fill trench.
9. Label cable.

REFERENCES:
1. FM 11-372-2 Outside Plant Cable Placement
2. MCO 3500.27_ Operational Risk Management (ORM)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Trenching equipment. 2. Cable for burying. 3. Labeling equipment. 4. PPE 5. Equipment lifting capability

---

0613-INST-1404: Install a pole line system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0613

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided required tools, materials, equipment, and references.

STANDARD: To extend cable infrastructure.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Prepare pole truck.
3. Auger hole for pole.
4. Cut pole to proper length.
5. Place pole in hole.
6. Secure pole in center of hole.
7. Install down guide-wires.
8. Install messenger.
9. Label pole.

REFERENCES:
1. FM 11-372-2 Outside Plant Cable Placement
2. FM 24-20 Tactical Wire and Cable Techniques
3. MCO 3500.27_ Operational Risk Management (ORM)
4. Applicable Technical Publications/Manuals

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. PPE. 2. Pole truck. 3. Chain saw. 4. Shovels. 5. Packing rod. 6. Mounting hardware. 7. Guide wire. 8. Pole sling. 9. Messenger and mounting hardware. 10. Labeling material. 11. Equipment lifting capability.

0613-MANT-1601: Perform commercial cable systems corrective maintenance

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0613

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided faulty cable, references, Test, Measurement, and Diagnostic Equipment (TMDE), materials, and tools.

STANDARD: To restore connectivity between end points.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify cable type.
3. Identify cable fault.
4. Locate cable fault.
5. Repair cable fault.
6. Conduct operational check.
7. Document authorized maintenance

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 4700-15/1_ Ground Equipment Record Procedures
3. Applicable Technical Publications/Manuals

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. PPE. 2. TMDE. 3. Cable splicing equipment. 4. Spare cable. 5. Cable splicing materials.

10002. 2000-LEVEL EVENTS

0613-OPER-2501: Operate ditching equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0613

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided tools, equipment, and reference.

STANDARD: To prepare for installation of cable infrastructure.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Configure as required.
3. Conduct operational check.
4. Operate ditching equipment.

CHAINED EVENTS: 0613-INST-1403

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. Applicable Technical Publications/Manuals

0613-MNGT-2701: Manage aerial cable installation

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0613

GRADES: CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided cable plan, personnel, tools, equipment, and references.

STANDARD: To ensure safe and proper installation of cable.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Allocate required equipment.
3. Assign required personnel.
4. Supervise project.
5. Conduct quality control inspection.

CHAINED EVENTS:
0613-INST-1401 0613-MANT-1601 0613-INST-1404
0613-INST-1402

REFERENCES:

1. FM 11-372-2 Outside Plant Cable Placement
2. FM 24-20 Tactical Wire and Cable Techniques
3. MCO 3500.27_ Operational Risk Management (ORM)

SUPPORT REQUIREMENTS:

EQUIPMENT: Cable plan

COMM T&R MANUAL

CHAPTER 11

MOS 0619 INDIVIDUAL EVENTS

CHAPTER 11

MOS 0619 INDIVIDUAL EVENTS

11000. INDEX OF INDIVIDUAL EVENTS

11001. 2000-LEVEL EVENTS

0619-PLAN-2101: Plan a Telephony Network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0619

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To support all command and control telephony requirements, per the references.

PERFORMANCE STEPS:
1. Review planning documents.
2. Identify interface requirements.
3. Evaluate subscriber secure and non-secure requirements.
4. Identify types and locations of all internal and external network interfaces.
5. Identify voice network timing relationships.
6. Identify interface parameters for each voice switch in the network.
7. Identify redundant network paths.
8. Identify cable system requirements.
9. Identify power requirements.
10. Identify grounding requirements.
11. Draft telephony network documents.
12. Submit telephony network documents for approval.

REFERENCES:
1. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications (Joint Voice Communications Systems)
2. Data, Voice and Video Cabling, 2nd Edition Author Jim Hayes, Paul Rossenberg, pub. 2005 Delmar Learning
3. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
4. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
5. MCO 3500.27_ Operational Risk Management (ORM)
6. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
7. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
8. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62
9. The Irwin Handbook of Telecommunications, Fifth Edition Author James Harry Green, 2006 Pantel Inc.

SUPPORT REQUIREMENTS:

MATERIAL: 1. Switching network diagrams. 2. Operational Risk Assessment Worksheet (ORAW).

0619-PLAN-2102: Plan a cabling system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0619

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching and data systems, multiplexing systems, termination points, and transmission mediums.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Review data, switching, multiplexing, and transmission planning documents for cable requirements.
3. Identify locations of subscribers.
4. Identify types of cable based on distance and interface requirements.
5. Determine installation priority.
6. Identify required ancillary/supporting equipment for installation.
7. Identify power requirements.
8. Identify grounding requirements.
9. Draft design documents.
10. Submit design documents for approval.

REFERENCES:
1. CX-13295/G (300m) and CX-13295/G (1000m) Operator's Manual
2. FM 11-372-2 Outside Plant Cable Placement
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
6. TIA/EIA Telecommunications Industry Association/Electronics Industry Association 568 wiring standard
7. TM 11-5805-574-24P Cable Assemblies, Assault, Communications CX-4566 (25, 50, 100, 250, 500 ft lengths)
8. TM 11-5995-208-24&P Cable Assembly, Special Purpose Cx-11230/G

0619-PLAN-2103: Plan installation of ancillary equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0619

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance and references.

STANDARD: To ensure connectivity between switching, data, multiplexing systems, terminating points, transmission mediums, and subscribers.

PERFORMANCE STEPS:
1. Review planning documents.
2. Identify ancillary equipment requirements.
3. Validate cutsheets.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 11332A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63
3. TM 11333A-OI/1 Operation and Maintenance Manual with Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62

0619-MNGT-2701: Manage a telephony network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0619

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To support all command and control telephony requirements.

PERFORMANCE STEPS:
1. Manage safety controls.
2. Manage cable system installation.
3. Manage Information Security (INFOSEC) procedures.
4. Implement quality control procedures.
5. Coordinate troubleshooting procedures.
6. Coordinate corrective action.
7. Review changes to the telephony network.
8. Submit changes for approval.

CHAINED EVENTS: 0612-MANT-2601

REFERENCES:
1. Data, Voice and Video Cabling, 2nd Edition Author Jim Hayes, Paul Rossenberg, pub. 2005 Delmar Learning
2. ISBN 0-471-45133-9 Telecommunications System Engineering, by Roger L. Freeman, 4th Edition, John Wiley and Sons, Inc., Hoboken, NJ, 2004
3. ISBN 1-58053-088-5 Telephone Switching Systems, by Richard A. Thompson, Artech House Publishing, Boston, 2000
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. TM 11332A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Remote Subscriber Access Module AN/TTC-63

7. TM 11333A-OI/1 Operation and Maintenance Manual With Components Inventory and Repair Parts Lists Deployable End Office Suite AN/TTC-62
8. The Irwin Handbook of Telecommunications, Fifth Edition Author James Harry Green, 2006 Pantel Inc.

0619-MNGT-2702: Manage a cabling system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0619

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To ensure connectivity between switching and data systems, multiplexing systems, termination points, and transmission mediums.

PERFORMANCE STEPS:
1. Supervise safety controls.
2. Supervise cable system installation.
3. Supervise physical security.
4. Implement quality control procedures.
5. Coordinate troubleshooting procedures.
6. Coordinate corrective action.
7. Review changes to the cabling network.
8. Submit changes for approval.

CHAINED EVENTS:

0612-MNGT-2704	0612-MNGT-2705	0613-OPER-2501
0613-MNGT-2701	0612-MNGT-2702	0612-MNGT-2703
0612-MNGT-2701		

RELATED EVENTS:

0619-PLAN-2102	0619-PLAN-2101	0619-MNGT-2701
0619-PLAN-2103		

REFERENCES:
1. CX-13295/G (300m) and CX-13295/G (1000m) Operator's Manual
2. FM 11-372-2 Outside Plant Cable Placement
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. TC 24-20 TACTICAL WIRE AND CABLE TECHNIQUES
6. TIA/EIA Telecommunications Industry Association/Electronics Industry Association 568 wiring standard
7. TM 11-5805-574-24P Cable Assemblies, Assault, Communications CX-4566 (25, 50, 100, 250, 500 ft lengths)
8. TM 11-5995-208-24&P Cable Assembly, Special Purpose Cx-11230/G

COMM T&R MANUAL

CHAPTER 12

MOS 0620 INDIVIDUAL EVENTS

CHAPTER 12

MOS 0620 INDIVIDUAL EVENTS

12000. INDEX OF INDIVIDUAL EVENTS

12001. 2000-LEVEL EVENTS

0620-PLAN-2101: Plan a Transmission Network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: Outline a redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Evaluate the commander's intent.
2. Analyze command available resources.
3. Evaluate area of operation terrain and frequencies limitations.
4. Determine a transmission network plan.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. MCWP 5-1 Marine Corps Planning Process (MCPP)
4. Unit SOP Unit SOP

0620-PLAN-2102: Plan a Multiplexing Network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: Outline a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Evaluate the commander's intent.

2. Analyze the transmission plan.
3. Analyze command available resources.
4. Determine a multiplexing network plan.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. MCWP 5-1 Marine Corps Planning Process (MCPP)
4. UNIT SOP Unit's Standing Operating Procedures

0620-PLAN-2103: Plan a Transmission Network for a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Outline a redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Evaluate the commander's intent.
2. Analyze command available resources.
3. Evaluate area of operation terrain and frequencies limitations.
4. Determine a transmission network plan.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. MCWP 5-1 Marine Corps Planning Process (MCPP)
4. Unit SOP Unit SOP

0620-PLAN-2104: Plan a Multiplexing Network for a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Outline a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Evaluate the commander's intent.
2. Analyze the transmission plan.
3. Analyze command available resources.
4. Determine a multiplexing network plan.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. MCWP 5-1 Marine Corps Planning Process (MCPP)
4. UNIT SOP Unit's Standing Operating Procedures

0620-DSGN-2201: Design a transmission network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Develop a redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Design a SATCOM network plan.
2. Design a terrestrial network plan.
3. Design a cable network plan.
4. Analyze a single channel radio network plan.
5. Develop transmission network plan tabs/enclosures.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. UNIT SOP Unit's Standing Operating Procedures

0620-DSGN-2202: Design a Multiplexing Network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Develop a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Design a multiplexing network plan.
2. Design a network timing plan.
3. Identify Transmission Security (TRANSEC) requirements.
4. Develop multiplexing network plan tabs/enclosures.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. Unit SOP Unit SOP

0620-DSGN-2203: Design a Transmission Network for a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Develop redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Design a SATCOM network plan.
2. Design a terrestrial network plan.
3. Design a cable network plan.
4. Analyze a single channel radio network plan.
5. Develop transmission network plan tabs/enclosures.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. UNIT SOP Unit's Standing Operating Procedures

0620-DSGN-2204: Design a Multiplexing Network for a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Develop a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Design a multiplexing network plan.
2. Design a network timing plan.
3. Identify Transmission Security (TRANSEC) requirements.
4. Develop multiplexing network plan tabs/enclosures.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. Unit SOP Unit SOP

0620-ENGR-2301: Engineer a Transmission Network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineer redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL
CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Validate transmission network design.
2. Specify equipment configurations.
3. Develop appropriate service requests.
4. Submit appropriate service requests.
5. Develop appropriate communication plan database.
6. Evaluate transmission network cut sheets.

REFERENCES:
1. ASC - 3 Army Space Circular 3
2. ASC-1 Army Space Circular 1
3. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. Unit SOP Unit SOP

0620-ENGR-2302: Engineer a Multiplexing Network for an element of a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineer a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: WO-1, CWO-2

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Validate multiplexing network design.
2. Specify equipment configurations.
3. Specify Communications Security (COMSEC) requirements.
4. Specify portside circuit characteristics.
5. Develop appropriate service requests.
6. Submit appropriate service requests.
7. Evaluate multiplexing network cutsheets.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. UNIT SOP Unit's Standing Operating Procedures

~~**0620-ENGR-2303:** Engineer a Transmission Network for a Marine Air Ground Task Force (MAGTF)~~

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineer redundant, reliable and robust transmission architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Validate transmission network design.
2. Specify equipment configurations.
3. Develop appropriate service requests.
4. Submit appropriate service requests.
5. Develop appropriate communication plan database.
6. Evaluate transmission network cut sheets.

REFERENCES:
1. ASC - 3 Army Space Circular 3
2. ASC-1 Army Space Circular 1
3. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. UNIT SOP Unit's Standing Operating Procedures

0620-ENGR-2304: Engineer a Multiplexing Network for a Marine Air Ground Task Force (MAGTF)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Engineer a redundant, reliable and robust multiplexing architecture with the flexibility to meet mission requirements.

MOS PERFORMING: 0620

GRADES: CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, commander's guidance, and references.

STANDARD: To meet the operational demands and requirements of the command.

PERFORMANCE STEPS:
1. Validate multiplexing network design.
2. Specify equipment configurations.
3. Specify Communications Security (COMSEC) requirements.
4. Specify portside circuit characteristics.
5. Develop appropriate service requests.
6. Submit appropriate service requests.

7. Evaluate multiplexing network cut sheets.

REFERENCES:

1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. UNIT SOP Unit's Standing Operating Procedures

COMM T&R MANUAL

CHAPTER 13

MOS 0621 INDIVIDUAL EVENTS

CHAPTER 13

MOS 0621 INDIVIDUAL EVENTS

13000. INDEX OF INDIVIDUAL EVENTS

13001. 1000-LEVEL EVENTS

0621-OPER-1501: Operate a tactical radio

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

DESCRIPTION: This event is designed to encompass all High Frequency, Very High Frequency, and Ultra High Frequency radio assets.

MOS PERFORMING: 0621

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Performing a successful radio check with a distant station within 45 minutes of arrival on site.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Ground equipment, if applicable
3. Install radio system.
4. Configure radio for basic operations.
5. Establish secure radio communication.
6. Utilize proper radio procedures.
7. Maintain a circuit log.
8. Employ Electronic Protection (EP) techniques, as required.
9. Troubleshoot radio system, as required.
10. Restore Radio system, as required.

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. FMFRP 3-34 Field Antenna Handbook
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCRP 3-40.3B Radio Operator's Handbook
5. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

0621-OPER-1502: Operate a tactical radio remoting device

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

DESCRIPTION: This event is designed to encompass the following equipment, but not limited to: RC-111, ANGRA-39, and OK-648

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, operational radio, and references.

STANDARD: Establishing a radio check with a distant station within 20 minutes.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Install remoting device.
3. Establish radio communication.
4. Troubleshoot radio system, as required.
5. Restore Radio system, as required.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)

0621-OPER-1503: Operate a Global Positioning System (GPS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0621

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, grid coordinates, and references.

STANDARD: Verifying your position in accordance with the grid coordinates provided, and demonstrating the ability to load time from the GPS device to a tactical radio.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Configure GPS for operation.
3. Access satellites.
4. Obtain time/almanac.
5. Obtain location.
6. Load time into tactical radio

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 09880A-10 AN/PSN-11
3. TM 09880C Satellite Signal Navigation AN/PSN 13

0621-MANT-1601: Conduct preventive maintenance checks and services (PMCS) on radio equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0621

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment and references.

STANDARD: In accordance with unit maintenance management standing operating procedures.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify hazardous waste for disposal.
3. Conduct operator PMCS as scheduled.
4. Maintain Stock Listing (SL-3).
5. Identify equipment discrepancies.
6. Induct into maintenance, as required.
7. Document authorized maintenance

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCO 5100.25 Hazardous Material Information System
4. MCO P4790.2_ MIMMS Field Procedures Manual
5. Unit SOP Unit SOP

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: This event encompasses all radio and vehicle components.

13002. 2000-LEVEL EVENTS

0621-PLAN-2101: Create a radio section Bill of Materials (BOM)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0621

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and reference.

STANDARD: Prior to the start of operations in order to meet mission requirements.

PERFORMANCE STEPS:
1. Identify the length of the mission.
2. Determine the number of communication sites.
3. Determine the amount of material support required by each site.
4. Create a Bill of Materials to support the mission.
5. Submit the Bill of Materials to appropriate agencies for acquisition.

REFERENCES:
1. UNIT SOP Unit's Standing Operating Procedures

0621-PLAN-2102: Develop a MAGTF Radio Communications Plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: This event is an enhancement to basic 2000 level events unique to Communications Marines assigned to the Marine Expeditionary Units. This training will be conducted by Expeditionary Warfare Training Group Pacific (EWTGPAC).

MOS PERFORMING: 0621

GRADES: SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and references.

STANDARD: Enable effective command and control for the MAGTF which satisfies the commanders information exchange requirement during amphibious operations.

PERFORMANCE STEPS:
1. Identify mission requirements for a MAGTF.
2. Determine radio net requirement for all supporting agencies of a MAGTF.
3. Prepare a radio guard chart for all supporting agencies of a MAGTF.

4. Prepare a radio communications diagram for all supporting agencies of a MAGTF.
5. Submit for approval.

0621-INST-2401: Construct field expedient antennas

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0621

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Ensuring that the field expedient antenna selected is compatible with the tactical radio being used.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify appropriate field expedient antenna.
3. Determine length of antenna.
4. Gather required materials.
5. Select a site.
6. Construct the antenna.
7. Connect the antenna to the radio.
8. Establish radio communication.

CHAINED EVENTS:
0621-OPER-1501 0621-OPER-1503 0621-OPER-1502

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. FMFRP 3-34 Field Antenna Handbook
3. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

0621-OPER-2501: Operate a tactical radio system with advanced configurations

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Establishing communications within 30 minutes of arrival on site.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Load 3G HF radio configurations, as applicable.
3. Load UHF Have Quick radio configurations, as applicable.
4. Load DAMA wide band and narrow band configurations, as applicable.
5. Load Internet Protocol (IP) configurations, as applicable.
6. Troubleshoot radio system, as required.
7. Restore Radio system, as required.

CHAINED EVENTS:
0621-OPER-1501 0621-OPER-1503 0621-OPER-1502

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)

0621-OPER-2502: Operate an Enhanced Position Location Reporting System (EPLRS) Radio

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Establishing communications within 1 hour of arrival on site.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Install radio system.
3. Configure radio system.
4. Establish communications with EPLRS Network Manager (ENM).
5. Troubleshoot radio system, as required.
6. Restore Radio system, as required.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)

SUPPORT REQUIREMENTS:

EQUIPMENT: CF-28 Panasonic Tough Book with EPLRS Network Manager (ENM) software.

0621-OPER-2503: Operate Commercial Satellite Communications Terminal

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: This event is designed to encompass the following equipment, but is not limited to: International Maritime Satellite (INMARSAT), Broadband Global Area Network (BGAN), Iridium, and SWE-Dish.

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Within time limit established by the commander.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Coordinate satellite access, as required.
3. Install system.
4. Configure system.
5. Establish communications.
6. Troubleshoot radio system, as required.
7. Restore Radio system, as required.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)

0621-OPER-2504: Perform advanced operations of a Data Transfer Device (DTD)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0622

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Successfully transmit key mat to the distant end user by performing Over the Air Rekey (OTAR) procedures.

PERFORMANCE STEPS:
1. Conduct Variable Generated (VG) operation.
2. Conduct Automatic Rekey (AK) operation.
3. Conduct Manual Rekey (MK) net controller to subscriber operation.
4. Conduct MK net controller to alternate net controller operation.
5. Conduct operator level maintenance.
6. Troubleshoot equipment.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

0621-MNGT-2701: Manage radio systems sites

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Ensuring compliance of all established procedures to include; employment of personnel and equipment, site security, and circuit log content.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Manage the employment/deployment of personnel and equipment.
3. Establish watch schedule.
4. Supervise watch schedule.
5. Enforce communication security measures.
6. Enforce Circuit discipline.
7. Manage radio message traffic according to Unit's Standing Operating Procedures.

REFERENCES:
1. ACP 125(D) Communication Instructions for Radio Telephone Procedures
2. ACP-131 Communications Instruction - Operating Procedures
3. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
4. Unit SOP Unit SOP

CHAPTER 14

MOS 0622 INDIVIDUAL EVENTS

CHAPTER 14

MOS 0622 INDIVIDUAL EVENTS

14000. INDEX OF INDIVIDUAL EVENTS

14001. 1000-LEVEL EVENTS

0622-OPER-1501: Operate a Line-Of-Sight (LOS) multi-channel radio system

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references

STANDARD: In order to establish communications with the distant end within an acceptable bit error rate (BER).

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Site equipment.
3. Ground equipment.
4. Install system.
5. Configure equipment.
6. Establish communications.
7. Troubleshoot, as required.
8. Restore communications, as required.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 09543A-14 Operator & Troubleshooting Checklist for Radio Terminal Set, AN/MRC-142

0622-OPER-1502: Operate a single channel radio

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0622

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Performing a successful radio check with a distant station within 45 minutes of arrival on site.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Install system.
3. Configure radio for operations.

4. Establish radio communication.
5. Troubleshoot, as required.
6. Restore communications, as required.

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. FMFRP 3-34 Field Antenna Handbook
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCRP 3-40.3B Radio Operator's Handbook
5. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

0622-MANT-1601: Conduct preventive maintenance checks and services (PMCS) on radio equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0621

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment and references.

STANDARD: In accordance with unit maintenance management standing operating procedures.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify hazardous waste for disposal.
3. Conduct operator PMCS as scheduled.
4. Maintain Stock Listing (SL-3).
5. Identify equipment discrepancies.
6. Induct into maintenance, as required.
7. Document authorized maintenance.

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCO 5100.25 Hazardous Material Information System
4. MCO P4790.2_ MIMMS Field Procedures Manual
5. Unit SOP Unit SOP

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: This is to include all radio and vehicle components.

14002. 2000-LEVEL EVENTS

0622-PLAN-2101: Select a line-of-sight multi-channel radio system location

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and references.

STANDARD: Prior to the start of operations and ensuring the area is clear of obstructions for line-of-site communications.

PERFORMANCE STEPS:
1. Plot military grid coordinates.
2. Determine elevation of plotted grid coordinates.
3. Identify all natural and manmade obstacles.
4. Determine antenna azimuth.

REFERENCES:
1. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
2. UNIT SOP Unit's Standing Operating Procedures

0622-PLAN-2102: Create a multi-channel radio section Bill of Materials (BOM)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and reference.

STANDARD: Prior to the start of operations.

PERFORMANCE STEPS:
1. Identify the length of the mission.
2. Determine the number of communication sites.
3. Determine the amount of material support required by each site.
4. Create a Bill of Materials to support the mission.
5. Submit the Bill of Materials for appropriate routing for acquisition.

REFERENCES:
1. Unit SOP Unit SOP

0622-OPER-2501: Operate a Global Positioning System (GPS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0622

GRADES: LCPL, CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, equipment, grid coordinates, and references.

STANDARD: Verifying your position in accordance with the grid coordinates provided.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Configure GPS for operation.
3. Access satellites.
4. Obtain time/almanac.
5. Obtain location.

REFERENCES:
1. TM 09880A-10 AN/PSN-11
2. TM 09880C Satellite Signal Navigation AN/PSN 13

0622-OPER-2502: Perform advanced operations of a Data Transfer Device (DTD)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0622

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: In order to perform Over the Air Rekey (OTAR) by successfully transmitting key mat to the distant end user.

PERFORMANCE STEPS:
1. Conduct Variable Generated (VG) operation.
2. Conduct Automatic Rekey (AK) operation.
3. Conduct Manual Rekey (MK) net controller to subscriber operation.
4. Conduct MK net controller to alternate net controller operation.
5. Conduct operator level maintenance.
6. Troubleshoot equipment.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. TM 11-5810-292-13 Comm Security Equip KOI-18/TSEC

0622-MNGT-2701: Manage multi-channel radio systems sites

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: By ensuring compliance of all established procedures to include: employment of personnel and equipment, site security, and circuit log content.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Manage the employment/deployment of personnel and equipment.
3. Establish watch schedule.
4. Supervise watch schedule.
5. Enforce communication security measures.
6. Enforce circuit discipline.

REFERENCES:
1. ACP 125(D) Communication Instructions for Radio Telephone Procedures
2. ACP-131 Communications Instruction - Operating Procedures
3. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment

CHAPTER 15

MOS 0623 INDIVIDUAL EVENTS

CHAPTER 15

MOS 0623 INDIVIDUAL EVENTS

15000. INDEX OF INDIVIDUAL EVENTS

15001. 1000-LEVEL EVENTS

0623-OPER-1501: Operate a AN/TRC-170(V)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0623

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provide planning documents, installed equipment, an AN/TRC-170 team, and references.

STANDARD: To establish and maintain communications services with the distant end.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Install system.
3. Monitor readings.
4. Maintain circuit logbook.
5. Troubleshoot system, as required.
6. Restore communications, as required.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 08658A-14/1 Radio Terminal Set, AN/TRC-170(V)3
3. TM 09280A-14&P/1 Operation and Maintenance Instructions with Parts List for Microwave Antenna Group, OE-468/TRC

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Tropospheric scatter radio system. 2. COMSEC equipment and material. 3. Power Source.

0623-MANT-1601: Conduct preventive maintenance checks and services on radio equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment and references.

STANDARD: In accordance with unit maintenance management standing operating procedures.

PERFORMANCE STEPS:

1. Identify safety hazards.
2. Identify hazardous waste for disposal.
3. Conduct operator PMCS as scheduled.
4. Maintain Stock Listing (SL-3).
5. Identify equipment discrepancies.
6. Induct into maintenance, as required.
7. Document authorized maintenance.

REFERENCES:

1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCO 5100.25 Hazardous Material Information System
4. MCO P4790.2_ MIMMS Field Procedures Manual
5. Unit SOP Unit SOP

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: This is to include all radio and vehicle components.

15002. 2000-LEVEL EVENTS

0623-PLAN-2101: Select troposcatter radio system location

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0623

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and references.

STANDARD: Prior to the start of operations, ensuring the site is clear of obstructions, and ensuring there will be proper distance from radiation hazards (0-950 feet).

PERFORMANCE STEPS:
1. Plot military grid coordinates.
2. Determine elevation of plotted grid coordinates.
3. Determine path resistance.
4. Identify all natural and manmade obstacles.

REFERENCES:
1. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

0623-PLAN-2102: Create a troposcatter section Bill of Materials (BOM)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0623

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and reference.

STANDARD: Prior to the start of operations.

PERFORMANCE STEPS:
1. Identify the length of the mission.
2. Determine the number of communication sites.
3. Determine the amount of material support required by each site.
4. Create a Bill of Materials to support the mission.
5. Submit the Bill of Materials for appropriate routing for acquisition.

REFERENCES:
1. UNIT SOP Unit's Standing Operating Procedures

0623-OPER-2501: Operate a Global Positioning System (GPS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0623

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, grid coordinates, and references.

STANDARD: Verify your position in accordance with the grid coordinates provided.

PERFORMANCE STEPS:
1. Access satellites.
2. Obtain time/almanac.
3. Obtain location.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. TM 11-5820-1172-13 Operator and Maintenance Manual, Defense Advanced GPS Receiver (DAGR) Satellite Signals Navigation Set AN/PSN-13

0623-OPER-2502: Perform advanced operations of a Data Transfer Device (DTD)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0623

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment and references.

STANDARD: In order to perform Over the Air Rekey (OTAR) by successfully transmitting key mat to the distant end user.

PERFORMANCE STEPS:
1. Conduct Variable Generated (VG) operation.
2. Conduct Automatic Rekey (AK) operation.
3. Conduct Manual Rekey (MK) net controller to subscriber operation.
4. Conduct MK net controller to alternate net controller operation.
5. Conduct operator level maintenance.
6. Troubleshoot equipment.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. TM 11-5810-292-13 Comm Security Equip KOI-18/TSEC

0623-MNGT-2701: Manage troposcatter radio systems sites

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0623

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment and references.

STANDARD: By ensuring compliance of all established procedures to include: employment of personnel and equipment, site security and circuit log content.

PERFORMANCE STEPS:
1. Manage the employment/deployment of personnel and equipment.
2. Establish watch schedule.
3. Supervise watch schedule.
4. Enforce communication security measures.
5. Enforce circuit discipline.

REFERENCES:
1. ACP 125(D) Communication Instructions for Radio Telephone Procedures
2. ACP-131 Communications Instruction - Operating Procedures
3. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment

COMM T&R MANUAL

CHAPTER 16

MOS 0627 INDIVIDUAL EVENTS

CHAPTER 16

MOS 0627 INDIVIDUAL EVENTS

16000. INDEX OF INDIVIDUAL EVENTS

16001. 1000-LEVEL EVENTS

0627-INST-1401: Install a satellite communications antenna

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, antenna, compass, required tools, and references.

STANDARD: In performance step sequence, within the time limits established by the Commander.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Orient the antenna support structure.
3. Remove stored equipment.
4. Level antenna support structure.
5. Assemble the antenna.
6. Install components.
7. Connect power cables.
8. Conduct power-up procedures.
9. Deploy antenna following proper procedures.
10. Install proper feed assembly.
11. Connect all configuration cables.
12. Ground the antenna.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MIL-HDBK 419A Grounding Techniques
3. TM 11-5985-431-13&P Operator's Unit and Direct Support Maintenance Manual (Including Repair Parts and Special Tools List) Antenna Communications, Trailer Mounted AS-4429/TSC
4. TM 11381A-OD/1 OPERATOR AND DIRECT SUPPORT MAINTENANCE MANUAL for Large Aperture Multi-Band Deployable Antenna AS-4429D/TSC
5. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

0627-OPER-1501: Operate a satellite communications terminal

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

DESCRIPTION: This task encompasses the operation of the following platforms but is not limited to: LMST and Phoenix.

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: Formal

CONDITION: Provided planning documents, satellite terminal equipment, TEST Measurement Diagnostic Equipment (TMDE), COMSEC equipment and software, power source, and references.

STANDARD: In performance step sequence, within the time limits established by the Commander.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Determine system site orientation
3. Position terminal.
4. Assemble antenna.
5. Install power cables.
6. Install COMSEC.
7. Install configuration cables.
8. Connect interface computing device.
9. Ground the equipment.
10. Conduct power-up procedures.
11. Check GPS.
12. Utilizing proper power up procedures, power up the terminal.
13. Configure parameters from cut sheets.
14. Deploy antenna.
15. Acquire the satellite.
16. Track the satellite.
17. Utilizing proper satellite access procedures, access designated satellite.
18. Establish the link(s).
19. Maintain the link(s).
20. Perform troubleshooting, as required.
21. Restore link as required.
22. Properly de-access satellite.
23. Complete shutdown procedures.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MIL-HDBK 419A Grounding Techniques
4. TM 10877A/10878A-12&P/1_ Operation and Maintenance Instructions w/Illustrated Parts Breakdown For SATCOM System Lightweight Multi-Band Satellite Terminal (LMST) (Transit Case)
5. TM 11358A-OI/1 Technical & Operator's Manual Satellite Communication System AN/TSC-156B
6. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Satellite Communication System. 2. Test Measurement and Diagnostic Equipment (TMDE). 3. COMSEC equipment. 4. Data Transfer Device (DTD). 5. Generator set.

0627-OPER-1502: Operate the Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0627

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided AN/TSC-154, power source, COMSEC equipment and software, and references.

STANDARD: Within the time limits established by the commander.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Determine system site orientation.
3. Level support structure.
4. Deploy stabilizer legs.
5. Connect Hand held terminal unit (HTU).
6. Install COMSEC.
7. Ground the equipment.
8. Perform power-up procedures.
9. Load database.
10. Load appropriate keys.
11. Deploy antenna.
12. Acquire satellite.
13. Create designated net.
14. Join designated net.
15. Request OTAR, as required.
16. Maintain link(s).
17. Perform Troubleshooting, as required.
18. Restore link as required.
19. Perform normal shutdown procedures.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. MCO 3500.27_ Operational Risk Management (ORM)
3. TM 10432A-12/1 Operator's and Unit Maintenance Manual for Terminal, Satellite Communication AN/TSC-154
4. TM 10433-30/2 Direct Support Maintenance Manual for Satellite Communication Terminal AN/TSC-154

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T). 2. Test Measurement and Diagnostic Equipment. (TMDE). 3. Data Transfer Device (DTD). 4. Generator set. 5. Compass. 6. Tools.

0627-MANT-1601: Complete satellite communications terminal Preventive Maintenance (PM)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0627

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, satellite terminal equipment, power source, required tools, Test Measurement Diagnostic Equipment (TMDE), and references.

STANDARD: In accordance with unit maintenance standing operating procedures.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Ensure all equipment is free of dirt, debris, rust, and corrosion.
3. Employ Built in Testing (BIT) software.
4. Identify faulty component(s).
5. Replace faulty component(s) as required.
6. Verify repair by performing equipment operational inspection.
7. Document authorized maintenance.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. MCO P4790.2_ MIMMS Field Procedures Manual
3. TM 4700-15/1_ Ground Equipment Record Procedures
4. Applicable Satellite Communication Terminal Technical Manuals

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Satellite Communication System. 2. Test Measurement and Diagnostic Equipment (TMDE). 3. COMSEC equipment. 4. Generator Set. 5. Tools.

16002. 2000-LEVEL EVENTS

0627-PLAN-2101: Create a satellite communications section Bill of Materials (BOM)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0627

GRADES: CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents and references.

STANDARD: Prior to the start of operations.

PERFORMANCE STEPS:
1. Identify the length of the mission.
2. Determine number of communication sites.
3. Determine amount of material support required by each site.
4. Create a Bill of Materials to support the mission.
5. Submit the Bill of Materials for purchase.

REFERENCES:
1. Operations Order Annex K
2. Unit SOP Unit SOP

0627-PLAN-2102: Conduct a site survey

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0627

GRADES: CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents, compass, maps, satellite elevation, azimuth, and take-off angle.

STANDARD: In accordance with the unit's requirements and commander's intent.

PERFORMANCE STEPS:
1. Identify mission requirements.
2. Determine location of satellite communication terminal.
3. Identify clear-sky obstructions to selected satellite.
4. Identify force protection limitations.
5. Identify power requirements.
6. Draw a layout of the site.
7. Brief team members on the execution of the plan.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. Operations Order Annex K
3. Unit SOP Unit SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: Compass

0627-PLAN-2103: Determine Satellite Access Request (SAR) requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0627

GRADES: CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided planning documents and references.

STANDARD: To complete SAR.

PERFORMANCE STEPS:
1. Provide terminal type.
2. Provide terminal capabilities.
3. Provide crypto key requirements.
4. Submit draft SAR to Communications Planner.

REFERENCES:
1. CJCSM 6231.04B MANUAL FOR EMPLOYING TACTICAL COMMUNICATIONS
2. Operations Order Annex K

0627-OPER-2501: Perform proper generator power-up procedures

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0627

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided generator set and references.

STANDARD: In performance step sequence, within the time limits established by the Commander.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Maintain ground.

3. Check gauges for acceptable generator parameters.
4. Power-up generator.
5. Check frequency, voltage, and amperage levels.
6. Execute terminal power up procedures.

REFERENCES:
1. MCO 3500.27_ Operational Risk Management (ORM)
2. Applicable Technical Publications/Manuals

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Generator set. 2. Tools.

0627-OPER-2502: Perform advanced operations of a Data Transfer Device (DTD).

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0622

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: In order to perform Over the Air Rekey (OTAR) by successfully transmitting key mat to the distant end user.

PERFORMANCE STEPS:
1. Conduct Variable Generated (VG) operation.
2. Conduct Automatic Rekey (AK) operation.
3. Conduct Manual Rekey (MK) net controller to subscriber operation.
4. Conduct MK net controller to alternate net controller operation.
5. Conduct operator level maintenance.
6. Troubleshoot equipment.

0627-MANT-2601: Supervise satellite communications terminal preventive maintenance

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0627

GRADES: CPL, SGT

INITIAL TRAINING SETTING: MOJT

CONDITION: With the aid of references, and provided a satellite communication terminal and Equipment Repair Order (ERO).

STANDARD: Ensuring the equipment is clean, rust free, SL-3 complete, and Operational.

PERFORMANCE STEPS:
1. Supervise satellite PMCS.
2. Properly open an Equipment Repair Order (ERO), as required.
3. Properly close an Equipment Repair Order (ERO), as required.
4. Verify Equipment Repair Order (ERO) status on Daily Progress Report (DPR).

REFERENCES:
1. MCO P4790.2_ MIMMS Field Procedures Manual
2. Applicable Satellite Communication Terminal Technical Manuals

SUPPORT REQUIREMENTS:

EQUIPMENT: Satellite Communication Terminal.

MATERIAL: Equipment Repair Order (ERO) forms.

COMM T&R MANUAL

CHAPTER 17

MOS 0629 INDIVIDUAL EVENTS

CHAPTER 17

MOS 0629 INDIVIDUAL EVENTS

17000. INDEX OF INDIVIDUAL EVENTS

17001. 2000-LEVEL EVENTS

0629-PLAN-2101: Prepare a radio mission plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0629

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, and references.

STANDARD: To support all tactical radio requirements including single channel, multi-channel, terrestrial, and satellite communications.

PERFORMANCE STEPS:
1. Review planning documents.
2. Identify mission requirements.
3. Identify the locations of communication nodes.
4. Determine radio link reliability, using available hardware/software engineering analysis tools.
5. Determine transmission system requirements and availability.
6. Determine personnel requirements.
7. Determine power requirements.
8. Identify resource shortfalls and request support.
9. Determine the employment/deployment of personnel and equipment.
10. Determine antenna site.
11. Develop the Automated Communications Electronic Operating Instructions (ACEOI).
12. Develop radio guard chart
13. Determine CMS/EKMS requirements.
14. Determine network timing relationships.
15. Complete crew assignment worksheet.
16. Coordinate channelization with wire plan.
17. Submit frequency request.
18. Submit SAR/GAR.
19. Prepare an estimate of supportability for a communications plan.
20. Develop radio plan.
21. Submit radio plan.

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
3. MCWP 3-1 Ground Combat Operations
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

0629-PLAN-2102: Create a SPEED profile

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0629

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and references.

STANDARD: Utilizing provided grid coordinates, specific radio and frequency range and ensuring optimal radio operations.

PERFORMANCE STEPS:
1. Input operational parameters.
2. Analyze radio links.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. SPEED-SUM-001-ROCO Software User's Manual

0629-PLAN-2103: Plan field expedient antenna installation

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0629

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To ensure antennas offer maximum effectiveness and associated with the proper tactical high-frequency (HF) radio for radio operations.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify proper location for field expedient antenna.
3. Identify the proper antenna configuration.
4. Identify the correct length of antenna.

REFERENCES:
1. FM 24-18 Tactical Single-Channel Radio Communications Techniques
2. FMFRP 3-34 Field Antenna Handbook
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. TM 9406-15 Grounding Procedures for Electromagnetic Interference Control and Safety (Aug 91)

0629-MNGT-2701: Manage the radio transmissions plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0629

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents and references.

STANDARD: In order to meet all mission requirements, radio nets and location to include personnel, equipment and logistical requirements.

PERFORMANCE STEPS:
1. Supervise the employment of personnel.
2. Supervise the employment of COMSEC.
3. Supervise the employment of transmission systems.
4. Supervise radio systems logistical re-supply.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
3. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
4. EKMS-1 (Series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

0629-MNGT-2702: Supervise the maintenance cycle of tactical radio equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0629

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, Commander's guidance, and references.

STANDARD: Ensuring the equipment meets unit readiness standards of mission capable.

PERFORMANCE STEPS:
1. Supervise equipment induction into the maintenance cycle.
2. Monitor equipment maintenance progress.
3. Brief equipment status to higher.
4. Reconcile equipment reports with appropriate authority.
5. Supervise equipment return from maintenance cycle.
6. Supervise quarterly CMR reconciliations.

REFERENCES:
1. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio

Procedures in Joint Environment
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. TM 4700-15/1_ Ground Equipment Record Procedures
4. TM 4790.2_ MIMMS Field Procedures Manual
5. UM 4790-5 MIMMS AIS, Field Maintenance Procedures

CHAPTER 18

MOS 0640 INDIVIDUAL EVENTS

CHAPTER 18

MOS 0640 INDIVIDUAL EVENTS

18000. INDEX OF INDIVIDUAL EVENTS

18001. 2000-LEVEL EVENTS

0640-PLAN-2101: Write a spectrum management appendix to Annex K

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Task is applicable to a MAGTF, MARFOR, or Joint Command.

MOS PERFORMING: 0640

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Commander's guidance, planning documents, and references.

STANDARD: To produce the spectrum management appendix to Annex K of the operations order.

PERFORMANCE STEPS:
1. Determine pertinent existing policy and procedures.
2. Identify and define roles, responsibilities and operational relationships.
3. Identify and define submission criteria.
4. Produce the spectrum management appendix to Annex K of the operations order.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
6. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
7. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
8. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
9. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
10. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
11. DODI 5000.01 The Defense Acquisition System
12. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
13. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
14. DoDD 4650.1 Policy for Management and Use of the Electromagnetic Spectrum
15. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
16. DoDI 5000.2 Operation of the Defense Acquisition System
17. JANAP 119 Joint Voice Call Sign Book
18. JSC-HDBK-05-001 Joint Spectrum Management Handbook
19. Joint Pub 3-13.1 Electronic Warfare

20. Joint Pub 3-30 Command and Control of Joint Air Operations
21. Joint Pub 3-31 Command and Control for Joint Land Operations.
22. Joint Pub 3-32 Command and Control for Joint Maritime Operations 8 August 2006Incorporating Change 127 May 2008
23. Joint Pub 6-0 Joint Communications System, 10 June 2010.
24. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
25. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
26. MCO 2410.2_ Electromagnetic Environmental Effects (E3) Control Program
27. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
28. MCWP 3-40.5 Electronic Warfare
29. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management
30. Installation Spectrum Management Guide

0640-MNGT-2701: Supervise the maintenance of electromagnetic spectrum management databases

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Commander's guidance, planning documents, and references.

STANDARD: To maintain frequency assignments in the appropriate spectrum management databases for major subordinate commands.

PERFORMANCE STEPS:
1. Ensure spectrum management systems and automated tools are operating most current software versions.
2. Create user accounts as necessary.
3. Perform data exchanges as necessary.
4. Ensure frequency assignments are reviewed, validated and updated prior to expiration.
5. Submit for modifications and frequency assignments as required.
6. Ensure frequency assignments are properly registered in appropriate spectrum management databases.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
3. JANAP 119 Joint Voice Call Sign Book
4. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
5. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
6. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0640-MNGT-2702: Supervise Host Nation Coordination (HNC)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a frequency request or request for spectrum supportability.

STANDARD: To ensure host nation coordination has been completed prior to operation of the system.

PERFORMANCE STEPS:
1. Identify and verify spectrum certification and/or host nation coordination status.
2. Coordinate with appropriate acquisition, Service and Joint level spectrum management agencies.
3. Ensure appropriate spectrum management databases are updated.
4. Submit updates as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. ACP 194 Policy for the Coordination of Military Radio Frequency Allocations and Assignments between Cooperating Nations
3. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
4. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
5. DODD 5000.1 The Defense Acquisition System
6. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
7. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
8. DoDD 4650.1 Policy for Management and Use of the Electromagnetic Spectrum
9. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
10. MCO 2410.2_ Electromagnetic Environmental Effects (E3) Control Program
11. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
12. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0640-MNGT-2703: Determine electromagnetic spectrum requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: spectrum requirements from subordinate commands.

STANDARD: To produce the spectrum requirements summary in support of a MAGTF, MARFOR or Joint command.

PERFORMANCE STEPS:
1. Publish a spectrum data call.
2. Collect spectrum requirements.
3. Consolidate and analyze spectrum requirements.
4. Produce the spectrum requirements summary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
4. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
5. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
6. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
7. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
8. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
9. JANAP 119 Joint Voice Call Sign Book
10. Joint Pub 3-13.1 Electronic Warfare
11. Joint Pub 6-0 Joint Communications System, 10 June 2010.
12. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
13. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
14. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
15. MCWP 3-40.5 Electronic Warfare
16. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0640-MNGT-1704: Supervise the development of the Joint Communication Electronics Operation Instruction (JCEOI)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided with Joint Standard automated tools, and a spectrum requirements summary or Master Net List (MNL).

STANDARD: To produce a JCEOI and SINCGARS hopset resources in support of a MAGTF, MARFOR or Joint command.

PERFORMANCE STEPS:
1. Develop the Master Net List (MNL).
2. Generate frequency requests.
3. Submit and coordinate frequency requests.
4. Obtain approved frequency assignments.
5. Generate the JCEOI.

6. Generate the SINCGARS hopset resources.
7. Publish approved JCEOI and SINCGARS hopset resources.
8. Update and maintain as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
3. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
4. JANAP 119 Joint Voice Call Sign Book
5. JSC-HDBK-05-001 Joint Spectrum Management Handbook
6. Joint Pub 6-0 Joint Communications System, 10 June 2010.
7. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
8. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

0640-MNGT-2705: Supervise the development of the Joint Restricted Frequency List (JRFL)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided with JRFL recommendations, Commander's guidance and planning documents.

STANDARD: To produce the JRFL in support of a MAGTF, MARFOR or Joint command.

PERFORMANCE STEPS:
1. Identify priority friendly command and control frequencies.
2. Identify international distress, navigation and safety-of-life/flight frequencies.
3. Identify enemy frequencies to be exploited.
4. Coordinate electronic warfare deconfliction.
5. Publish approved JRFL.
6. Update and maintain as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
6. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
7. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08

8. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
9. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
10. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
11. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
12. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
13. JSC-HDBK-05-001 Joint Spectrum Management Handbook
14. Joint Pub 3-13.1 Electronic Warfare
15. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
16. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
17. MCWP 3-40.5 Electronic Warfare
18. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0640-MNGT-2706: Supervise spectrum supportability and certification

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a frequency request or request for spectrum supportability.

STANDARD: To ensure equipment supportability and certification has been completed prior to operation of the system.

PERFORMANCE STEPS:
1. Identify and verify spectrum certification and/or host nation coordination status.
2. Coordinate with appropriate acquisition, Service and Joint level spectrum management agencies.
3. Ensure appropriate spectrum management databases are updated.
4. Submit updates as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
4. DODD 5000.1 The Defense Acquisition System
5. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
6. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
7. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
8. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
9. MCO 2410.2_ Electromagnetic Environmental Effects (E3) Control Program

10. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
11. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0640-PROT-2801: Supervise Joint Spectrum Interference Resolution

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the details of an electromagnetic interference (EMI) event.

STANDARD: To produce and submit a JSIR report in support of a MAGTF, MARFOR or Joint command.

PERFORMANCE STEPS:
1. Ensure the victim and co-located systems are operating in accordance with their authorized frequency assignments.
2. Analyze appropriate spectrum management databases to identify potential sources of interference.
3. Coordinate and deconflict victim system with electronic warfare (EW) operations.
4. Produce and submit a JSIR report.
5. Coordinate mitigation efforts to resolve EMI effects to victim systems.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
6. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
7. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
8. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
9. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
10. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
11. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
12. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
13. JCS-HDBK-05-001 Joint Spectrum Management Handbook
14. Joint Pub 3-13.1 Electronic Warfare
15. Joint Pub 6-0 Joint Communications System, 10 June 2010.
16. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum

17. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
18. MCWP 3-40.5 Electronic Warfare
19. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

CHAPTER 19

MOS 0648 INDIVIDUAL EVENTS

CHAPTER 19

MOS 0648 INDIVIDUAL EVENTS

19000. INDEX OF INDIVIDUAL EVENTS

19001. 2000-LEVEL EVENTS

0648-PLAN-2101: Write a spectrum management appendix to Annex K

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Commander's guidance, planning documents, and references.

STANDARD: To produce the spectrum management appendix to Annex K of the operations order.

PERFORMANCE STEPS:
1. Determine pertinent existing policy and procedures.
2. Identify and define roles, responsibilities and operational relationships.
3. Identify and define submission criteria.
4. Produce the spectrum management appendix to Annex K of the operations order.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
6. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
7. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
8. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
9. DODD 5000.1 The Defense Acquisition System
10. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
11. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
12. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
13. JSC-HDBK-05-001 Joint Spectrum Management Handbook
14. Joint Pub 3-13.1 Electronic Warfare
15. Joint Pub 3-30 Command and Control of Joint Air Operations
16. Joint Pub 3-31 Command and Control for Joint Land Operations.
17. Joint Pub 3-32 Command and Control for Joint Maritime Operations 8 August 2006Incorporating Change 127 May 2008
18. Joint Pub 6-0 Joint Communications System, 10 June 2010.
19. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
20. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
21. MCO 2410.2A Electromagnetic Environmental Effects (E3) Control Program

22. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
23. MCWP 3-40.5 Electronic Warfare
24. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0648-DSGN-2201: Determine electromagnetic spectrum requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided spectrum requirements from subordinate commands.

STANDARD: To produce a spectrum requirements summary.

PERFORMANCE STEPS:
1. Publish a spectrum data call.
2. Collect spectrum requirements.
3. Consolidate and analyze spectrum requirements.
4. Produce the spectrum requirements summary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
4. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
5. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
6. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
7. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
8. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
9. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
10. JANAP 119 Joint Voice Call Sign Book
11. Joint Pub 3-13.1 Electronic Warfare
12. Joint Pub 6-0 Joint Communications System, 10 June 2010.
13. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
14. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
15. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
16. MCWP 3-40.5 Electronic Warfare
17. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0648-DSGN-2202: Develop the Communication Electronics Operation Instruction (CEOI)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided with Joint Standard automated tools, and a spectrum requirements summary or Master Net List (MNL).

STANDARD: To produce a CEOI and SINCGARS hopset resource.

PERFORMANCE STEPS:
1. Develop the Master Net List (MNL).
2. Generate frequency requests.
3. Submit and coordinate frequency requests.
4. Obtain approved frequency assignments.
5. Generate the CEOI.
6. Generate the SINCGARS hopset resource.
7. Publish approved CEOI and SINCGARS hopset resource.
8. Update and maintain as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
4. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
5. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
6. JANAP 119 Joint Voice Call Sign Book
7. JSC-HDBK-05-001 Joint Spectrum Management Handbook
8. Joint Pub 6-0 Joint Communications System, 10 June 2010.
9. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
10. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
11. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

0648-DSGN-2203: Develop the Restricted Frequency List (RFL)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided with RFL recommendations, Commander's guidance and planning documents.

STANDARD: To produce the RFL.

PERFORMANCE STEPS:
1. Identify priority friendly command and control frequencies.
2. Identify international distress, navigation and safety-of-life/flight frequencies.
3. Identify enemy frequencies to be exploited.
4. Coordinate electronic warfare deconfliction.
5. Publish approved RFL.
6. Update and maintain as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSI 3320.03 Joint Communications Electronic Operating Instructions
6. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
7. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
8. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
9. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
10. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
11. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
12. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
13. JANAP 119 Joint Voice Call Sign Book
14. JSC-HDBK-05-001 Joint Spectrum Management Handbook
15. Joint Pub 3-13.1 Electronic Warfare
16. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
17. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
18. MCWP 3-40.5 Electronic Warfare
19. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0648-MANT-2601: Maintain electromagnetic spectrum management databases

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Commander's guidance, planning documents, and references.

STANDARD: To maintain frequency assignments in the appropriate spectrum management databases.

PERFORMANCE STEPS:
1. Ensure spectrum management systems and automated tools are operating most current software versions.
2. Create user accounts as necessary.
3. Perform data exchanges as necessary.
4. Ensure frequency assignments are reviewed, validated and updated prior to expiration.
5. Submit for modifications and frequency assignments as required.
6. Ensure frequency assignments are properly registered in appropriate spectrum management databases.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
3. JANAP 119 Joint Voice Call Sign Book
4. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format
5. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
6. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0648-MNGT-2701: Manage spectrum certification

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided a frequency request.

STANDARD: To ensure equipment certification and/or host nation coordination has been completed prior to operation of the system.

PERFORMANCE STEPS:
1. Identify and verify spectrum certification and/or host nation coordination using the appropriate databases.
2. Submit updates as necessary.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
4. DODD 5000.1 The Defense Acquisition System
5. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
6. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
7. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
8. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
9. MCO 2410.2A Electromagnetic Environmental Effects (E3) Control Program

10. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
11. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

---

0648-PROT-2801: Conduct electromagnetic spectrum interference resolution

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the details of an electromagnetic interference (EMI) event.

STANDARD: To produce and submit a spectrum interference report.

PERFORMANCE STEPS:
1. Ensure the victim and co-located systems are operating in accordance with their authorized frequency assignments.
2. Analyze appropriate spectrum management databases to identify potential sources of interference.
3. Coordinate and deconflict victim system with electronic warfare (EW) operations.
4. Produce and submit an interference report.

REFERENCES:
1. ACP 190 Guide to Spectrum Management in Military Operation
2. CJCSI 3320.01B ELECTROMAGNETIC SPECTRUM USE IN JOINT MILITARY OPERATIONS 1 May 2005
3. CJCSI 3320.02B Joint Spectrum Interference Resolution (JSIR)
4. CJCSI 3320.02C-1 Classified Supplement to the Joint Spectrum Interference Resolution (JSIR)
5. CJCSM 3212.02B Performing Electronic Attack in the United States and Canada for Tests, Training and Exercises
6. CJCSM 3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada, 15 Dec 08
7. CJCSM 3212.03-1 Classified Supplement to Performing Tests, Training and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
8. CJCSM 3320.01A Joint Operations in the Electromagnetic Battlespace
9. CJCSM 3320.02A Joint Spectrum Interference Resolution (JSIR) Procedures
10. DoD Guide DoD Frequency Assignment and Equipment Spectrum Certification Security guide".
11. DoDD 3222.3 DoD Electromagnetic Environmental Effects (E3) Program
12. DoDI 4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
13. JSC-HDBK-05-001 Joint Spectrum Management Handbook
14. Joint Pub 3-13.1 Electronic Warfare
15. Joint Pub 6-0 Joint Communications System, 10 June 2010.
16. MCO 2400.2 USMC Mgmt of Radio Frequency Spectrum
17. MCO 2410.2A Electromagnetic Environmental Effects (E3) Control Program
18. MCWP 3-40.3 MAGTF Communications System, 8 January 2010

19. MCWP 3-40.5 Electronic Warfare
20. NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management

CHAPTER 20

MOS 0650 INDIVIDUAL EVENTS

CHAPTER 20

MOS 0650 INDIVIDUAL EVENTS

20000. INDEX OF INDIVIDUAL EVENTS

20001. 2000-LEVEL EVENTS

0650-PLAN-2101: Plan a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: DESCRIPTION: T&R Event should be accomplished at the MSC, MEF, MARFOR, and Joint/Coalition commands.

MOS PERFORMING: 0650

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters Annex K and references.

STANDARD: That provides secure, reliable, and scalable communications in support of the commander's operational requirements.

PERFORMANCE STEPS:
1. Plan the LAN architecture.
2. Plan the WAN architecture.
3. Plan the NOS architecture.
4. Plan the virtualization Architecture.
5. Plan the COOP/DR architecture.
6. Plan the messaging architecture.
7. Plan the network assurance architecture.
8. Validate MSC basic data network concept.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. DoD Directive O-8530.1 Computer Network Defense
4. DoDD 8500.1 Information Assurance (IA)
5. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
6. Joint Pub 6-0 Joint Communications System, 10 June 2010.
7. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
8. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
9. Tri-MEF SOP Tri-MEF Communication SOP

0650-PLAN-2102: Develop a Cyberspace Network Operations (CNO) plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: T&R Event is accomplished at the MSC, MEF, MARFOR, and Joint/Combined Component Command levels.

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters CNO plans, higher Headquarters Annex K, and references.

STANDARD: That supports the commanders operational requirements.

PERFORMANCE STEPS:
1. Identify Cyberspace Network Operations (CNO) requirements.
2. Develop Cyberspace Network Management plan.
3. Develop Cyberspace Network Assurance plan.
4. Develop Cyberspace Content Management plan.
5. Validate CNO plan.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. Deputy Secretary of Defense Deputy Secretary of Defense CyberOps Memorandum, 15 October 2008
3. DoD Capstone Concept DoD Capstone Concept for Joint Operations, Version 3.0, 15 January 2009
4. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
5. Gray Book Gray Book, Marine Corps Operating Concepts for a Changing Security Environment, March 2006
6. Joint Operating Concept Joint Operating Concept Version 2.0, Irregular Warfare: Countering Irregular Threats, 17 May 2010
7. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
8. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
9. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
10. National Military Strategy for Cyberspace Operations National Military Strategy for Cyberspace Operations, December 2006
11. National Security Strategy National Security Strategy, May 2010
12. Operation/Exercise Order
13. TRADOC Pamphlet 525-7-8 TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010
14. Tri-MEF SOP Tri-MEF Communication SOP
15. UNIT SOP Unit's Standing Operating Procedures
16. UNIT T/O&E Unit's Table of Organization and Equipment
17. USMC Cyberspace Concept USMC Cyberspace Concept, 17 July 2009

0650-DSGN-2201: Design a CNO plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: T&R Event is accomplished at the MSC, MEF, MARFOR, and Joint/Combined Component Command levels.

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters CNO plans, higher Headquarters operations order, and references.

STANDARD: To support the commanders integrated, operational requirements.

PERFORMANCE STEPS:
1. Design Cyberspace Network Management (CNM) plan.
2. Design Cyberspace Network Assurance (CNA) plan.
3. Design Cyberspace Content Management (CCM) plan.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. Deputy Secretary of Defense Deputy Secretary of Defense CyberOps Memorandum, 15 October 2008
3. DoD Capstone Concept DoD Capstone Concept for Joint Operations, Version 3.0, 15 January 2009
4. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
5. Gray Book Gray Book, Marine Corps Operating Concepts for a Changing Security Environment, March 2006
6. Joint Operating Concept Joint Operating Concept Version 2.0, Irregular Warfare: Countering Irregular Threats, 17 May 2010
7. Joint Pub 6-0 Joint Communications System, 10 June 2010.
8. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
10. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
11. National Military Strategy for Cyberspace Operations National Military Strategy for Cyberspace Operations, December 2006
12. National Security Strategy National Security Strategy, May 2010
13. Operation/Exercise Order
14. TRADOC Pamphlet 525-7-8 TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010
15. The National Security Strategy to Secure Cyberspace The National Strategy to Secure Cyberspace, February 2003
16. Tri-MEF SOP Tri-MEF Communication SOP
17. UNIT SOP Unit's Standing Operating Procedures
18. UNIT T/O&E Unit's Table of Organization and Equipment
19. USMC Cyberspace Concept USMC Cyberspace Concept, 17 July 2009

0650-DSGN-2202: Design a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: This T&R event should be accomplished at the MSC, MEF, MARFOR, and Joint/Coalition commands.

MOS PERFORMING: 0650

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters' Annex K and references.

STANDARD: That provides secure, reliable, and scalable communications in support of the commander's operational requirements.

PERFORMANCE STEPS:
1. Design the LAN architecture.
2. Design the WAN architecture.
3. Design the Network Operating System (NOS) architecture.
4. Design MSC Messaging architectures.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. DoD Directive O-8530.1 Computer Network Defense
4. DoDD 8500.1 Information Assurance (IA)
5. JP6-0 Joint Communications System
6. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
7. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)

0650-ENGR-2301: Engineer a Data Network Architecture

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: This T&R event should be accomplished at the MSC, MEF, MARFOR, and Joint/Coalition commands.

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters Annex K and references.

STANDARD: That provides secure, reliable, and scalable communications in support of the commander's operational requirements.

PERFORMANCE STEPS:
1. Engineer the LAN Architecture.
2. Engineer the WAN Architecture.
3. Engineer the Network Operating System (NOS) architecture.
4. Engineer the messaging architecture.
5. Engineer the Network Defense Architecture.
6. Engineer the Continuity of operations (COOP) / Disaster Recovery (DR) Architecture.
7. Engineer the Virtualization Architecture.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. CJCSM 6231.02B Manual for the Employment of Joint Tactical Communications

(Joint Voice Communications Systems)
3. DoD Directive O-8530.1 Computer Network Defense
4. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
5. JP6-0 Joint Communications System
6. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
7. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)

0650-MNGT-2701: Manage data network operations commodity section operational readiness

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0650

GRADES: WO-1, CWO-2, CWO-3

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Commander's guidance, Commanders Critical Information Requirements, organic resources, Standard Operating Procedures and references.

STANDARD: That supports a mission capable status as defined in the units Standard Operating Procedures.

PERFORMANCE STEPS:
1. Review commander's guidance.
2. Maintain accountability of personnel.
3. Maintain accountability of equipment.
4. Supervise appropriate level of maintenance.
5. Inspect commodity area Turnover Folders or Desktop Procedures.

REFERENCES:
1. DoDD 7730.65 Department of Defense Readiness Reporting System (DRRS)
2. FMFM 0-1 UNIT TRAINING MANAGEMENT GUIDE.
3. MCBUL 3000 Marine Corps Automated Readiness Evaluation System (MARES) Equipment
4. MCO P4790.2_ MIMMS Field Procedures Manual

0650-MNGT-2702: Manage Information Technology (IT) projects

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0650

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Commander's guidance.

STANDARD: That meets the parameters established by the Commander.

PERFORMANCE STEPS:
1. Verify IT project requirement.
2. Create life cycle documentation.
3. Create a Plan of Action and Milestones (POA&M).
4. Supervise IT project development.
5. Communicate periodic updates of IT project.
6. Supervise IT project testing.
7. Supervise IT project implementation.
8. Report IT project results.
9. Execute life cycle management plan.
10. Act as a contracting officer representative, as required.
11. Act as a contracting officer technical representative, as required.

REFERENCES:
1. DOD 5200.28 Security Requirements for Automated Information Systems (AIS)
2. DOD 5200.28-STD DOD Trusted Computer System Evaluation Criteria
3. DoDD 5200.40 DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
4. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
5. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
6. UNIT SOP Unit's Standing Operating Procedures
7. Applicable Contract Documentation
8. Applicable Technical Publications/Manuals
9. Application Language Specific Manual

0650-MNGT-2703: Manage strategic C4 programs, operations and actions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0650

GRADES: CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Commander's guidance.

STANDARD: That meets the parameters established by the Commander.

PERFORMANCE STEPS:
1. Analyze commander's/director's priorities.
2. Evaluate appropriate C4 courses of action.
3. Create C4 plan of action and milestones.
4. Coordinate with outside agencies.
5. Manage support functions for the Marine Corps Enterprise Network.

6. Manage program life cycle.
7. Determine Total Cost of Ownership.
8. Develop a Continuity of Operations Plan.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. DoD Directive O-8530.1 Computer Network Defense
4. DoDD 8500.1 Information Assurance (IA)
5. JP6-0 Joint Communications System
6. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
7. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
8. Operation/Exercise Order
9. UNIT SOP Unit's Standing Operating Procedures
10. UNIT T/O&E Unit's Table of Organization and Equipment

0650-MNGT-2704: Manage a CNO plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: T&R Event is accomplished at the MSC, MEF, MARFOR, and Joint/Combined Component Command levels.

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, higher Headquarters CNO plans, higher Headquarters operations order, and references.

STANDARD: To support the commanders integrated, operational requirements.

PERFORMANCE STEPS:
1. Supervise CNO architecture development.
2. Supervise Cyberspace Network Management (CNM) plan.
3. Supervise Cyberspace Network Assurance (CNA) plan.
4. Supervise Cyberspace Content Management (CCM) plan.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. Deputy Secretary of Defense Deputy Secretary of Defense CyberOps Memorandum, 15 October 2008
3. DoD Capstone Concept DoD Capstone Concept for Joint Operations, Version 3.0, 15 January 2009
4. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
5. Gray Book Gray Book, Marine Corps Operating Concepts for a Changing Security Environment, March 2006
6. Joint Operating Concept Joint Operating Concept Version 2.0, Irregular Warfare: Countering Irregular Threats, 17 May 2010
7. Joint Pub 6-0 Joint Communications System, 10 June 2010.

8. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
10. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
11. National Military Strategy for Cyberspace Operations National Military Strategy for Cyberspace Operations, December 2006
12. National Security Strategy National Security Strategy, May 2010
13. Operation/Exercise Order
14. TRADOC Pamphlet 525-7-8 TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010
15. The National Security Strategy to Secure Cyberspace The National Strategy to Secure Cyberspace, February 2003
16. Tri-MEF SOP Tri-MEF Communication SOP
17. UNIT SOP Unit's Standing Operating Procedures
18. UNIT T/O&E Unit's Table of Organization and Equipment
19. USMC Cyberspace Concept USMC Cyberspace Concept, 17 July 2009

0650-MNGT-2705: Obtain Information Assurance Management (IAM) Level I certification

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 24 months

GRADES: CAPT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the criteria set by DoD 8570.01_and C4 Information Assurance workforce memorandum, dtd 10 Dec 2008.

STANDARD: Within six months of being assigned to an IAM Level I billet.

PERFORMANCE STEPS:
1. Achieve certification.
2. Demonstrate proficiency in IAM Level II knowledge and skills.

REFERENCES:
1. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management

---

0650-MNGT-2706: Obtain Information Assurance Management (IAM) Level II certification

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 24 months

GRADES: CAPT, MAJ

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the criteria set by DoD 8570.01_and C4 Information Assurance workforce memorandum, dtd 10 Dec 2008.

STANDARD: Within six months of being assigned to an IAM Level II billet.

PERFORMANCE STEPS:
1. Achieve certification.
2. Demonstrate proficiency in IAM Level II knowledge and skills.

REFERENCES:
1. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management

---

0650-MNGT-2707: Obtain Information Assurance Management (IAM) Level III certification

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 24 months

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the criteria set by DoD 8570.01_and C4 Information Assurance workforce memorandum, dtd 10 Dec 2008.

STANDARD: Within six months of being assigned to an IAM Level III billet.

PERFORMANCE STEPS:
1. Achieve certification.

0650-MNGT-2708: Write CNO documentation

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided commander's guidance, higher Headquarters Annex K and references.

STANDARD: To support the commander’s operational requirements.

PERFORMANCE STEPS:
1. Analyze requirements.
2. Conduct research.
3. Draft, staff, and finalize document.
4. Supervise implementation.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. Deputy Secretary of Defense Deputy Secretary of Defense CyberOps Memorandum, 15 October 2008

3. DoD Capstone Concept DoD Capstone Concept for Joint Operations, Version 3.0, 15 January 2009
4. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
5. Gray Book Gray Book, Marine Corps Operating Concepts for a Changing Security Environment, March 2006
6. Joint Operating Concept Joint Operating Concept Version 2.0, Irregular Warfare: Countering Irregular Threats, 17 May 2010
7. Joint Pub 6-0 Joint Communications System, 10 June 2010.
8. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
10. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
11. National Military Strategy for Cyberspace Operations National Military Strategy for Cyberspace Operations, December 2006
12. National Security Strategy National Security Strategy, May 2010
13. Operation/Exercise Order
14. TRADOC Pamphlet 525-7-8 TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010
15. The National Security Strategy to Secure Cyberspace The National Strategy to Secure Cyberspace, February 2003
16. Tri-MEF SOP Tri-MEF Communication SOP
17. UNIT SOP Unit's Standing Operating Procedures
18. UNIT T/O&E Unit's Table of Organization and Equipment
19. USMC Cyberspace Concept USMC Cyberspace Concept, 17 July 2009

0650-MNGT-2709: Manage CNO commodity section operational readiness

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Commander's guidance, Commanders Critical Information Requirements, organic resources, Standard Operating Procedures and references.

STANDARD: To support a mission capable status as defined in the units Standard Operating Procedures.

PERFORMANCE STEPS:
1. Review commander's guidance.
2. Maintain accountability of personnel.
3. Maintain accountability of equipment.
4. Supervise appropriate level of maintenance.
5. Inspect commodity area Turnover Folders or Desktop Procedures.

REFERENCES:
1. DoDD 7730.65 Department of Defense Readiness Reporting System (DRRS)
2. FMFM 0-1 UNIT TRAINING MANAGEMENT GUIDE.
3. MCBUL 3000 Marine Corps Automated Readiness Evaluation System (MARES) Equipment
4. MCO P4790.2_ MIMMS Field Procedures Manual

5. MCRP 3-0A Unit Training Management Guide
6. MCRP 3-0B How to Conduct Training

0650-MNGT-2710: Manage strategic CNO activities

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Commander's guidance.

STANDARD: To support the commander’s operational requirements.

PERFORMANCE STEPS:
1. Identify commander's/director's priorities.
2. Evaluate courses of action.
3. Draft Plan of Action and Milestones.
4. Coordinate with outside agencies.
5. Manage support functions.
6. Manage program life cycle.
7. Determine Total Cost of Ownership.
8. Validate Continuity of Operations Plan.

REFERENCES:
1. CISCO PRESS BOOKS Cisco books (http://www.ciscopress.com)
2. Deputy Secretary of Defense Deputy Secretary of Defense CyberOps Memorandum, 15 October 2008
3. DoD Capstone Concept DoD Capstone Concept for Joint Operations, Version 3.0, 15 January 2009
4. DoDI 8410.2 NETOPS for the Global Information Grid (GIG)
5. Gray Book Gray Book, Marine Corps Operating Concepts for a Changing Security Environment, March 2006
6. Joint Operating Concept Joint Operating Concept Version 2.0, Irregular Warfare: Countering Irregular Threats, 17 May 2010
7. Joint Pub 6-0 Joint Communications System, 10 June 2010.
8. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
10. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
11. National Military Strategy for Cyberspace Operations National Military Strategy for Cyberspace Operations, December 2006
12. National Security Strategy National Security Strategy, May 2010
13. Operation/Exercise Order
14. TRADOC Pamphlet 525-7-8 TRADOC Pamphlet 525-7-8, The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 22 February 2010
15. The National Security Strategy to Secure Cyberspace The National Strategy to Secure Cyberspace, February 2003
16. Tri-MEF SOP Tri-MEF Communication SOP
17. UNIT SOP Unit's Standing Operating Procedures

18. UNIT T/O&E Unit's Table of Organization and Equipment
19. USMC Cyberspace Concept USMC Cyberspace Concept, 17 July 2009

0650-MNGT-2711: Manage Information Technology program

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: T&R Event is accomplished at the MSC, MEF, MARFOR, and Joint/Combined Component Command levels.

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided commander's guidance, and acquisition regulations.

STANDARD: To meet the goals established by the command.

PERFORMANCE STEPS:
1. Verify requirements
2. Create POA&M
3. Supervise development
4. Supervise integrated product teams
5. Communicate periodic progress risk and issues
6. Manage testing requirements
7. Develop statements of work and statements of objectives
8. Manage a schedule
9. Draft lifecycle documentations
10. Manage lifecycle plan
11. Perform contracting officer requirements
12. Achieve defense acquisition workforce improvement ACT (DAWIA) level II program management certification

REFERENCES:
1. Contract Applicable Contract documentation
2. Contracting Officer's Representative (COR) Duties & Responsibilities Guidebook(s)
3. DAWIA DAWIA public law 101-510, title 10 USC
4. DOD 5200.28 Security Requirements for Automated Information Systems (AIS)
5. DOD 5200.28-STD DOD Trusted Computer System Evaluation Criteria
6. MARCORSYSCOM MARCORSYSCOM.usmc.mil
7. Technical Applicable Technical publications and manuals
8. UNIT SOP Unit's Standing Operating Procedures

COMM T&R MANUAL

CHAPTER 21

MOS 0651 INDIVIDUAL EVENTS

CHAPTER 21

MOS 0651 INDIVIDUAL EVENTS

21000. INDEX OF INDIVIDUAL EVENTS

21001. 1000-LEVEL EVENTS

0651-INST-1401: Install network equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0651

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To ensure network connectivity is verified via ICMP traffic between network components.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Identify network equipment components.
3. Install network components.
4. Configure network components.
5. Install operating system.
6. Configure operating system.
7. Install authorized software.
8. Configure authorized software.

REFERENCES:
1. DISA STIGS DISA Security Technical Implementation Guides
2. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
5. NAVY INFORMATION ASSURANCE Navy Information Assurance (http://www.infosec.navy.mil/dcuments/)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Server. 2. Workstation. 3. Layer 2 Device. 4. Layer 3 Device. 5. Encryption Device.

0651-OPER-1501: Operate network equipment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0651

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Operations Order, references, data communications equipment, and commander's intent.

STANDARD: Providing reliable data and network services.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Administer network components.
3. Monitor network components.
4. Optimize network components.
5. Implement authorized changes.

REFERENCES:
1. DISA STIGS DISA Security Technical Implementation Guides
2. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Server. 2. Workstation. 3. Layer 2 Device. 4. Layer 3 Device. 5. Encryption Device.

0651-MANT-1601: Maintain network components

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Marines will need to repair/replace components, restore network services, and perform PMCS; as it relates to hardware/software, and operational networks.

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To restore network equipment to reliable state.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Perform Preventative Maintenance Checks and Services (PMCS).
3. Identify faulty component.
4. Perform corrective action.
5. Maintain authorized software.
6. Perform backups.
7. Restore backups.
8. Document authorized maintenance.

REFERENCES:
1. DISA STIGS DISA Security Technical Implementation Guides
2. MCNOSC Marine Corps Network Operations and Security Center

(https://www.mcnosc.usmc.mil)
3. MCO 3500.27_ Operational Risk Management (ORM)
4. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
5. MCO P4790.2_ MIMMS Field Procedures Manual
6. NAVY INFORMATION ASSURANCE Navy Information Assurance (http://www.infosec.navy.mil/dcuments/)

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Server. 2. Workstation. 3. Layer 2 Device. 4. Layer 3 Device. 5. Encryption Device.

21002. 2000-LEVEL EVENTS

0651-PLAN-2101: Plan a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 3 months

DESCRIPTION: Description: Include transmission paths, node addresses, and equipment strings that are organic to a Battalion.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning guidance, references, and requirements.

STANDARD: That meets unit mission requirements.

PERFORMANCE STEPS:
1. Identify unit requirements.
2. Identify required network components.
3. Develop a data network addressing scheme.
4. Develop network diagram.

REFERENCES:
1. CISCO ONLINE Cisco Connection Online (http://www.cisco.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. NAVY INFORMATION ASSURANCE Navy Information Assurance (http://www.infosec.navy.mil/dcuments/)
6. Tri-MEF SOP Tri-MEF Communication SOP
7. DISA Defense Information System Network Integrated Tactical - Strategic Data Networking (ITSDN) Internet Protocol Addressing Plan

---

0651-INST-2401: Configure encryption devices on a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Description: Marines will install both hardware, and software encryption solution.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: Verifying the data is encrypted while traversing the network.

PERFORMANCE STEPS:
1. Identify connected network(s).
2. Identify encryption devices.
3. Load key material.
4. Adjust settings.
5. Conduct operational check.
6. Perform network check.

REFERENCES:
1. CISCO ONLINE Cisco Connection Online (http://www.cisco.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. DISA STIGS DISA Security Technical Implementation Guides
4. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
5. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
6. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
7. SECNAVINST 5510.36_ Dept of the Navy Information and Personnel Security Program Regulations

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Line encryption device. 2. Bulk encryption device. 3. DTD

0651-INST-2402: Configure quality of service (QOS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Description: Marines will need to configure QOS on network devices to ensure voice, video, network services are prioritized in support of the unit mission.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To optimize network performance ensuring priority is given to identical critical network services.

PERFORMANCE STEPS:
1. Identify QOS requirements.
2. Identify bandwidth limitations.
3. Implement QOS configuration.
4. Validate network performance.

REFERENCES:
1. CISCO ONLINE Cisco Connection Online (http://www.cisco.com)
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. DISA STIGS DISA Security Technical Implementation Guides
4. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)

5. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
6. Tri-MEF SOP Tri-MEF Communication SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Server. 2. Workstation. 3. Layer 2 device. 4. Layer 3 device. 5. Encryption device. 6. Network Management Solution.

0651-INST-2403: Install a multiplexer

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

DESCRIPTION: Description: Marines will multiplex Non-Secure/Secure Voice, Video, and network services.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To allow multiple networks to communicate through a multiplexing device.

PERFORMANCE STEPS:
1. Validate existing network plans.
2. Identify network equipment.
3. Identify connected network(s).
4. Configure multiplexing devices.
5. Conduct operational checks.
6. Conduct network check.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
4. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
5. Tri-MEF SOP Tri-MEF Communication SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Multiplexer. 2. Layer 3 device.

0651-INST-2404: Configure network timing

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Configure network timing source, and end devices.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To verify all devices that requires timing function properly.

PERFORMANCE STEPS:
1. Identify timing device.
2. Conduct operational check.
3. Conduct network check.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. Tri-MEF SOP Tri-MEF Communication SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Timing source device. 2. Timing end device.

0651-OPER-2501: Operate a data network helpdesk

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a data network mission requirement, software, equipment and references.

STANDARD: to provide end user support.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Establish helpdesk.
3. Process helpdesk trouble tickets.
4. Report helpdesk statistics.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. INFOSEC Navy Information Assurance (IA) publications, (http://www.mcnosc.usmc.mil)
3. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)

6. MCO P5233.1 Marine Corps ADP Management Standards Manual
7. MCO P5271.4A E-MAIL POLICY AND GUIDANCE
8. MCO P5510.14 USMC ADP SECURITY MANUAL
9. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
10. Tri-MEF SOP Tri-MEF Communication SOP

0651-OPER-2502: Implement a data communications network plan.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Operations Order, references, and data communications equipment.

STANDARD: To provide secure and reliable network communications.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Execute network plan.
3. Conduct operational test.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
4. MCO 3500.27_ Operational Risk Management (ORM)
5. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
6. MCO P5233.1 Marine Corps ADP Management Standards Manual
7. MCO P5271.4A E-MAIL POLICY AND GUIDANCE
8. MCO P5510.14 USMC ADP SECURITY MANUAL
9. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
10. Tri-MEF SOP Tri-MEF Communication SOP

0651-OPER-2503: Monitor data network services

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 6 months

DESCRIPTION: Execute performance steps as they relate to LAN services and WAN/LAN transmissions.

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided network monitoring, equipment, and references.

STANDARD: To provide secure and reliable communications.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Execute network monitoring plan.
3. Report network status.

REFERENCES:
1. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4)
4. Tri-MEF SOP Tri-MEF Communication SOP

0651-MANT-2601: Maintain a data network.

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0651

GRADES: CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To provide secure and reliable communications.

PERFORMANCE STEPS:
1. Backup network infrastructure.
2. Backup Network Operating System (NOS).
3. Backup data.
4. Restore network infrastructure.
5. Restore NOS.
6. Restore data.
7. Implement authorized updates.
8. Document network configuration changes.
9. Conduct operational checks.
10. Document authorized maintenance.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCO 3500.27_ Operational Risk Management (ORM)
3. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
4. MCO P5233.1 Marine Corps ADP Management Standards Manual
5. MCO P5271.4A E-MAIL POLICY AND GUIDANCE
6. MCO P5510.14 USMC ADP SECURITY MANUAL
7. MICROSOFT TECHNET ONLINE Technet online (http://www.microsoft.com/technet/)
8. Tri-MEF SOP Tri-MEF Communication SOP

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Server. 2. Workstation. 3. Layer 2 device.

COMM T&R MANUAL

CHAPTER 22

MOS 0652 INDIVIDUAL EVENTS

CHAPTER 22

MOS 0652 INDIVIDUAL EVENTS

22000. INDEX OF INDIVIDUAL EVENTS

22001. 2000-LEVEL EVENTS

0652-INST-2401: Install Certification Authority Workstation (CAW) Components

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the CAW hardware, software, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Inventory CAW hardware, Certification Authority (CA) material, and software.
2. Install CAW monitor, printer, label maker, and FORTEZZA card reader.
3. Perform initial operation check.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

MATERIAL: Blank FORTEZZA cards.

0652-OPER-2501: Operate the Certification Authority Workstation (CAW)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a CAW, FORTEZZA cards, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Login to CAW application as Certification Authority (CA).
2. Generate the X.509 Certificate for FORTEZZA card.

3. Verify organizational and distinguished name in X.500 Directory and complete registration in CAW database.
4. Program X.509 certificate onto FORTEZZA Card.
5. Post certificate to the directory.
6. Print PIN letter and User Acceptance (UA) and receipt for FORTEZZA card.
7. Copy X.509 Certificate onto domain FORTEZZA cards.
8. Update organizational FORTEZZA user in the CAW database.
9. Update CA default inputs for certificates and Certificate Revocation List windows as required.
10. Update X.509 Certificate in accordance with submitted X.509 Certificate Request Form.
11. Logout and perform orderly shutdown of the system.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

MATERIAL: Blank Fortezza Cards, X.509 Certificate Request Form (CRF).

0652-OPER-2502: Perform Certification Authority Workstation (CAW) Certification Authority (CA) functions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the CAW, FORTEZZA card, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Update FORTEZZA cards PIN.
2. Report a compromise.
3. Maintain the database.
4. Perform an annual inventory.
5. Verify X.509 Certificate information on FORTEZZA card.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)

2. DOD Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals

MATERIAL: Blank FORTEZZA cards, FORTEZZA cards with X.509 Certificate

---

0652-OPER-2503: Revoke X.509 Certificate on FORTEZZA card

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the CAW, V3 X.509 Certificate request form, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Authenticate revocation request form.
2. Verify the need for revocation.
3. Enter certificate information on the Certificate Revocation List (CRL).

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practices Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

MATERIAL: X.509 Certificate Request Form (Revocation block checked).

0652-MNGT-2701: Implement FORTEZZA card procedural controls

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given Commander's guidance, FORTEZZA Cards, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Manage created FORTEZZA cards.
2. Create FORTEZZA card delivery procedures.
3. Create PIN issuing procedures.
4. Notify users of FORTEZZA card renewal.
5. Notify users of mandatory re-key.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practices Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

MATERIAL: FORTEZZA cards with X.509 Certificate.

0652-MNGT-2702: Provide procedural controls for the CAW

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a CAW, FORTEZZA cards, and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Complete, obtain command signature, and post CAW Authorized Access Memorandum (AAM).
2. Distribute FORTEZZA Cards and PIN letters.
3. Check Indirect Certificate Revocation List (ICRL).
4. Report compromises.
5. Create, post, and maintain Certificate Revocation List (CRL) at least weekly.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practices Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

0652-MNGT-2703: Maintain personnel controls to the Certification Authorization Workstation (CAW).

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided a CAW and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Ensure training in hardware/software version of the CAW is current.
2. Maintain CAW procedures updates.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practices Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

0652-PROT-2801: Provide physical security controls to the CAW

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a CAW and references.

STANDARD: To provide secure communications.

PERFORMANCE STEPS:
1. Protect equipment from unauthorized access.
2. Secure CA and blank FORTEZZA cards.
3. Protect media from damage
4. Ensure the CAW SA/ISSO performs weekly system backups.
5. Secure system backups.

REFERENCES:
1. DOD CP X.509 Certificate Policy for the United States Department of Defense (DoD)
2. DOD Certification Practice Statement (CPS) for the Class 4 FORTEZZA/CAW PKI
3. NAG-69 Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations (CAW)
4. USMC Certificate Practice Statement (CPS) for the Class 4 FORTEZZA/PKI
5. Certification Authority (CA) Procedural Handbook

SUPPORT REQUIREMENTS:

EQUIPMENT: Certification Authority Workstation with peripherals.

MATERIAL: 1. FORTEZZA cards, both blank and with certificates. 2. Magnetic data tapes.

CHAPTER 23

MOS 0653 INDIVIDUAL EVENTS

CHAPTER 23

MOS 0653 INDIVIDUAL EVENTS

23000. INDEX OF INDIVIDUAL EVENTS

23001. 2000-LEVEL EVENTS

0653-INST-2401: Install a Defense Message System (DMS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0653

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To provide reliable organizational messaging capabilities.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Adhere to security procedures.
3. Install hardware.
4. Install software.
5. Configure equipment.

REFERENCES:
1. DISA DMSIP Defense Information System Agency (DISA) DMS Interim Procedures
2. DMS FENS DMS Field Engineering Notices (FEN's) Matrix
3. DODD 5200.1-R Information Security Program
4. MCO 3500.27_ Operational Risk Management (ORM)
5. SDA System Architecture Design (SDA) ver 3.1 12 Sep 2006
6. SDD Site Detail Design

SUPPORT REQUIREMENTS:

EQUIPMENT: DMS SUITE

0653-OPER-2501: Operate a Defense Message System (DMS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0653

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: Passing message traffic with a minimum reliability standard of 98 percent.

PERFORMANCE STEPS:
1. Identify safety hazards.

2. Adhere to security procedures.
3. Process message traffic.
4. Perform account administration.
5. Conduct operational checks.

REFERENCES:
1. DISA DMSIP Defense Information System Agency (DISA) DMS Interim Procedures
2. DMS FENS DMS Field Engineering Notices (FEN's) Matrix
3. DODD 5200.1-R Information Security Program
4. MCO 3500.27_ Operational Risk Management (ORM)
5. SDA System Architecture Design (SDA) ver 3.1 12 Sep 2006
6. SDD Site Detail Design

SUPPORT REQUIREMENTS:

EQUIPMENT: DMS SUITE

0653-MANT-2601: Maintain a Defense Message System (DMS)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0653

GRADES: PVT, PFC, LCPL, CPL, SGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided equipment, planning documents, and references.

STANDARD: To provide reliable organizational messaging capabilities.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Adhere to security procedures.
3. Verify server settings.
4. Update server software.
5. Modify server settings.
6. Modify network settings.
7. Verify peripheral settings.
8. Update peripheral software.
9. Modify peripheral settings.
10. Conduct PMCS.
11. Document authorized maintenance.

REFERENCES:
1. DISA DMSIP Defense Information System Agency (DISA) DMS Interim Procedures
2. DMS FENS DMS Field Engineering Notices (FEN's) Matrix
3. DODD 5200.1-R Information Security Program
4. MCO 3500.27_ Operational Risk Management (ORM)
5. SDA System Architecture Design (SDA) ver 3.1 12 Sep 2006
6. SDD Site Detail Design

SUPPORT REQUIREMENTS:

EQUIPMENT: DMS SUITE

COMM T&R MANUAL

CHAPTER 24

MOS 0659 INDIVIDUAL EVENTS

CHAPTER 24

MOS 0659 INDIVIDUAL EVENTS

24000. INDEX OF INDIVIDUAL EVENTS

24001. 2000-LEVEL EVENTS

0659-PLAN-2101: Plan a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 6 months

MOS PERFORMING: 0659

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Operations Order, references, and commander's intent.

STANDARD: To ensure the data plan adheres to the Information Assurance plan, and by verifying network, software, and Information Security requirements.

PERFORMANCE STEPS:
1. Plan a LAN architecture.
2. Plan a WAN architecture.
3. Plan an organizational messaging architecture.
4. Plan an individual messaging architecture.
5. Plan a NOS architecture.
6. Plan virtualization.
7. Plan for disaster recovery.
8. Coordinate power management.
9. Coordinate HVAC requirements.
10. Coordinate Information Assurance (IA) requirements.

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
3. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4)
4. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
5. Tri-MEF SOP Tri-MEF Communication SOP

0659-PLAN-2102: Plan Help Desk operations

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0659

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, references, and commander's intent.

STANDARD: To deliver on time and accurate end user support.

PERFORMANCE STEPS:
1. Plan standard operating procedures.
2. Plan watch schedule.
3. Plan training procedures.

REFERENCES:
1. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
2. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
3. NAVY INFORMATION ASSURANCE Navy Information Assurance (http://www.infosec.navy.mil/dcuments/)
4. Tri-MEF SOP Tri-MEF Communication SOP

0659-MNGT-2701: Manage a data help desk

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0659

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Operations Order, references, and commander's intent.

STANDARD: To deliver on time and accurate end user support.

PERFORMANCE STEPS:
1. Identify safety hazards.
2. Supervise watch duties.
3. Supervise quality control.
4. Report helpdesk statistics.

REFERENCES:
1. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
2. MCO 3500.27_ Operational Risk Management (ORM)
3. Tri-MEF SOP Tri-MEF Communication SOP

0659-MNGT-2702: Manage the operation of a data network

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0659

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided an Operations Order, references, and commander's intent.

STANDARD: To ensure that the data network is secure and reliable.

PERFORMANCE STEPS:

1. Identify safety hazards.
2. Validate equipment placement.
3. Verify installation.
4. Validate configuration of network components.
5. Validate configuration of network services.
6. Validate configuration of network security components.
7. Conduct system operations check.
8. Report status to SYSCON.
9. Ensure compliance with Information Assurance (IA) policies.
10. Monitor network performance.
11. Direct reconfiguration of network systems.
12. Validate network documentation.

REFERENCES:

1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. CMS-21 COMSEC Material System Policy and Procedures
3. DISA STIGS DISA Security Technical Implementation Guides
4. MCNOSC Marine Corps Network Operations and Security Center (https://www.mcnosc.usmc.mil)
5. MCO 3500.27_ Operational Risk Management (ORM)
6. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP)(C4)
7. NAVY INFORMATION ASSURANCE Navy Information Assurance (http://www.infosec.navy.mil/dcuments/)
8. Tri-MEF SOP Tri-MEF Communication SOP

CHAPTER 25

MOS 0681 INDIVIDUAL EVENTS

CHAPTER 25

MOS 0681 INDIVIDUAL EVENTS

25000. INDEX OF INDIVIDUAL EVENTS

0681-PROT-2801	Describe COMSEC safeguarding requirements and procedures	25-20
0681-PROT-2802	Execute the Emergency Action Plan (EAP)	25-21
0681-PROT-2803	Identify the type of insecurities	25-22

25001. 2000-LEVEL EVENTS

0681-PLAN-2101: Define national COMSEC structure

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided the EKMS (series) publications.

STANDARD: Correctly describing COMSEC tiers and identifying locations.

PERFORMANCE STEPS:
1. Describe EKMS tier structure.
2. Identify locations of EKMS tiers.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

0681-PLAN-2102: Describe the need for COMSEC material and allowances

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided EKMS (series) publications.

STANDARD: By identifying COMSEC KEYMAT, equipment, and COMSEC related material with respect to format, purpose, type, state and use.

PERFORMANCE STEPS:
1. Identify KEYMAT based on its short title.
2. Explain the types of COMSEC equipment and CCI.
3. Explain COMSEC related information.
4. Explain Accounting Legend Codes (ALCs).
5. Explain status and supersession information.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

0681-PLAN-2103: Develop a COMSEC Standard Operating Procedure (SOP)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given EKMS (series) publications.

STANDARD: In accordance with pertinent directives.

PERFORMANCE STEPS:
1. Gather references.
2. Draft policy which addresses local command issues.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. UNIT SOP Unit's Standing Operating Procedures

0681-PLAN-2104: Validate COMSEC KEYMAT Modification of Allowance (MOA)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given a subordinate account MOA request.

STANDARD: By submitting an MOA endorsement to the controlling authority (ConAuth).

PERFORMANCE STEPS:
1. Receive MOA.
2. Validate request.
3. Submit endorsement to ConAuth via COMSEC chain of command.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

0681-OPER-2501: Demonstrate logon and logoff procedures

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given Local COMSEC Management Software (LCMS) and Local Management Device.

STANDARD: To perform the proper logon and logoff sequence.

PERFORMANCE STEPS:
1. Perform system start up Logon
2. Perform Logoff and proper shutdown procedures.

REFERENCES:
1. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite

0681-OPER-2502: Perform message server (X.400 and X.500) functions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given Local COMSEC Management Software (LCMS) and Local Management Device (LMD).

STANDARD: To communicate with your Tier 1 via LCMS.

PERFORMANCE STEPS:
1. Electronically wrap/unwrap EKMS messages.
2. Send/receive electronic packages via X.400 message server.
3. Upload/download Common Account Data (CAD) information from Directory Server (X.500).

REFERENCES:
1. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. LMD/KP; 2. Secure Telephone Equipment (STE)

0681-OPER-2503: Perform transfer/receipt of physical COMSEC material sent from a DON COMSEC account

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given EKMS (series) publications.

STANDARD: To transfer/receipt of COMSEC material.

PERFORMANCE STEPS:
1. Properly document the transfer/receipt of COMSEC material with an SF-153.
2. Report transfer/receipt to originating/destination account and to your Tier 1 via X400.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

MATERIAL: Incoming COMSEC material to EKMS account.

0681-OPER-2504: Demonstrate the ten (10) steps for destroying physical COMSEC material

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given EKMS (series) publications and Controlling Authority (ConAuth) status messages.

STANDARD: By performing required destruction steps.

PERFORMANCE STEPS:
1. Assemble required personnel.
2. Verify status of material.
3. Create working destruction document.
4. Assemble material to be destroyed.
5. Transport material to destruction location.
6. Properly destroy material.
7. Sign working destruction document.
8. Confirm destruction within LCMS.
9. Prepare and sign consolidated destruction reports.
10. Foreword documentation via X400 and file report.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual
3. NSA EPL-02-01-AA NSA evaluated product list

SUPPORT REQUIREMENTS:

EQUIPMENT: NSA approved destruction device; 2. LMD/KP suite.

MATERIAL: Standard Form (SF)-153 COMSEC material report.

0681-OPER-2505: Perform basic AN/CYZ-10 Data Transfer Device (DTD), AN/PYQ-10 Simple Key Loader (SKL) functions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given an operational DTD/SKL requiring KEYMAT.

STANDARD: By demonstrating basic user functions.

PERFORMANCE STEPS:
1. Receive KEYMAT.
2. Issue KEYMAT.
3. Load KEYMAT.
4. Destroy KEYMAT.

REFERENCES:
1. EE130-EF-MMC-010 Operator's Manual for AN/CYZ-10 (v) 3 Data Transfer Device
2. EE180-KT-IMC-010 SKL Operator Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. AN/CYZ-1 Data Transfer Device (DTD); 2. AN/PYQ Simple Key Loader (SKL).

0681-OPER-2506: Perform basic Secure Terminal Equipment (STE) functions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a STE phone.

STANDARD: By demonstrating basic setup and user functions.

PERFORMANCE STEPS:
1. Establish Terminal Privilege Authority (TPA) card with provided KSV-21.
2. Create User card.
3. Complete Seed Key conversion call.
4. Complete a secure phone call.

REFERENCES:
1. EE160-AM-TRN-E10 STE User's Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. Secure Telephone Equipment (STE); 2. KSV-21.

0681-OPER-2507: Demonstrate logon and logoff procedures for the Key Processor (KP)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a Local Management Device/Key Processor (LMD/KP) suite.

STANDARD: By logging on/off of the KP.

PERFORMANCE STEPS:
1. Log on to LMD.
2. Log on to LCMS.
3. Log on to KP.
4. Log off KP.
5. Log off LCMS.

REFERENCES:
1. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2508: Produce electronic keying material (KEYMAT)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a requirement for locally generated key.

STANDARD: To support local COMSEC needs for encrypting communications circuits.

PERFORMANCE STEPS:
1. Order Key from LCMS.
2. Confirm Order of Key.
3. Produce KEYMAT.
4. Originate a generation report.
5. Sign appropriate documentation and file.

REFERENCES:
1. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2509: Transfer/receive electronic KEYMAT

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given the requirement to support another COMSEC account and Controlling Authority (CA) approval.

STANDARD: By performing in order, the performance steps.

PERFORMANCE STEPS:
1. Generate the bulk encryption transaction (BET).
2. Wrap transaction and send to destination account and Tier 1.
3. Receive electronic package from transferring account.
4. Unwrap and process received KEYMAT.
5. Wrap receipt transaction and send to originating account and Tier 1.

REFERENCES:
1. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2510: Issue electronic KEYMAT to a Local Element (LE)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a requirement to issue electronic KEYMAT.

STANDARD: To support communications requirements.

PERFORMANCE STEPS:
1. Log in to LMD/KP.
2. Issue KEYMAT to LE fill device.
3. Sign local custody documentation.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. LMD/KP suite; 2. fill device.

0681-OPER-2511: Demonstrate destruction of electronic KEYMAT

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given the need to destroy COMSEC KEYMAT.

STANDARD: By properly destroying/deleting KEYMAT.

PERFORMANCE STEPS:
1. Delete KEYMAT from fill devices.
2. Destroy KEYMAT from LMD/KP.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. LMD/KP suite; 2. fill device.

0681-OPER-2512: Perform routine, required KP maintenance functions

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given an LMD/KP suite.

STANDARD: To ensure the KP is operating IAW Navy EKMS policies.

PERFORMANCE STEPS:
1. Describe the purpose and frequency of KP Changeover.
2. Describe the purpose and frequency of KP Rekey.
3. Describe the purpose and frequency of KP Reinitialization.
4. Describe the purpose and frequency of KP operator Pin changes.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2513: Perform Over-The-Air Distribution (OTAD)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a requirement to issue KEYMAT to authorized distant users.

STANDARD: By issuing KEYMAT via secure phone.

PERFORMANCE STEPS:
1. Prepare the phone for Secure Data connection.
2. Prepare the fill device.
3. Transfer KEYMAT via OTAD.
4. Verify distant end received KEYMAT and document.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. NAG-16 Field Generation and Over the Air Distribution of COMSEC Key in Support of Tactical Operations and Exercises

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. AN/CYZ-10 Data Transfer Device (DTD); 2. AN/PYQ-10 Simple Key Loader (SKL); 3. Secure Terminal Equipment (STE); 4. KSV-21.

0681-OPER-2514: Register new items within LCMS

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given new type of COMSEC material.

STANDARD: By performing in order, the performance steps.

PERFORMANCE STEPS:
1. Receive material.
2. Process the receipt.
3. Apply attributes to the material.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2515: Maintain Central Facility User Representative (UR) data

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given an account which holds modern KEYMAT.

STANDARD: By keeping UR data up-to-date with the EKMS Central Facility.

PERFORMANCE STEPS:
1. Process Order Privilege Manager (OPM) transactions.
2. Submit UR data changes to Command Authority (CA).
3. CA submits UR modifications changes to Central Facility.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

0681-OPER-2516: Perform LMD/KP functions as required/scheduled

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given an LMD/KP suite.

STANDARD: To ensure the KP operates properly.

PERFORMANCE STEPS:
1. Execute a KP Changeover.
2. Execute a KP Rekey.
3. Load Privilege Certificate (PrivCert) and KG rules.
4. Configure KP communications interface.
5. Reinitialize KP using bound or signed PrivCert.
6. Zeroize KP as required and return to COMSEC Material Issuing Office (CMIO).
7. Change PINs on KP and passwords on LMD.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-OPER-2517: Communicate with COR and other EKMS accounts

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given the need to communicate electronically via LCMS.

STANDARD: By sending and receiving wrapped electronic messages.

PERFORMANCE STEPS:
1. Send/receive EKMS messages via x.400.
2. Send/receive EKMS message via floppy disk.
3. Send/receive electronic messages after establishing direct communications with distant account(s).

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

MATERIAL: 3.5 inch floppy disk.

0681-OPER-2518: Induct devices in/out of the Marine Corps Maintenance/Repair Cycle

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given an account with Controlled Cryptographic Items (CCI) requiring maintenance.

STANDARD: Ensuring equipment is repaired/replaced and returned to owning EKMS account.

PERFORMANCE STEPS:
1. Identify if CCI is a floatable item.
2. Prepare documentation.
3. Induct CCI into the Consolidated Repair Facility (CRF) retain local custody document.
4. Pick up CCI from CRF.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. LMD/KP suite; 2. CCI requiring maintenance.

0681-MANT-2601: Perform system backups

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given LMD/KP suite.

STANDARD: To ensure recovery of the LCMS data base in the event of catastrophic failure.

PERFORMANCE STEPS:
1. Log into LMD using Root account.
2. Run the data base backup script.
3. Perform Dev/root backup.
4. Perform Dev/U backup.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

MATERIAL: Backup tapes.

0681-MANT-2602: Perform data archiving

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given LMD/KP suite.

STANDARD: To close out transactions within UNIX to free up table space in the operating system/data base.

PERFORMANCE STEPS:
1. Log on to LCMS & KP.
2. Open Archive screen from KP menu.
3. Archive to diskette.
4. Label archive media.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

MATERIAL: selected archive media.

0681-MANT-2603: Manage software upgrades

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Given CCI requiring software upgrades.

STANDARD: By ensuring equipment is at current software version/baseline.

PERFORMANCE STEPS:
1. Contact Service Authority for baseline standards.
2. Acquire software/firmware.
3. Oversee/perform upgrade and verify.
4. Document authorized maintenance.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-5A Cryptographic Equipment Information/Guidance Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: Non-NMCI Laptop.

0681-MANT-2604: Manage items within LCMS

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided a LCMS database.

STANDARD: To maintain up to date information.

PERFORMANCE STEPS:
1. Add/modify/delete COMSEC accounts.
2. Modify and post Common Account Data (CAD).

3. Add/modify/delete Local Elements (LEs).
4. Add/modify/delete equipment types.
5. Add/modify/delete benign fill equipment.
6. Add/modify/delete COMSEC material.
7. Add/modify/delete administrators and operators.
8. Register physical KMID data.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-MNGT-2701: Perform transfer / receipt of physical COMSEC material

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given COMSEC material from a Non-DON agency.

STANDARD: To properly complete the transfer/receipt of COMSEC material sent from a Non-DON COMSEC account.

PERFORMANCE STEPS:
1. Properly document the relief of accountability report of the physical COMSEC material to a Non-DON account.
2. Provide DD-1149/DD-1348 documentation of the transaction to the Non-DON account.
3. When provided a DD-1149/DD-1348 for physical COMSEC material from a Non-DOD account, receipt for the physical COMSEC material by performing a possession report.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-5A Cryptographic Equipment Information/Guidance Manual
3. EKMS-704 (series) LMD/KP Operators Manual

0681-MNGT-2702: Manage COMSEC related files

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given EKMS (series) publications.

STANDARD: To maintain accountability of COMSEC material.

PERFORMANCE STEPS:
1. Ensure completion of SF-153(s).
2. Properly maintain a current Accountable Items Summary (AIS).
3. Maintain a correct Transaction Status Log.
4. Maintain Chronological file, Correspondence file, Directives file, General Message File (GMF), Local Custody files and logs.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

SUPPORT REQUIREMENTS:

MATERIAL: 1. SF-153; 2. Chronological file, Correspondence file, Directives file, General Message File (GMF) and Local Custody files.

0681-MNGT-2703: Manage Transfer Key Encryption Key (TrKEK)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Give a data transfer device (DTD) and a requirement for a TrKEK.

STANDARD: To support the transfer of encrypted KEYMAT between DTDs, enabling the receiving DTD to unencrypted the received KEYMAT.

PERFORMANCE STEPS:
1. Determine proper classification.
2. Determine Crypto period.
3. Preposition TrKEK in fill device.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: 1. AN/CYZ-10; 2. SKL; 3. LMD/KP suite.

0681-MNGT-2704: Describe COMSEC inventory requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given EKMS (series) publications.

STANDARD: To know when and how to conduct proper COMSEC/EKMS account inventories.

PERFORMANCE STEPS:
1. Describe types, periodicities, and requirements for inventories.
2. Describe the steps to conduct an annual inventory.
3. Explain the Inventory Reconciliation Status Transaction (IRST) process.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-704 (series) LMD/KP Operators Manual

SUPPORT REQUIREMENTS:

EQUIPMENT: LMD/KP suite.

0681-MNGT-2705: Describe the COMSEC Inspection Program

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given EKMS (series) publications.

STANDARD: By explaining the various aspects of inspections.

PERFORMANCE STEPS:
1. State the purpose/frequency of inspections.
2. Describe inspection evaluation criteria.
3. Describe the CMS A&A program.
4. Perform a quarterly self-assessment.
5. Perform monthly LE inspections.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-3 (series) EKMS Inspection Manual

0681-MNGT-2706: Conduct EKMS account inspection

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 24 months

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided an EKMS account.

STANDARD: To ensure accounts are in compliance with COMSEC policy.

PERFORMANCE STEPS:
1. Conduct in-brief with commander.
2. Conduct inspection of EKMS account and Local Elements.
3. Validate latest Physical Security Evaluation (PSE).
4. Conduct out-brief with commander.
5. Report inspection results as required.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. EKMS-3 (series) EKMS Inspection Manual

0681-PROT-2801: Describe COMSEC safeguarding requirements and procedures

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given COMSEC publications and approved security containers.

STANDARD: By explaining authorized methods of storing and safeguarding COMSEC material.

PERFORMANCE STEPS:
1. Describe Two-Person Integrity (TPI) requirements and methods.
2. Describe storage requirements for different types of COMSEC material.
3. Set combination for security container.
4. Describe/conduct procedures to record and protect combinations, passwords, and PINs on Standard Form-700 (SF-700).

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. SECNAVINST 5510.36_ Dept of the Navy Information and Personnel Security Program Regulations

SUPPORT REQUIREMENTS:

EQUIPMENT: Safe with electromagnetic combination lock.

MATERIAL: SF-700.

0681-PROT-2802: Execute the Emergency Action Plan (EAP)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a copy of the Commands Emergency Action Plan (EAP).

STANDARD: By demonstrating the required actions to destroy/safeguard COMSEC material in an emergency.

PERFORMANCE STEPS:
1. Explain the guidelines for emergency protection planning.
2. Identify types of destruction and priority lists.
3. Describe emergency destruction procedures.
4. Complete required annual EAP training and document.
5. Execute EAP as required.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
2. SECNAVINST 5510.36_ Dept of the Navy Information and Personnel Security Program Regulations

SUPPORT REQUIREMENTS:

MATERIAL: Destruction material as identified in the Commands EAP.

0681-PROT-2803: Identify the type of insecurities

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given COMSEC insecurity.

STANDARD: By differentiating between COMSEC Incidents and Practices Dangerous to Security (PDS).

PERFORMANCE STEPS:
1. Identify the types of COMSEC Incidents.
2. Identify the categories of PDS.
3. Draft COMSEC Incident Report (CIR) and/or PDS documentation.

REFERENCES:
1. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3

COMM T&R MANUAL

CHAPTER 26

MOS 0689 INDIVIDUAL EVENTS

CHAPTER 26

MOS 0689 INDIVIDUAL EVENTS

26000. INDEX OF INDIVIDUAL EVENTS

26001. 2000-LEVEL EVENTS

0689-PLAN-2101: Determine Information Assurance program requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, and references.

STANDARD: To ensure DOD Information Systems maintain an appropriate level of Confidentiality, Integrity, Authentication, Non-repudiation, and Availability.

PERFORMANCE STEPS:
1. Determine applicable policies.
2. Determine certification requirements.
3. Determine accreditation requirements.
4. Determine information assurance training requirements.
5. Determine information assurance vulnerability management requirements.
6. Determine contingency planning requirements.
7. Determine auditing requirements.
8. Determine physical security requirements.
9. Determine configuration management requirements.
10. Determine incident response requirements.
11. Determine joint requirements.
12. Determine information assurance roles.
13. Determine information assurance responsibilities.
14. Determine budget requirements.
15. Determine reporting requirements.
16. Determine information conditions requirements.
17. Determine operational security requirements.
18. Determine information assurance metrics.
19. Determine personnel security requirements.
20. Determine access requirements.
21. Determine information assurance supporting documentation requirements.
22. Determine information exchange requirements.
23. Determine assessment requirements.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DON IA PUBS Department of Navy Information Assurance Publications
7. DoD 8570.01_ Information Assurance Training, Certification, and Workforce Program Manual
8. DoDD 8500.1 Information Assurance

9. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
10. DoDD 8570.1 Information Assurance Training, Certification, and Workforce Management
11. DoDI 8500.2 Information Assurance Implementation
12. MCIAED Marine Corps Information Assurance Enterprise Directives
13. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
14. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
15. Information Assurance Technical Framework Release 3.1, September 2002
16. NIST Special Publication 800 Series
17. NSA Operational Security Doctrine Publications
18. NSA Security Recommendation Guides
19. TRI-MEF SOP

0689-PLAN-2102: Determine Information Assurance architecture requirements

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, and references.

STANDARD: To provide an Information Assurance capability that supports an interoperable, robust infrastructure-wide defense in depth solution.

PERFORMANCE STEPS:
1. Determine certification requirements.
2. Determine accreditation requirements.
3. Determine enclave boundary requirements.
4. Determine network environment requirements.
5. Determine computing environment requirements.
6. Determine supporting environment requirements.
7. Determine configuration management requirements.
8. Determine applicable policies.
9. Identify communication plan requirements.
10. Determine joint requirements.
11. Determine estimate of supportability.
12. Identify commanders' intent.
13. Determine risk.
14. Identify mission assurance categories.
15. Identify confidentiality levels.
16. Determine Information Assurance baselines.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists

4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DON IA PUBS Department of Navy Information Assurance Publications
7. DoD 8570.01_ Information Assurance Training, Certification, and Workforce Program Manual
8. DoDD 8500.1 Information Assurance
9. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
10. DoDD 8570.1 Information Assurance Training, Certification, and Workforce Management
11. DoDI 8500.2 Information Assurance Implementation
12. DoDI 8510.1_ DITSCAP Application Manual
13. MCIAED Marine Corps Information Assurance Enterprise Directives
14. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
15. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
16. Applicable Technical Publications/Manuals
17. Information Assurance Technical Framework Release 3.1, September 2002
18. NIST Special Publication 800 Series
19. NSA Operational Security Doctrine Publications
20. NSA Security Recommendation Guides
21. TRI-MEF SOP

0689-DSGN-2201: Develop an Information Assurance program

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, and references.

STANDARD: To ensure interoperability and integration of Defense-in-Depth Information Assurance solutions.

PERFORMANCE STEPS:
1. Draft certification requirements.
2. Draft accreditation requirements.
3. Draft Information Assurance training policy.
4. Draft Information Assurance vulnerability management policy.
5. Validate contingency policy.
6. Validate auditing policy.
7. Validate physical security policy.
8. Validate configuration management policy.
9. Draft incident response policy.
10. Draft Information Assurance roles.
11. Draft Information Assurance responsibilities.
12. Draft budget strategy.
13. Draft reporting policy.
14. Validate access policy.

15. Draft assessment policy.
16. Draft information conditions policy.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DON IA PUBS Department of Navy Information Assurance Publications
7. DoD 8570.01_ Information Assurance Training, Certification, and Workforce Program Manual
8. DoDD 8500.1 Information Assurance
9. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
10. DoDD 8570.1 Information Assurance Training, Certification, and Workforce Management
11. DoDI 8500.2 Information Assurance Implementation
12. MCIAED Marine Corps Information Assurance Enterprise Directives
13. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
14. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
15. Applicable Technical Publications/Manuals
16. Information Assurance Technical Framework Release 3.1, September 2002
17. NIST Special Publication 800 Series
18. NSA Operational Security Doctrine Publications
19. NSA Security Recommendation Guides
20. TRI-MEF SOP

0689-DSGN-2202: Draft an Information Assurance plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, and references.

STANDARD: To provide interoperability and integration of an Information Assurance program and its solutions.

PERFORMANCE STEPS:
1. Identify applicable Information Assurance policies.
2. Review Information Assurance program requirements.
3. Identify Information Assurance architecture requirements.
4. Identify computer network defense providers.
5. Identify computer network defense provider requirements.
6. Identify information operations requirements.
7. Identify non-technical controls.

8. Identify technical controls.
9. Validate contingency plan.
10. Draft incident response procedures.
11. Draft Information Assurance vulnerability management procedures.
12. Determine Information Assurance personnel requirements.
13. Validate access control procedures.
14. Draft Information Assurance training procedures.
15. Validate contingency procedures.
16. Validate auditing procedures.
17. Validate physical security procedures.
18. Validate configuration management procedures.
19. Draft Information Assurance roles.
20. Draft Information Assurance responsibilities.
21. Draft Information Assurance reporting procedures.
22. Draft assessment procedures.
23. Identify classification levels.
24. Draft information conditions procedures.
25. Draft joint procedures.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DON IA PUBS Department of Navy Information Assurance Publications
7. DoD 8570.01_ Information Assurance Training, Certification, and Workforce Program Manual
8. DoDD 8500.1 Information Assurance
9. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
10. DoDD 8570.1 Information Assurance Training, Certification, and Workforce Management
11. DoDI 8500.2 Information Assurance Implementation
12. MCIAED Marine Corps Information Assurance Enterprise Directives
13. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
14. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
15. Applicable Technical Publications/Manuals
16. Information Assurance Technical Framework Release 3.1, September 2002
17. NIST Special Publication 800 Series
18. NSA Operational Security Doctrine Publications
19. NSA Security Recommendation Guides
20. TRI-MEF SOP

0689-DSGN-2203: Draft an Information Assurance architecture

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, and references.

STANDARD: To ensure interoperability and integration of Defense-in-Depth Information Assurance solutions.

PERFORMANCE STEPS:
1. Design IA Architecture enclave boundary.
2. Design IA Architecture network environment.
3. Design IA Architecture computing environment.
4. Design IA Architecture supporting environment.
5. Draft risk management strategies.
6. Develop secure router solutions.
7. Develop access control lists.
8. Develop secure remote access service.
9. Develop secure switch solutions.
10. Develop intrusion prevention solutions.
11. Develop firewall solutions.
12. Develop intrusion detection solutions.
13. Develop virtual private network solutions.
14. Develop content filtering solutions.
15. Develop email filtering solutions.
16. Develop cryptographic solutions.
17. Develop remediation solutions.
18. Develop system hardening solutions.
19. Develop secure wireless solutions.
20. Develop secure network services.
21. Develop malicious code solutions.
22. Develop vulnerability assessments solutions.
23. Develop auditing solutions.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Information Assurance Technical Framework Release 3.1, September 2002
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-ENGR-2301: Develop an Information Assurance plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, equipment, and references.

STANDARD: In accordance with DODD_8500.1, DODI_8500.2, CJCSM_6510.1, DISA_STIGS, and NIST SP_800 Series.

PERFORMANCE STEPS:
1. Develop secure router solutions.
2. Engineer access control lists.
3. Engineer secure remote access service.
4. Engineer secure switch solutions.
5. Engineer intrusion prevention solutions.
6. Engineer firewall solutions.
7. Engineer intrusion detection solutions.
8. Engineer virtual private network solutions.
9. Engineer content filtering solutions.
10. Engineer email filtering solutions.
11. Engineer cryptographic solutions.
12. Engineer remediation solutions.
13. Engineer system hardening solutions.
14. Engineer secure wireless solutions.
15. Engineer secure network services.
16. Engineer malicious code solutions.
17. Engineer vulnerability assessments solutions.
18. Engineer auditing solutions.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Information Assurance Technical Framework Release 3.1, September 2002
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-INST-2401: Implement technical Information Assurance controls

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To provide protect, detect, react and recover capabilities on information systems and computer networks.

PERFORMANCE STEPS:
1. Configure secure router solutions.
2. Configure access control lists.
3. Configure secure remote access services.
4. Configure secure switch solutions.
5. Configure IDS solutions.
6. Install IDS solutions.
7. Install IPS solutions.
8. Configure IPS solutions.
9. Configure firewall solutions.
10. Install firewall solutions.
11. Configure VPN solutions.
12. Install VPN solutions.
13. Configure content filtering solutions.
14. Install content filtering solutions.
15. Configure e-mail filtering solutions.
16. Install e-mail filtering solutions.
17. Configure remediation solutions.
18. Install remediation solutions.
19. Apply system hardening solutions.
20. Configure secure network services.
21. Configure malicious code solutions.
22. Configure vulnerability assessments solutions.
23. Configure auditing solutions.
24. Configure forensic solutions.
25. Install forensic solutions.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Information Assurance Technical Framework Release 3.1, September 2002
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-OPER-2501: Implement non-technical Information Assurance Controls

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, planning policies, equipment, and references.

STANDARD: To provide a policy framework to establish, update and support the Information Assurance program.

PERFORMANCE STEPS:
1. Employ non-technical Information Assurance controls.
2. Coordinate with computer network defense providers.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Information Assurance Technical Framework Release 3.1, September 2002
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-OPER-2502: Perform a certification and accreditation process

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Information Assurance policies, systems documentation, system concept of operations, planning documents, equipment, and references.

STANDARD: To ensure only certified trusted systems are authorized to operate on the Global Information Grid.

PERFORMANCE STEPS:
1. Perform certification process.
2. Provide accreditation recommendation.
3. Perform connection approval process.

REFERENCES:
1. DoDD 8500.1 Information Assurance
2. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
3. DoDI 8500.2 Information Assurance Implementation
4. MCIAED Marine Corps Information Assurance Enterprise Directives
5. TRI-MEF SOP

0689-OPER-2503: Conduct non-technical Information Assurance assessment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Information Assurance policies, personnel, and references.

STANDARD: To validate adherence to Information Assurance policies and procedures.

PERFORMANCE STEPS:
1. Identify applicable policy.
2. Determine assessment scope.
3. Determine assessment objectives.
4. Create assessment plan.
5. Perform document review.
6. Perform personnel interviews.
7. Analyze assessment results.
8. Report assessment results.
9. Provide remediation plan.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DoDD 8500.1 Information Assurance
4. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
5. DoDI 8500.2 Information Assurance Implementation
6. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
7. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
8. Applicable Technical Publications/Manuals
9. JITC Assessment Methodologies
10. Marine Corps Assessment Methodologies
11. TRI-MEF SOP

0689-OPER-2504: Administer technical Information Assurance controls

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, equipment, and references.

STANDARD: To ensure adherence to Information Assurance constructs, policies, and procedures.

PERFORMANCE STEPS:
1. Administer secure router solutions.
2. Administer access control lists.
3. Administer secure remote access services.
4. Administer secure switch solutions.
5. Administer intrusion prevention solutions.
6. Administer firewall solutions.
7. Administer intrusion detection solutions.
8. Administer virtual private network solutions.
9. Administer content filtering solutions.
10. Administer e-mail filtering solutions.
11. Administer remediation solutions.
12. Administer secure network service solutions.
13. Administer malicious code solutions.
14. Administer vulnerability assessments solutions.
15. Administer auditing solutions.
16. Administer forensic solutions.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Information Assurance Technical Framework Release 3.1, September 2002
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-OPER-2505: Conduct technical Information Assurance assessment

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning policies, equipment, and references.

STANDARD: To internally validate network security posture and provide recommendations on vulnerabilities.

PERFORMANCE STEPS:
1. Obtain approval to perform assessment.
2. Identify applicable policies.
3. Determine assessment scope.
4. Determine assessment objectives.
5. Create assessment plan.
6. Gather network documentation.
7. Determine tool types.
8. Operate assessment tools.
9. Analyze assessment results.
10. Report assessment results.
11. Provide remediation plan.

REFERENCES:
1. DISA STI CHKLST DISA Security Technical Implementation Checklists
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCIAED Marine Corps Information Assurance Enterprise Directives
4. Applicable Technical Publications/Manuals
5. JITC Assessment Methodologies
6. Marine Corps Assessment Methodologies
7. NIST Special Publication 800 Series
8. NSA Operational Security Doctrine Publications
9. NSA Security Recommendation Guides
10. TRI-MEF SOP

0689-OPER-2506: Conduct advanced technical Information Assurance (IA)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning policies, equipment, and references.

STANDARD: To externally validate network security posture and provide recommendations on vulnerabilities.

PERFORMANCE STEPS:
1. Identify applicable policies.
2. Determine assessment scope.
3. Determine assessment objectives.

4. Create assessment plan.
5. Gather network documentation.
6. Obtain approval to perform assessment.
7. Determine tool types.
8. Operate assessment tools.
9. Conduct penetration testing.
10. Analyze assessment results.
11. Provide remediation plan.

REFERENCES:
1. DISA STI CHKLST DISA Security Technical Implementation Checklists
2. DISA STIGS DISA Security Technical Implementation Guides
3. MCIAED Marine Corps Information Assurance Enterprise Directives
4. Applicable Technical Publications/Manuals
5. JITC Assessment Methodologies
6. Marine Corps Assessment Methodologies
7. NIST Special Publication 800 Series
8. NSA Operational Security Doctrine Publications
9. NSA Security Recommendation Guides
10. TRI-MEF SOP

0689-OPER-2507: Conduct Incident Handling

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning policies, equipment, and references.

STANDARD: To provide effective and timely network operations reporting for incidents on information systems and computer networks.

PERFORMANCE STEPS:
1. Collect intrusion artifacts.
2. Analyze intrusion artifacts.
3. Coordinate with CND technicians.
4. Document CND incidents from detection to resolution.
5. Correlate incident data.
6. Perform trend analysis.
7. Coordinate with intelligence analysts.
8. Coordinate with law enforcement agencies.
9. Publish guidance and documents on incident findings.

REFERENCES:
1. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
2. DoDI 8500.2 Information Assurance Implementation
3. Applicable Technical Publications/Manuals
4. NIST Special Publication 800 Series

0689-OPER-2508: Conduct Computer and Computer Network Forensics

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning policies, equipment, and references.

STANDARD: To collect and analyze information and systems pertaining to incidents on information systems and computer networks.

PERFORMANCE STEPS:
1. Identify applicable laws and policies.
2. Engineer network logging functions.
3. Engineer traffic analysis function.
4. Collect network event information.
5. Correlate network event information.
6. Collect data from computer system.
7. Recover data from a computer system.
8. Analyze a computer system.
9. Document digital evidence.
10. Coordinate with law enforcement agencies.
11. Document findings.

REFERENCES:
1. DoDI 8500.2 Information Assurance Implementation
2. Applicable Technical Publications/Manuals
3. NIST Special Publication 800 Series
4. TRI-MEF SOP

0689-MANT-2601: Maintain technical Information Assurance controls

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Information Assurance policies, planning documents, equipment, and references.

STANDARD: To protect, monitor, analyze, detect and respond to unauthorized activity on information systems and computer networks.

PERFORMANCE STEPS:
1. Maintain secure router solutions.
2. Maintain access control lists.

3. Maintain secure remote access services.
4. Maintain secure switch solutions.
5. Maintain intrusion prevention solutions.
6. Maintain firewall solutions.
7. Maintain intrusion detection solutions.
8. Maintain virtual private network solutions.
9. Maintain content filtering solutions.
10. Maintain e-mail filtering solutions.
11. Maintain remediation solutions.
12. Maintain secure network service solutions.
13. Maintain malicious code solutions.
14. Maintain vulnerability assessments solutions.
15. Maintain auditing solutions.
16. Maintain forensic solutions.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DoDI 8500.2 Information Assurance Implementation
7. MCIAED Marine Corps Information Assurance Enterprise Directives
8. Applicable Technical Publications/Manuals
9. NIST Special Publication 800 Series
10. NSA Operational Security Doctrine Publications
11. NSA Security Recommendation Guides
12. TRI-MEF SOP

0689-MNGT-2701: Supervise an Information Assurance program

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Information Assurance policies, planning documents, planning policies, and references.

STANDARD: In accordance with DODD_8500.1, CJCSM_6510.1, and SECNAVMAN 5239.1.

PERFORMANCE STEPS:
1. Validate compliance with applicable policies.
2. Validate compliance with certification and accreditation policy.
3. Validate compliance with Information Assurance training policy.
4. Validate compliance with Information Assurance vulnerability management policy.
5. Validate compliance with contingency policy.

6. Validate compliance with auditing policy.
7. Validate compliance with physical security policy.
8. Validate compliance with configuration management policy.
9. Validate compliance with incident response policy.
10. Validate compliance with Joint policy.
11. Validate compliance with Information Assurance roles.
12. Validate compliance with Information Assurance Responsibilities.
13. Validate compliance with reporting policy.
14. Validate compliance with information condition policy.
15. Validate compliance with operational security policy.
16. Validate compliance with personnel security policy.
17. Validate compliance with access policy.
18. Validate compliance with assessment policy.

REFERENCES:
1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DON IA PUBS Department of Navy Information Assurance Publications
6. DoDD 8500.1 Information Assurance
7. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
8. DoDI 8500.2 Information Assurance Implementation
9. MCIAED Marine Corps Information Assurance Enterprise Directives
10. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
11. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
12. Applicable Technical Publications/Manuals
13. Information Assurance Technical Framework Release 3.1, September 2002
14. NIST Special Publication 800 Series
15. NSA Operational Security Doctrine Publications
16. NSA Security Recommendation Guides
17. TRI-MEF SOP

0689-MNGT-2702: Enforce Information Assurance plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

MOS PERFORMING: 0689

GRADES: SGT, SSGT, GYSGT, MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided Information Assurance policies, planning documents, planning policies, and references.

STANDARD: To provide validation of compliance with the Information Assurance program.

PERFORMANCE STEPS:

1. Validate compliance with applicable policies.
2. Validate compliance with certification and accreditation policy.
3. Validate compliance with Information Assurance training policy.
4. Validate compliance with Information Assurance vulnerability management policy.
5. Validate compliance with contingency policy.
6. Validate compliance with auditing policy.
7. Validate compliance with physical security policy.
8. Validate compliance with configuration management policy.
9. Validate compliance with incident response policy.
10. Validate compliance with Joint policy.
11. Validate compliance with Information Assurance roles.
12. Validate compliance with Information Assurance Responsibilities.
13. Validate compliance with reporting policy.
14. Validate compliance with information condition policy.
15. Validate compliance with operational security policy.
16. Validate compliance with personnel security policy.
17. Validate compliance with access policy.
18. Validate compliance with assessment policy.
19. Validate compliance with Information Assurance plan.
20. Supervise implementation of Information Assurance plan.

REFERENCES:

1. CJCSI 6510.01_ Information Assurance and Computer Network Defense
2. CJCSM 6510.1 Defense in Depth, Information Assurance and Computer Network Defense
3. DISA STI CHKLST DISA Security Technical Implementation Checklists
4. DISA STIGS DISA Security Technical Implementation Guides
5. DODI 8551.1 Ports, Protocols and Services Management
6. DON IA PUBS Department of Navy Information Assurance Publications
7. DoD 8570.01_ Information Assurance Training, Certification, and Workforce Program Manual
8. DoDD 8500.1 Information Assurance
9. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
10. DoDD 8570.1 Information Assurance Training, Certification, and Workforce Management
11. DoDI 8500.2 Information Assurance Implementation
12. MCIAED Marine Corps Information Assurance Enterprise Directives
13. MCO 5239.2 Marine Corps Information Assurance Program (MCIAP) (C4) (NOV 2002)
14. SECNAVINST 5239.3_ Department of Navy Information Assurance Policy
15. Applicable Technical Publications/Manuals
16. Information Assurance Technical Framework Release 3.1, September 2002
17. NIST Special Publication 800 Series
18. NSA Operational Security Doctrine Publications
19. NSA Security Recommendation Guides
20. TRI-MEF SOP

COMM T&R MANUAL

CHAPTER 27

MOS 0699 INDIVIDUAL EVENTS

CHAPTER 27

MOS 0699 INDIVIDUAL EVENTS

27000. INDEX OF INDIVIDUAL EVENTS

27001. 2000-LEVEL EVENTS

0699-MNGT-2701: Supervise the execution of a communications plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, operational conditions, operational plans, and communications systems architecture.

STANDARD: That satisfies the commander's communications system requirements for command and control during a given operation.

PERFORMANCE STEPS:
1. Direct the execution of a communications plan.
2. Direct communications control functions and procedures.
3. Direct communication security functions and procedures.
4. Direct information assurance functions and procedures.
5. Evaluate communications system architecture performance.
6. Determine communications system architecture modifications.
7. Oversee System Control (SYSCON).

REFERENCES:
1. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
2. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
3. MCWP 5-1 Marine Corps Planning Process (MCPP)

0699-MNGT-2702: Manage communication resources

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 18 months

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's Mission Essential Task List, Training Exercise and Employment Plan, Table of Organization and Equipment, resource readiness documents, and mission.

STANDARD: To ensure resource availability to satisfy the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Determine equipment resources.
2. Organize equipment resources.
3. Determine logistical requirements.
4. Determine equipment readiness.
5. Address HAZMAT considerations.
6. Address Safety considerations.

7. Maintain equipment accountability.
8. Identify personnel resources.
9. Organize personnel resources.

REFERENCES:
1. DoDD 8570.01 Information Assurance Training, Certification, and Workforce Management
2. HAZMAT BASE AND UNIT SOP'S
3. MATERIAL SAFETY MATERIAL SAFETY DATA SHEETS
4. MCO 5100.25 Hazardous Material Information System
5. MCO P4790.2_ MIMMS Field Procedures Manual
6. MCRP 3-0A Unit Training Management Guide
7. MCWP 4-11 Combat Service Support
8. NREA/EPA FEDERAL, STATE AND LOCAL NREA/EPA REQUIREMENTS

0699-MNGT-2703: Prepare a communications plan

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given a command's mission, task organization, table of organization and equipment, constraints, restraints, commanders battlespace area evaluation, initial planning guidance, intelligence preparation of the battlespace (IPB) products, and higher headquarters Annex K.

STANDARD: To provide guidance and to satisfy the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Identify mission tasks, constraints and restraints.
2. Analyze planning documents.
3. Analyze Courses of Actions.
4. Identify communications resources available.
5. Identify communications resources limitations.
6. Determine a command's radio network requirements.
7. Determine a command's telephony requirements.
8. Determine a command's data requirements.
9. Determine a command's information assurance requirements.
10. Determine communications control reporting procedures.
11. Determine requirements for communications control facility.
12. Draft the communication plan.
13. Prepare confirmation brief.

REFERENCES:
1. CJCSI 6510.01E Information Assurance (IA) and Computer Network Defense (CND) 15 August 2007
2. CJCSM 6231 (Series) Manual for Employing Joint Tactical Communications
3. CJCSM 6231.04B MANUAL FOR EMPLOYING TACTICAL COMMUNICATIONS
4. DoDI 8500.2 Information Assurance (IA) Implementation
5. JOINT PUB 3-02 Joint Doctrine for Amphibious Operations
6. MCEB Pub 7 Frequency Resource Record System (FRRS) Standard Frequency Action Format

7. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
8. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
9. MCWP 5-1 Marine Corps Planning Process (MCPP)
10. TM 2000-15/1_ Brief Description of U.S. Marine Corps Communication-Electronics Equipment

---

0699-MNGT-2704: Manage the embarkation of communications resources

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: Provided Table of Organization and Equipment, planning documents, and Commander's guidance.

STANDARD: By validating the Equipment Density List (EDL) to ensure that all required assets are properly inventoried, marked, embarked and available to satisfy the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Supervise the embarkation NCO.
2. Establish liaison with unit embarkation chief.
3. Ensure adequate embarkation materials are available and properly marked.
4. Prioritize items for embarkation.
5. Prepare the personnel manifest for the unit.
6. Review Equipment Density List (EDL).
7. Coordinate special lifting/handling requirements for Communications-Electronics (C-E) equipment.
8. Rehearse embarkation procedures.
9. Supervise embarkation/debarkation of personnel and equipment.

REFERENCES:
1. DODD 4500.9E Transportation and Traffic Management September 11, 2007
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. JOINT PUB 3-02 Joint Doctrine for Amphibious Operations
4. MCO P4600.7_ USMC Transportation Manual
5. MCRP 3-40-3_ Multi-Service Communications Procedures and Tactical Radio Procedures in Joint Environment
6. MCWP 3-40.3 MAGTF Communications System, 8 January 2010
7. MCWP 5-1 Marine Corps Planning Process (MCPP)

0699-MNGT-2705: Manage Communications Security (COMSEC)/Electronic Key Management System (EKMS) Local Element (LE)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

MOS PERFORMING: 0699

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, Commander's guidance and references.

STANDARD: Ensuring the unit's security policies are maintained and enforced, accountability of all Local Element COMSEC equipment, and per the references.

PERFORMANCE STEPS:
1. Identify EKMS requirements.
2. Verify unit clearance/access roster.
3. Monitor adherence to current EKMS regulations.
4. Monitor COMSEC incident reports, as required.
5. Review Emergency Action Plan (EAP) and recommend changes/updates, as required.
6. Complete local element CBT.

REFERENCES:
1. CMS-9 DON Certification Authority Policy and Procedures (DRAFT)
2. EKMS-1 (series) EKMS Policy and Procedures for Navy EKMS Tiers 2 & 3
3. EKMS-3 (series) EKMS Inspection Manual
4. EKMS-5A Cryptographic Equipment Information/Guidance Manual
5. Joint PUB 6-05.5 JT COMSEC
6. NAG-14_ Safeguarding COMSEC Material and Facilities
7. OPNAVINST 2201.3 COMSEC Monitoring
8. SECNAVINST 5510.30_ Dept of Navy Personnel Security Program
9. SECNAVINST 5510.36_ Dept of the Navy Information and Personnel Security Program Regulations

---

0699-MNGT-2706: Manage Communication-Electronic Maintenance programs

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL:** 12 months

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided planning documents, maintenance management automated system and, Commander's guidance.

STANDARD: To ensure readiness status of equipment assets are accurate, current and capable of satisfying the commander's communications system requirements for command and control.

PERFORMANCE STEPS:
1. Review relevant maintenance reports.
2. Review Publication Control program.
3. Review Modification Control program.
4. Review Calibration Control program.

REFERENCES:
1. MCO P4400.82_ Regulated/Controlled Item Management Manual

2. MCO P4790.2_ MIMMS Field Procedures Manual
3. UM 4790-5 MIMMS AIS, Field Maintenance Procedures

0699-PROT-2801: Manage Information Assurance (IA) in a computing environment (CE)

EVALUATION-CODED: NO **SUSTAINMENT INTERVAL**: 12 months

DESCRIPTION: The CE is defined as local area network(s) server host and its operating system, peripherals and applications.

MOS PERFORMING: 0602

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Provided a computing environment, IA directives and IA trained personnel.

STANDARD: To maintain availability, integrity, authentication, confidentiality, and non-repudiation of information systems and information infrastructures.

PERFORMANCE STEPS:
1. Adhere to HQMC C4 IA Directives.
2. Provide system related input on IA security requirements.
3. Ensure data retention and recovery within the CE.
4. Coordinate with higher headquarters IAM in the development or modification of the computer environment IA security program plans and requirements.
5. Ensure CE users meet systems authorization access requirements.
6. Recognize security violations.
7. Report security violations.
8. Supervise corrective measures to IA vulnerabilities.
9. Supervise the adherence of system security configuration guidelines.
10. Comply with IA security requirements in a CE.
11. Coordinate IA inspections, tests, and reviews.
12. Participate in the Certification and Accreditation process.
13. Collect data for IA reporting requirements.
14. Within six months of being assigned to an IAM Level I billet, obtain IA certification appropriate to position.
15. Maintain IA Certification appropriate to position.

REFERENCES:
1. CJCSI 6510.01E Information Assurance (IA) and Computer Network Defense (CND) 15 August 2007
2. CJCSM 6510.01A Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program) 24 June 2009
3. DoD 8570.01-M Information Assurance Workforce Improvement Program Incorporating Change 2, April 20, 2010
4. DoDD 8500.1 Information Assurance (IA)
5. DoDD 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)

6. DoDI 8500.2 Information Assurance (IA) Implementation
7. SECNAVINST 5239.3B DEPARTMENT OF THE NAVY INFORMATION ASSURANCE POLICY 17 June 2009

MISCELLANEOUS:

ADMINISTRATIVE INSTRUCTIONS: Certification is obtained from an authorized commercial vendor or Communication Training Centers.

SPECIAL PERSONNEL CERTS: COMP TIA SY0-101 Security + Certification

COMM T&R MANUAL

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ABCS . . . . . Army Battle Command System
ACE . . . . . Aviation Combat Element
ADCON . . . . . Administrative Control
ADP . . . . . Automatic Data Processing
AEHF . . . . . Advanced Extremely High Frequency
AES . . . . . Advanced Encryption Standard
AIS . . . . . Automated Information System
AMHS . . . . . Automated Message Handling System
AO . . . . . Area of Operations
AOC . . . . . Air Operations Center
AOR . . . . . Area of Responsibility
ASCII . . . . . American Standard Code for Information Interchange
ASD (NII) Assistant Secretary of Defense (Network and Information Integration
ASI . . . . . Authorized Service Interruption
ATC . . . . . Air Traffic Control
ATE. . . . . Automated Test Equipment
ATM . . . . . Asynchronous Transfer Mode
ATO . . . . . Authorization to Operate
AUTODIN . . . . . Automatic Digital Network
AWS . . . . . Advanced Wideband System
BDA. . . . . Battle Damage Assessment
BER . . . . . Bit Error Rate
BGP . . . . . Border Gateway Protocol
C2. . . . . command and control
C2PC . . . . . Command and Control Personal Computer
C2W . . . . . Command and Control Warfare
C3 . . . . . Command, Control, Communications
C3I . . . . . Command, Control, Communications, and Intelligence
C4 . . . . . Command, Control, Communications, and Computers
C4I. . . . . Command, Control, Communications, Computers and Intelligence
C4ISR. . . . . Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C&A . . . . . Certification and Accreditation
CA . . . . . Civil Affairs
CA . . . . . Certification Authority
CAC . . . . . Common Access Card
CAG . . . . . Civil Affairs Group
CAP . . . . . Connection Approval Process
CATF . . . . . Commander Amphibious Task Force
CCC . . . . . Communications Control Center
CCDR . . . . . .Combatant Commander
CCIR . . . . . .Commander’s Critical Information Requirements
CCITT . . . Consultative Committee for International Telegraphy and Telephony
CCSD . . . . . Command Communications Service Designator
CDS . . . . . Cross Domain Solution
CE . . . . . .Command element

CE . . . . . .Computing Environment
CEOI . . . . . Communication Electronics Operating Instruction
CI . . . . . .Counterintelligence
CI/D . . . . . Combat Information / Detection
CIO . . . . . Chief Information Officer
CJCS . . . . . .Chairman of the Joint Chiefs of Staff
CJCSI . . . . . Chairman of the Joint Chiefs of Staff instruction
CJCSM . . . . . .Chairman of the Joint Chiefs of Staff manual
CJTF . . . . . Commander Joint Task Force
CLB . . . . . Combat Logistics Battalion
CLF . . . . . Commander Landing Force
CLR . . . . . Combat Logistics Regiment
CLS . . . . . Contractor Logistical Support
CND . . . . . Computer Network Defense
COA . . . . . .Course of Action
COC . . . . . .Combat Operations Center
COCOM . . . . . Combatant Command (Command Authority)
COG . . . . . .Centers of Gravity
COMM . . . . . Communications
COMMBN . . . . . Communications Battalion
COMMCON . . . . . .Communications Control
COMPUSEC . . . . . .Computer Security
COMSEC . . . . . .Communications security
CONOPS . . . . . .Concept of Operations
CONUS . . . . . Continental United States
COTS . . . . . Commercial off the Shelf
CND . . . . . Computer Network Defense
CS . . . . . Content Staging
C/S . . . . . Chief of Staff
CSN . . . . . Circuit Switch Network
CSS . . . . . Combat Service Support
CTO . . . . . Computer Tasking Order
DAA . . . . . Designated Approving Authority
DASC . . . . . Direct Air Support Center
DARPA . . . . . Defense Advanced Research Projects Agency
DATMS . . . . . DISN Asynchronous Transfer Mode Services
DCID . . . . . .Director of Center Intelligence Directive
DCN . . . . . Data Link Coordination Net
DCTS . . . . . Defense Collaboration Tool Suite
DISA . . . . . Defense Information Systems Agency
DISN . . . . . Defense Information Systems Network
DLR . . . . . Depot Level Reparable
DITS . . . . . .Deployable Integrated Transport Suite
DISA . . . . . .Defense Information Services Agency
DMS . . . . . .Defense Message System
DMZ . . . . . .Demilitarized Zone
DNS . . . . . .Domain Name Services
DoD . . . . . Department of Defense
DoDD . . . . . Department of Defense Directive
DoDI . . . . . Department of Defense Instruction
DoS . . . . . Denial of Service
DRSN . . . . . Defense Red Switch Network
DSCS . . . . . .Defense Satellite Communications System
DSID . . . . . Deployed Security Interdiction Device
DSN . . . . . Defense Switched Network

DSO . . . . . Defense Spectrum Office
DTC . . . . . .Digital Technical Control Facility
DVSG . . . . . DISN Video Services Global
E3 . . . . . .Electromagnetic environmental effects
EA . . . . . .Electronic Attack
EEFI . . . . . Essential Elements of Friendly Information
EGP . . . . . Exterior Gateway Protocol
EHF . . . . . .Extremely High Frequency
EIGRP . . . . . Enhanced Interior Gateway Routing Protocol
EKMS . . . . . Electronic Key Management System
ELMACO . . . . . .Electronics Maintenance Company
EMCON . . . . . Emissions Control
EMI . . . . . .Electromagnetic interference
EMO . . . . . Electronics Maintenance Officer
EOIP . . . . . Everything Over IP
EPLRS . . . . . .Enhanced Position Reporting System
ERO . . . . . .Equipment repair order
ES . . . . . Electronic Support
ESD . . . . . Electrostatic Discharge
ESG . . . . . Expeditionary Strike Group
EW . . . . . Electronic Warfare
FCC . . . . . Federal Communications Commission
FDC . . . . . Fire Direction Center
FDM . . . . . Frequency Division Multiplexing
FEC . . . . . Forward Error Correction
FFCC . . . . . Force Fires Coordination Center
FFIR . . . . . Friendly Force Information Requirements
FIPS . . . . . Federal Information Processing Standard
FLTSATCOM . . . . . .Fleet Satellite Communications
FM . . . . . .Field Manual (Army)
FORTEZZA . . . . . NSA encryption and security standard
FOUO . . . . . For Official Use Only
FRAGO . . . . . Fragmentary Order
FSCC . . . . . Fire Support Coordination Center
FTP . . . . . File Transfer Protocol
FTS . . . . . Federal Telecommunications System
GAA . . . . . Gateway Access Authorization
GAR . . . . . Gateway Access Request
GB . . . . . Gigabit
GBNP . . . . . Global Block Numbering Plan
Gbps . . . . . Gigabits per second
GBS . . . . . Global Broadcast System
GCCS . . . . . Global Command and Control System
GCE . . . . . Ground Combat Element
GHz . . . . . Gigahertz
GIG . . . . . Global Information Grid
GMF . . . . . .Ground Mobile Forces
GNCC . . . . . Global NetOps Control Center
GOTS . . . . . Government Off The Shelf
GPS . . . . . Global Positioning System
GPTE . . . . . General Purpose Test Equipment
H&S . . . . . Headquarters and Service
HAG . . . . . High Assurance Guard
HAIPE . . . . . High Assurance IPE Encryptor
HBSS . . . . . Host Based Security System

HF . . . . . High Frequency
HQ . . . . . Headquarters
HQMC . . . . . Headquarters Marine Corps
HTML . . . . . HyperText Markup Language
HTTP . . . . . HyperText Transfer Protocol
HTTP-S . . . . . HyperText Transfer Protocol-Secure
IA . . . . . Information Assurance
IAM . . . . . Information Assurance Manager
IAT . . . . . Information Assurance Technician
IATC . . . . . Interim Authority To Connect
IATO . . . . . Interim Authority To Operate
IAVA . . . . . Information Assurance Vulnerability Alert
IAVM . . . . . Information Assurance Vulnerability Management
IBGP . . . . . Interior Border Gateway Protocol
ICMP . . . . . Internet Control Message Protocol
IDNX . . . . . Integrated Data Network Exchange
IDS . . . . . Intrusion Detection System
IGMP . . . . . Internet Group Management Protocol
IGP . . . . . Internet Gateway Protocol
IGRP . . . . . Interior Gateway Routing Protocol
INFOCON . . . . . Information Operations Condition
INFOSEC . . . . . Information Security
INMARSAT . . . . . International Maritime Satellite
IOM . . . . . Install Operate Maintain
IP . . . . . Internet Protocol
IPS . . . . . Interim Polar System
IPV4 . . . . . Internet Protocol Version 4
IPV6 . . . . . Internet Protocol Version 6
IPX . . . . . Internet Packet Exchange Protocol
ISD . . . . . Information Services Directory
ISDN . . . . . Integrated Services Digital Network
ISP . . . . . Internet Service Provider
ITU-T . . . . . International Telecommunications Union-Telecommunications
JCCC . . . . . Joint Communications Control Center
JCMA . . . . . Joint COMSEC Monitoring Activity
JCS . . . . . Joint Chiefs of Staff
JCSE . . . . . Joint Communications Support Element
JDN . . . . . Joint Data Network
JEECS . . . . . .Joint Enhanced Core Communication System
JFC . . . . . Joint Force Commander
JIC . . . . . Joint Intelligence Center
JITC . . . . . .Joint Interoperability Test Command
JNCC . . . . . Joint NetOps Control Center
JOPES . . . . . Joint Operation Planning and Execution System
JP . . . . . .Joint Publication
JSC . . . . . Joint Spectrum Center
JTF . . . . . .Joint Task Force
JTF GNO . . . . . .Joint Task Force Global Network Operations
JTRS . . . . . .Joint Tactical Radio System
JWICS . . . . . .Joint Worldwide Intelligence Communications System
LRU . . . . . Line Replaceable Unit
LTI . . . . . .limited technical inspection
kW . . . . . Kilowatt
LAN . . . . . Local Area Network
LCE . . . . . Logistics Combat Element

LFOC . . . . . Landing Force Operations Center
LOC . . . . . Logistics Operations Center
LOS . . . . . Line of Sight
LPD . . . . . Low Probability Detection
LPI . . . . . Low Probability Intercept
MAC . . . . . .Media Access Control
MACCS . . . . . Marine Air Command and Control System
MACG . . . . . Marine Air Control Group
MAG . . . . . Marine Aircraft Group
MAGTF . . . . . .Marine Air-Ground Task Force
MARFOR . . . . . .Marine Corps Forces
MARFORCOM . . . . . United States Marine Corps Forces Command
MARFORCYBER . . . . . United States Marine Corps Forces Cyber
MARFORRES . . . . . United States Marine Corps Forces Reserve
MARFORPAC . . . . . United States Marine Corps Forces Pacific
MARSOC . . . . . United States Marine Corps Forces Special Operations Command
MAN . . . . . Metropolitan Area Network
MANET . . . . . Mobile Ad-Hoc Networking
MAW . . . . . Marine Aircraft Wing
Mbps . . . . . Megabytes per second
MCCC . . . . . .Marine Corps Command Center
MCDP . . . . . Marine Corps Doctrinal Publication
MCRP . . . . . Marine Corps Reference Publication
MCNOSC . . . . . Marine Corps Network Operations and Security Center
MCR . . . . . Multi-Channel Radio
MCS . . . . . MAGTF Communications System
MCT . . . . . Marine Corps Task
MCTL . . . . . Marine Corps Task List
MCTSSA . . . . . Marine Corps Tactical Systems Support Activity
MCWP . . . . . Marine Corps Warfighting Publication
MEB . . . . . Marine Expeditionary Brigade
MEDEVAC . . . . . Medical Evacuation
MEF . . . . . .Marine Expeditionary Force
MET . . . . . .Mission Essential Task
METL . . . . . .Mission Essential Task List
MEU . . . . . Marine Expeditionary Unit
MHz . . . . . Megahertz
MILSTAR . . . . . Military Strategic Tactical Relay
MIMMS . . . . . Marine Corps Integrated Maintenance Management System
MI . . . . . Modification Instruction
MIS . . . . . Maintenance Information Systems
MISSI . . . . . Multilevel Information Systems Security Initiative
MLC . . . . . Marine Logistics Command
MLG . . . . . Marine Logistics Group
MMS . . . . . Meteorological Measuring Station
MNL . . . . . Master Net List
MODEM . . . . . Modulator - Demodulator
MSC . . . . . Major Subordinate Command
MSDP . . . . . Multicast Source Discovery Protocol
MSOB . . . . . Marine Special Operations Battalion
MUOS . . . . . Mobile User Objective System
MUX . . . . . Multiplexer
MWCS . . . . . Marine Wing Communications Squadron
NAP . . . . . .Network Access Point
NAT . . . . . Network Access Translation

NATO . . . . . North Atlantic Treaty Organization
NCS . . . . . Net Control Station
NCTAMS . . . . . Naval Computer and Telecommunications Area Master Station
NES . . . . . Network Encryption System
NETOPS . . . . . Network Operations
NIC . . . . . Network Interface Card
NIPRNET . . . . . Non-Security Internet Protocol Router Network
NIST . . . . . National Institute of Standard and Technology
NMCI . . . . . Navy Marine Corps Intranet
NMS . . . . . Network Management System
NNTP . . . . . Network News Transfer Protocol
NOC . . . . . Network Operations Center
NOS . . . . . Network Operating System
NOSC . . . . . .Network Operation and Security Center
NSA . . . . . National Security Agency
NTISSC . National Telecommunications and Information Security System Council
NTP . . . . . Network Time Protocol
OAN . . . . . Operational Area Network
OC . . . . . Optical Carrier
OC-3 . . . . . Optical Carrier 3 (155.52 Mbps)
OC-12 . . . . . Optical Carrier 12 (622.08 Mbps)
OC-48 . . . . . Optical Carrier 48 (2.48832 Gbps)
OPCON . . . . . Operational Control
OPLAN . . . . . .Operation Plan
OPORD . . . . . Operation Order
OPSEC . . . . . Operations Security
ORM . . . . . Operational Risk Management
O/S . . . . . Operating System
OSCC . . . . . Operational Systems Control Center
OSI . . . . . Open Systems Interconnect
OSD . . . . . Office of the Secretary of Defense
OSPF . . . . . Open Shortest Path First
OTM . . . . . On the Move
OTN . . . . . Optical Transport Network
OTS . . . . . Optical Transport System
OWA . . . . . Outlook Web Access
PABX . . . . . Private Automatic Branch Exchange
PADS . . . . . Position Azimuth Determining System
PBX . . . . . Private Branch Exchange
PCMCIA . . . . . Personal Computer Memory Card Industry Association
PDA . . . . . Personal Data Assistant
PEB . . . . . Pre-Expended Bin
PED . . . . . Portable Electronic Device
PDS . . . . . Protective Distribution System
PII . . . . . Personally Identifiable Information
PING . . . . . Packet Internet Gopher
PIOM . . . . . Plan Install Operate and Maintain
PIR . . . . . Priority Information Requirements
PK . . . . . Public Key
PKE . . . . . Public Key Encryption
PKI . . . . . Public Key Infrastructure
PLA . . . . . Plain Language Address
PMPA . . . . . Promina Multiservice Access Platform
PMBX . . . . . Private Manual Branch Exchange
PnP . . . . . Ports and Protocols

POA&M . . . . . Plan of Action and Milestones
POES . . . . . Polar-orbiting Operational Environmental Satellite
POP . . . . . Point of Presence
POP3 . . . . . Post Office Protocol ver 3
POTS . . . . . Plain Old Telephone System
PPP . . . . . Point to Point Protocol
PPS . . . . . Ports, Protocols, and Services
PRSL . . . . . Primary Region Switch Locator
PSN . . . . . Packet Switch Network
PSTN . . . . . Public Switched Telephone Network
PTP . . . . . Point to Point
PVC . . . . . Permanent Virtual Circuit
PVP . . . . . Permanent Virtual Path
QA . . . . . Quality Assurance
QOS . . . . . Quality of Service
RadBn . . . . . Radio Battalion
RADIUS . . . . . Remote Authentication Dial In User Service
RARP . . . . . Reverse Address Resolution Protocol
RAS . . . . . Remote Access Server
RCC . . . . . Regional Control Center
RF . . . . . Radio Frequency
RIP . . . . . Routing Information Protocol
RM . . . . . Radiant Mercury
RNOSC . . . . Regional Network Operations and Security Center (now TNC/GNSC)
RSSC . . . . . Regional SATCOM Support Center
RSVP . . . . . Resource Reservation Protocol
RTS . . . . . Real Time Services
SA . . . . . System Administrator
SAA . . . . . Satellite Access Authorization
SAAR . . . . . System Authorization Access Request
SAP . . . . . Special Access Program
SAR . . . . . Satellite Access Request
SATCOM . . . . . Satellite communications
SBB . . . . . Switched Back Bone
SBU . . . . . Sensitive But Unclassified
SCI . . . . . Sensitive Compartmented Information
SCIP . . . . . Secure Communications Interoperability Protocol
SCR . . . . . Single Channel Radio
SDREN . . . . . Secure Defense Research and Engineering Network
SHF . . . . . Super High Frequency
SINCGARS . . . . . Single-Channel Ground and Airborne Radio System
SIP . . . . . Session Initiation Protocol
SIPRNET . . . . . Secret Internet Protocol Router Network
SLD . . . . . System Link Designator
SLIP . . . . . Serial Line Interface Protocol
SME-PED . . . . . Secure Mobile Environment Portable Electronic Device
SMTP . . . . . Simple Mail Transfer Protocol
SNA . . . . . Systems Network Architecture
SNMP . . . . . Simple Network Management Protocol
SOA . . . . . Services Oriented Architecture
SOAF . . . . . Services Oriented Architecture Framework
SONET . . . . . Synchronous Optical Network
SOP . . . . . Standing Operating Procedures
SPE . . . . . Systems Planning and Engineering
SPX . . . . . Sequenced Packet Exchange Protocol

SSA . . . . . Systems Security Administrator
SSAA . . . . . System Security Authorization Agreement
SSH . . . . . Secure Socket Shell
SSL . . . . . Secure Socket Layer
STDM . . . . . Statistical Time Division Multiplexing
STE . . . . . Secure Terminal Equipment
STEP . . . . . .Standardized Tactical Entry
PointSTIG . . . . . .Security Technical Implementation Guidance
STM . . . . . Synchronous Transfer Mode
STS . . . . . Synchronous Transport Signal
STU . . . . . Secure Telephone Unit
SVOIP . . . . . .Secure Voice Over IP
SYSCON . . . . . Systems Control
T-1 . . . . . T-carrier 1 (digital transmission line 1.54 Mbps)
T-3 . . . . . .T-carrier 3 (DIGITAL TRANSMISSION LINE, 44.763 Mbps)
TAC(A). . . . . Tactical Air Coordinator (Airborne)
TACC . . . . . Tactical Air Command Center
TACLANE . . . . . Tactical Local Area Network Encryptor
TACLOG . . . . . Tactical-Logistical Group
TACP . . . . . Tactical Air Control Party
TACSAT. . . . . Tactical Satellite
TAD . . . . . Tactical Air Direction
TADC . . . . . Tactical Air Direction Center
TADIL . . . . . Tactical Digital Information Link
TAOC . . . . . Tactical Air Operations Center
TATC . . . . . Tactical Air Traffic Control
TBMCS. . . . . Theater Battle Management Core System
TCCC . . . . . Theatre C4 Control Center
TCP . . . . . Transmission Control Protocol
TCP/IP . . . . . Transmission Control Protocol / Internet Protocol
TDM . . . . . Time Division Multiplexing
TDMA . . . . . Time Division Multiple Access
T/E . . . . . Table of Equipment
TECHCON . . . . . Technical Control
Telnet . . . . . .Remote Terminal Emulation
TFTP . . . . . Trivial File Transfer Protocol
TI . . . . . .Technical Instruction
TJTN . . . . . Theater Joint Tactical Network
TMDE. . . . . Test Measurement and Diagnostic Equipment
TNAPS . . . . . Tactical Network Analysis and Planning System
TNCC . . . . . Theatre NetOps Control Center
TO . . . . . Task Order
T/O . . . . . Table of Organization
T/O&E . . . . . Table of Organization and Equipment
TRANSEC . . . . . Transmission Security
TRC. . . . . Transcoder
TS . . . . . Top Secret
TS/SCI . . . . . Top Secret/Sensitive Compartmented Information
TSM . . . . . Transition Switch Module
TSO . . . . . Telecommunications Service Order
TSR . . . . . Telecommunications Service Request
TSN. . . . . Track Supervision Net
TTL . . . . . Time to Live
TTP . . . . . Tactics, Techniques, and Procedures
UAV . . . . . Unmanned Aerial Vehicle

UDP . . . . . User Datagram Protocol
UFO . . . . . Ultrahigh Frequency Follow-On
UHF . . . . . Ultrahigh Frequency
ULP . . . . . Upper Layer Protocol
UNI . . . . . User Network Interface
URL . . . . . Uniform Resource Locator
US . . . . . United States
USA . . . . . United States Army
USAF . . . . . United States Air Force
USCG . . . . . United States Coast Guard
USN . . . . . United States Navy
USSOCOM. . . . . United States Special Operations Command
USSTRATCOM . . . . . United States Strategic Command
UTP . . . . . Unshielded Twisted Pair
VA . . . . . Vulnerability Assessment
VHF . . . . . Very High Frequency
VLAN . . . . . Virtual Local Area Network
VMS . . . . . Vulnerability Management System
VOIP . . . . . Voice of IP
VOSIP . . . . . Voice Over Secure IP
VPN . . . . . Virtual Private Network
VTC . . . . . Video Teleconferencing
VTF . . . . . Video Teleconference Facility
VVOIP . . . . . Voice, Video Over IP
WAN . . . . . Wide-Area Network
WGS . . . . . Wideband Global Satellite Communications
WIR . . . . . Recoverable Items Report
WIN-T . . . . . Warfighter Information Network-Tactical
WISP . . . . . Wireless Internet Service Provider
WSOC . . . . . Wideband Satellite Operations Center
WSUS . . . . . Windows Server Update Services
WWW . . . . . World Wide Web
X.25 . . . . . CCITT packet switching protocol
X.121 . . . . . International Numbering Plan for Public Data Networks
X.400 . . . . . CCITT e-mail message protocol
X.500 . . . . . CCITT directory protocol
X.509 . . . . . ITU-T standard for a public key infrastructure (PKI)
XDSL . . . . . X Digital Subscriber Line
XML . . . . . Extensible Markup Language

COMM T&R MANUAL

APPENDIX B

TERMS AND DEFINITIONS

Terms in this glossary are subject to change as applicable orders and directives are revised. Terms established by Marine Corps orders or directives take precedence after definitions found in Joint Pub 1-02, DOD Dictionary of Military and Associated Terms.

A

After Action Review (AAR). A professional discussion of training events conducted after all training to promote learning among training participants. The formality and scope increase with the command level and size of the training evolution. For longer exercises, they should be planned for at predetermined times during an exercise. The results of the AAR shall be recorded on an after action report and forwarded to higher headquarters. The commander and higher headquarters use the results of an AAR to reallocate resources, reprioritize their training plan, and plan for future training.

C

Chaining. A process that enables unit leaders to effectively identify subordinate collective events and individual events that support a specific collective event. For example, collective training events at the 4000-level are directly supported by collective events at the 3000-level. Utilizing the building block approach to progressive training, these collective events are further supported by individual training events at the 1000 and 2000-levels. When a higher-level event by its nature requires the completion of lower level events, they are “chained”; Sustainment credit is given for all lower level events chained to a higher event.

D

Deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy’s interests. (JP 1-02)

E

E-Coded Event. An “E-Coded” event is a collective T&R event that is a noted indicator of capability or, a noted Collective skill that contributes to the unit’s ability to perform the supported MET. As such, only “E-Coded” events are assigned a CRP value and used to calculate a unit’s CRP.

I

Individual Readiness. The individual training readiness of each Marine is measured by the number of individual events required and completed for the rank or billet currently held.

M

Marine Corps Combat Readiness and Evaluation System (MCCRES). An evaluation system designed to provide commanders with a comprehensive set of mission performance standards from which training programs can be developed; and through which the efficiency and effectiveness of training can be evaluated. The Ground T&R Program will eventually replace MCCRES.

O

Operational Readiness (OR). (DoD or NATO) OR is the capability of a unit/formation, ship, weapon system, or equipment to perform the missions or functions for which it is organized or designed. May be used in a general sense or to express a level or degree of readiness.

P

Performance Step. Performance steps are included in the components of an Individual T&R Event. They are the major procedures (i.e., actions) a Marine unit must accomplish to perform an individual event to standard. They describe the procedure the task performer must take to perform the task under operational conditions and provide sufficient information for a task performer to perform the procedure (may necessitate identification of supporting steps, procedures, or actions in outline form). Performance steps follow a logical progression and should be followed sequentially, unless otherwise stated. Normally, performance steps are listed only for 1000-level individual events (those that are taught in the entry-level MOS school). Listing performance steps is optional if the steps are already specified in a published reference.

R

Readiness. (DoD) Readiness is the ability of U.S. military forces to fight and meet the demands of the national military strategy. Readiness is the synthesis of two distinct but interrelated levels: (a) Unit readiness--The ability to provide capabilities required by combatant commanders to execute assigned missions. This is derived from the ability of each unit to deliver the outputs for which it was designed. (b) Joint readiness--The combatant commander’s ability to integrate and synchronize ready combat and support forces to execute assigned missions.

S

Section Skill Tasks. Section skills are those competencies directly related to unit functioning. They are group rather than individual in nature, and require participation by a section (S-1, S-2, S-3, etc).

T

Training Task. This describes a direct training activity that pertains to an individual Marine. A task is composed of 3 major components: a description of what is to be done, a condition, and a standard.

U

Unit CRP. Unit CRP is a percentage of the E-coded collective events that support the unit METL accomplished by the unit. Unit CRP is the average of all MET CRP.

W

Waived Event. An event that is waived by a commanding officer when in his or her judgment, previous experience or related performance satisfies the requirement of a particular event.

APPENDIX C

REFERENCES

National Security Telecommunications and Information Systems Security (NSTISSI)

1000 National Information Assurance Certification / Accreditation Process (NIACAP)
3021 Operational Security Doctrine for the AN-CYZ-10/10A DTD
4002 Classification Guide for COMSEC information
4003 Reporting and Evaluation COMSEC Incidents
4004 Routine Destruction and Emergency Protection of COMSEC material
4005 Safeguarding COMSEC Facilities and materials

Department of Defense Directive (DODD)

Capstone Concept for joint Operations
3222.3 Electromagnetic Environmental Effects (E3) Program
3222.4 Electronic Warfare and Command and Control Warfare Countermeasures
4500.9E Transportation and Traffic Management
4640.13 Management of Base and Lon Haul Telecommunications Equipment and Services
4640.6 Communications Security Telephone Monitoring and Recording
4650.1 Policy for Management and Use of the Electromagnetic Spectrum
5000.1 The Defense Acquisition System
5200.1-R Information Security Program
5200.2-R Personnel Security Program
5200.28 Security Requirements for Automated Information Systems (AIS)
5200.28-STD DoD Trusted Computer System Evaluation Criteria
5200.40 DOD Information Technology Security Certification and Accreditation Process (DITSCAP)
5200.8-R Physical Security Program
7730.65 Defense Readiness Reporting System (DRRS)
8100.2 Use of Commercial Wireless Devices, Services and Technologies in DoD Global Information Grid (GIG)
8500.1 Information Assurance (IA)
8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP)
8530.1 Computer Network Defense
8570.01M Information Assurance Workforce Improvement Program

Department of Defense Instruction (DODI)

3600.2 Classification Guidance for Information Systems
5000.01 The Defense Acquisition System
4650.01 Policy and Procedures for Management and Use of the Electromagnetic Spectrum
5000.2 Operation of the Defense Acquisition System
8410.2 NETOPS for the Global Information Grid (GIG)
8500.2 Information Assurance (IA) Implementation
8510.1 DITSCAP Application Manual
8551.1 Port, Protocols and Services Management

Deputy Secretary of Defense (DEPSECDEF)
CYBEROPS Memo, 15 Oct 2008

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)
3320.01B Electromagnetic Spectrum use in Joint Military Operations
3320.02B Joint Spectrum Interference Resolution (JSIR)
3320.02C Classified Supplemental to the JSIR
3320.03 Joint Communications Electronic Operating Instructions (JCEOI)
6215.01 Policy for the Defense Switched Network
6510.01 Information Assurance (IA) and Computer Network Defense (CND)

Chairman of the Joint Chiefs of Staff Manual (CJCSM)
3122.03 Joint Operational Planning and Execution System Volume II, Planning Formats and Guidance
3212.02B Performing Electronic Attach in the United States and Canada for Tests, Training and Exercises
3212.03 Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
3212.03-1 Classified Supplement to Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada
3320-01 Joint Operations in the Electromagnetic Battlespace
3320-02 Joint Spectrum Interference Report
3320.02A Joint Spectrum Interference Resolution (JSIR) procedures
3320-03 Joint Communications Electronic Operation Instruction
6231 Series Manual for Employing Joint Tactical Communications
6231.01C Manual for Employing Joint Tactical Communications (Joint Systems Management)
6231.02B Manual for the Employment of the Joint Tactical Communications (Joint Voice Communications Systems)
6231.03B Manual for Employing Joint Tactical Communications (Joint Data Systems)
6231.04B Manual for Employing Tactical Communications
6231.05B Manual for Employing Joint Tactical Communications (Joint Communications Security
6231.06B Manual for Employing Joint Tactical Communications (Joint Technical Control Procedures and Systems)
6231.07D Manual for Employing Joint Tactical Communications (Joint Network Management and Control)
6510.01A Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program)

Joint Publications (JPs)
1-02 Department of Defense Dictionary of Military and Associated Terms
2-01.2 Joint Doctrine and Tactics, Techniques and Procedures for Counter Intelligence Support to Operations
3-13 Joint Doctrine for Information Operations
3-30 Command and Control of Joint Air Operations
3-31 Command and Control of Joint Land Operations
3-32 Command and Control of Joint Maritime Operations
3-51 Joint Doctrine for Electronic Warfare
3-54 Joint Doctrine for Operations Security
3-58 Joint Doctrine for Military Deception
5-03.1 Command and Control Systems Estimate
6-0 Joint Communications System

6-02 Joint Doctrine for Operations / Tactical C3 Systems
6-05 Employment of Joint Tactical Communications Systems
6-05.1 Joint Communication Systems Architecture and Management Procedures
6-05.2 Joint Voice Communication Systems
6-05.3 Joint Record Data Communications
6-05.4 Joint Transmission Systems
6-05.5 Joint COMSEC
6-05.7 joint Network Management and Control Systems
JCS Handbook 05-0001 Joint Spectrum Management Handbook

Joint Army, Navy, Air Force Publication (JANAP)
119 Joint Voice Call Sign Book
128 Automatic Digital Network (AUTODIN) Operating Procedures

Marine Corps Doctrinal Publications (MCDPs)
1. Warfighting
2. Intelligence

Marine Corps Warfighting Publications (MCWPs)
2-1 Intelligence Operations
2-6 Counterintelligence
2-22 Signals Intelligence
3-1 Ground Combat Operations
3-40.3 MAGTF Communications Systems
3-40.5 Electronic Warfare
4-11 Combat Service Support
4-26 Supply Operations
5-1 Marine Corps Planning Process
3-16 Fire Support Coordination in the Ground Combat Element
3-33.1 Marine Air-Ground Task Force Civil-Military Operations

Marine Corps Reference Publications (MCRPs)
3-0A Unit Training Management Guide
3-0B How to Conduct Training
3-22_ Spectrum Management
3-40.3A Tactical Radios
3-40.3B Radio Operators Handbook
3-40.3C Field Antenna Handbook
3-40.3E HF-ALE multi Service Procedures for high Frequency-Automatic Link E

Marine Corps Orders (MCO)
1510._ Individual Training Standards (ITS) System for the Communications Information Systems Occupations Field (OCCFLD) 06
2040.10 TSEC KYV-2A
2305.13 Telephone Services at Department of Defense Activities
2400.2 USMC Management of Radio Frequency Spectrum
2410.2_ Electromagnetic Environmental Effects (E3) Control Program
3120.6 Standard Embarkation Management System
3430.1 Performing Electronic Counter Measures in the United States and Canada
3430.2 Policy for Electronic Warfare (EW)
3430.3 Operations Reporting Meaconing, Intrusion, Jamming, and Interference of Electromagnetic Systems
3500.27 Operational Risk Management (ORM)
5100.25 Hazardous Material Information System

5230.1 Marine Corps Information Management Responsibilities
5231.1_ Life Cycle management for Automated Information Systems
5236.2 Automated Data Processing Resource Delegation Program
5239.2 Marine Corps Information Assurance Program (MCIAP) (C4)
5271.1 Information Resources Management (IRM) Standards and Guidelines Programs
5510.14 Marine Corps ADP Security Manual
5521.3 Personnel Security Investigation, Security Clearances and Access
P1200.7 Military Occupational Specialties (MOS) Manual
P2066.1 Marine Corps Installation Telephone System
P4400.15 Consumer Level Supply Policy Manual
P4400.82 Regulated / Controlled Item Management Manual
P4600.7_ Marine Corps Transportation Manual
P4750.3 Painting Camouflage Pattern Painting, Registration Marking and Identification of Marine Corps Tactical Equipment
P4790.1_ Marine Corps Integrated Maintenance Management System (MIMMS) Introduction Manual
P4790.2 MIMMS Field Procedures Manual
P5090.2_ Environmental Compliance and Protection Manual
P5230.14 Marine Corps Data Network (MCDN) Management and Control Manual
P5233.1 Marine Corps ADP Management Standards Manual
P5271.4A E-Mail Policy and Guidance
P5510.14 USMC ADP Security Manual

Marine Corps Information Assurance Operational Standards (MC IA OPSTD)
001 Incident Reporting
002 Firewalls
003 Routers
005 Portable Electronic Devises (PEDS)
006 Virtual Private Networks (VPN)
007 Remote Access

Marine Corps Information Resource Management (IRM)
5231-01 System Development Methodology Overview
5231-02 System Development Methodology Developer Perspective
5231-04 Functional Requirements Definition
5231-06 Detailed Design Specification
5231-20 Requirements Statement
5233-06 Library Management System
5234-01 Programming Standard
5234-04 Naming Conventions
5235-01 Data Dictionary
5239-04 Local and Wide Area Networks
5239-06 Data Access Security
5239-08 Computer Security Procedures
5239-09 Contingency Planning
5239-10 Small Systems Security
5239-13 System Security Plan
5510-01 Information Resources management Data Access Security Manual
5510-04 ADP Contingency Planning

Army Field Manual (FM)
11-372 Outside Plant Cable Placement
11-486 Outside Plant Cable Telecommunications
11-490 Long Haul Telecommunications Services

11-497 Standard Installation Practices HF Radio Communications Systems
11-64 Communications Electronics Fundamentals Transmission Lines, Wave Propagation and Antennas
11-65 High Frequency Radio Communications
20-31 Electric Power Generation in the Field
21-305 Manual for Wheeled Vehicle Driver
21-31 Topographic Symbols
24-16 Communication Electronic Operations Orders, Records and Reports
24-17 Tactical Record Traffic Systems
24-18 Tactical Single Channel Radio Communications Techniques
24-20 Tactical Wire and Cable Techniques
24-21 Tactical Multi-Channel Radio Communications and Techniques
24-22 Communication Electronic Management System
3-25-.26 Map Reading and Land Navigation
34-1 Intelligence and Electronic Warfare Operations
34-130 Intelligence Preparation of the Battlefield

Director of Central Intelligence Directive (DCID)
6/3 Protecting Sensitive Compartmented Information, (SCI) within Information Systems
7/3 Information Operations and Intelligence Community Related Activities

Allied Communications Publication (ACP)
117 Allied Routing Indicator Publication Maintenance System
121 Communication Instructions, General with US Supp 1&2
122 Communication Instructions, Security
125 Communication Instructions for Radio Telephone Procedures
126 Communication Instructions Teletype
127 Communication Instructions Tape Relay Procedures
131 Communication Instruction Operating Procedures
190 Guide to Spectrum Management in Military Operations
194 Policy for the Coordination of Military Radio Frequency Allocations and Assignments Between Cooperating Nations

Army Space Circular (ASC)
1 GMFSC DSCS Management and Operational Policies and Procedures
2 GMFSC Anti-jam Operating Procedures
3 GMFSC Management Policy and Procedures

Miscellaneous

CISCO Publications
7206 I&C: Installation and Configuration Guide
Deployment Guide: Configuring a Virtual Tunnel Interface with IP Security
Exploration LAN Switching and Wireless Text Book
IOS Desktop Switching Software Configuration Guide
IP Telephony Boot camp Student Manual
IP Video conferencing Solution Reference Network Design Guide
Connection on-line (www.cisco.com)
Press Books (www.ciscopress.com)
CISCO Router 24 seven Sybex Manual
SWAN-D Configuration Template Ver.5
IOS Enterprise VPN Configuration Guide
VPN Solution Center IPSEC Solution Provisioning Guide

COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS)
1 COMSEC Material System Policy and Procedures Manual
3 EKMS Inspection Manual
6 STU III Key Management
9 DON Certification Authority Policy and Procedures
21 COMSEC Material System Policy and Procedures

Defense Information Systems Agency (DISA)
Security Technical Implementation Checklists (STI CHKLST)
Security Technical Implementation Guides (STIG)

Department of the Navy (DON)
Department of Navy Information Assurance (IA) Publications

Office of the Secretary of the Navy Instruction (SECNAVINST)
2400.0 Electromagnetic Spectrum Policy and management
5239.3b DoN Information Assurance Policy
5510.30 DoN Personnel Security Program
5510.36 DoN Information and Personnel Security Program Regulations
5720.47 DoN Policy for Content of Publicly Accessible World Wide Web Sites

Office of the Chief of Naval Operations Instruction (OPNAVINST)
2060.8 Management and Business Administration of the DoD Telephone Systems and Base Telecommunications Services within the Department of the Navy
2201.3 COMSEC monitoring
2400.20 Navy Management of the Radio Frequency Spectrum
3850.4 Protection of DoN Personnel and Resources
5239.1 Automated Data processing Security Program
5510.H Information and Personnel Security Program
5530.14 Physical Security and loss Prevention
5530.18 Physical Security Program

Naval Telecommunications Procedures (NTP)
2 Super High Frequency Satellite Communications
3 Telecommunications User Manual
4 Naval Communications
6 Spectrum Management Manual

Director of Central Intelligence Directive (DCID)
6/3 Protecting Sensitive Compartmented Information within Information Systems

Electronic Key Management System (EKMS)
1 Series EKMS Policy and Procedures for Navy EKMS Tiers 2&3
1 Supp-1 CMS Policy and Procedures for Navy EKMS Tiers Legacy Accounts
3 Series EKMS Inspection Manual
5A Cryptographic Equipment Information/Guidance Manual
704 Series LMD/KP Operators Manual