DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

NAVMC 3500.124
C 466
29 June 2018

NAVMC 3500.124

From: Commandant of the Marine Corps
To: Distribution List

Subj: CYBERSPACE TRAINING AND READINESS MANUAL

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

Encl: (1) Cyber T&R Manual

1. Purpose. Per reference (a), this Training and Readiness (T&R) Manual, contained in enclosure (1), establishes training standards, regulations, and policies regarding the training of Marines in the cyberspace occupational field.

2. Cancellation. None.

3. Scope

a. 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. References (c) and (d) provide amplifying information for effective planning and management of training within the unit.

b. Formal school and training detachment commanders will use references (a) and (e) to ensure programs 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. All questions pertaining to the Marine Corps Ground T&R Program and unit training management should be directed to: CG, TECOM, Marine Air-Ground Task Force Training and Education Standards Division (C 466), 1019 Elliot Road, Quantico, Virginia 22134.

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

6. Certification. Reviewed and approved this date.

W. F. MULLEN III
By direction

DISTRIBUTION: 10031984500

LOCATOR SHEET

Subj: CYBERSPACE TRAINING AND READINESS 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

CYBER T&R MANUAL

TABLE OF CONTENTS

CYBER T&R MANUAL

CHAPTER 1

OVERVIEW

CYBER T&R MANUAL

CHAPTER 1

OVERVIEW

1000. INTRODUCTION

1. The training and readiness (T&R) program is the Corps' primary tool for planning, conducting and evaluating training, and assessing training readiness. Subject matter experts (SME) from the operating forces (OPFOR) developed core capability mission essential task lists (METL) for ground communities derived from the Marine Corps task list. This T&R Manual is built around these METLs and other related Marine Corps tasks (MCT). All events contained in this 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. This T&R Manual contains the collective and individual training requirements to prepare units to accomplish their combat mission. This 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. This 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. This T&R Manual is designed for use by unit commanders to determine pre-deployment training requirements in preparation for training and for formal schools and training detachments to create programs of instruction. This manual focuses on individual and collective tasks performed by OPFOR units and supervised by personnel in the performance of unit mission essential task(s) (MET).

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.

2. Commanders will ensure that all training is focused on their combat mission. Unit training should focus on achieving proficiency in the unit METL. This T&R Manual is a tool to help develop the unit's training plan based on the unit METL, as approved by their higher commander and reported in the Defense Readiness Reporting System (DRRS). Training will support the unit METL and be designed to meet T&R standards. Commanders at all levels are responsible for effective combat training. The conduct of standards based training consistent with Marine Corps T&R standards cannot be over emphasized.

1002. UNIT TRAINING MANAGEMENT

1. Effective unit training management (UTM) focuses the overall organization on development of training plans based on the unit METL and standards-based community T&R events. 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 mission.

2. Unit training management techniques, described in reference (b), (c), and (d) provide commanders with the requisite tools and techniques to analyze, design, develop, implement, and evaluate the training of their unit. To maintain an efficient and effective training program, leaders at every level must understand and implement UTM.

1003. SUSTAINMENT AND EVALUATION OF TRAINING

1. Marines are expected to maintain proficiency in the training events for their military occupational specialty (MOS) at the appropriate grade or billet to which assigned. Leaders are responsible for recording the training achievements of their Marines. For collective or individual training events not executed and evaluated as part of the daily routine, leaders must ensure proficiency is sustained by requiring retraining of each event at or before expiration of the designated sustainment interval.

2. 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). 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.

3. 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.

1004. ORGANIZATION. This Cyberspace T&R Manual is comprised of 10 chapters and 2 appendices. Chapter 1 is an overview of the ground T&R program. Chapter 2 lists the core METs/MCTs supported by the Community, which are used as part of DRRS. Chapter 3 contains collective events. Chapters 4 through 10 contain individual events specific to a particular MOS and/or billet, as noted. Appendix A contains acronyms; Appendix B contains terms and definitions.

1005. T&R EVENT CODING

1. Event Code. The event code is an up to 4-4-4 alphanumeric character set:

a. First up to 4 characters indicate MOS or community (e.g., 0321, 1812 or INTL)

b. Second up to 4 characters indicate functional or duty area (e.g. DEF, FSPT, MVMT, etc.)

c. Third 4 characters indicate the unit size and supported unit, if applicable (1000 through 9000), and sequence. Figure 1-1 shows the relationship of unit size to event code. NOTE: The titles for the various echelons are for example only, and are not exclusive. For example: 4000-level events are appropriate for section-level events as noted, but also for squad-level events.

Collective Training **Command Element**	**Collective Training** **Regiment/Group**	**Collective Training** **Battalion/Squadron**
9000-level	8000-level	7000-level
Collective Training **Company**	**Collective Training** **Platoon**	**Collective Training** **Squad**
6000-level	5000-level	4000-level
Collective Training **Team/Section/Crew**	**Individual Training Skills Progression MOJT, Advanced Level Schools (Core Plus Skills)**	**Individual Training Entry-Level Formal School Training (Core Skills)**
3000-level	2000-level	1000-level

Figure. 1-1 T&R Event Levels

2. Grouping. Categorizing events with the use of a recognizable code makes the type of skill or capability being referenced fairly obvious. Examples include: PAT for patrolling events, DEF for events in the defense, FSPT for events related to fire support, etc. There is no special significance to the functional areas, but they should be intuitive to make it as easy as possible for the T&R user to find events. When organizing this T&R Manual, functional areas are alphabetized then the associated events are numbered. The events will be numbered based upon the introduction of each new functional area, allowing up to "999" events. For example: if there are seven administrative events 4431 occupational field (OccFld), then the events should start 4431-ADMN-1001 and run through 1007. Next, the bulk fuel events, BUFL should start at 4431-BUFL-1001.

3. Sequencing. A numerical code is assigned to each collective (3000-9000 level) or individual (1000-2000 level) training event. The first number identifies the size of the unit performing the event, as depicted in figure 1-1. Exception: Events that relate to staff planning, to conduct of a command operations center, or to staff level decision making processes will be numbered according to the level of the unit to which the staff belongs. For example: an infantry battalion staff conducting planning for an offensive attack would be labeled as INF-PLAN-7001 even though the entire battalion is not actively involved in the planning of the operation. T&R event sequence numbers that begin with "9" are reserved for Marine air-ground task force (MAGTF) command element events. An example of event coding is displayed in figure 1-2.

Functional Area

MOS/Community--------> ####-####-#### <-1st event in sequence

Event level

Figure 1-2. T&R Event Coding

1006. T&R EVENT COMPOSITION

1. An event contained within a T&R manual is a collective or individual training standard. This section explains each of the components that make up the T&R event. These items will be included in all of the events in each T&R manual. Community-based T&R manuals may have several additional components not found in unit-based T&R manuals. The event condition, event title (behavior) and event standard should be read together as a grammatical sentence.

2. An example of a collective T&R event is provided in figure 1-3 and an example of an individual T&R event is provided in figure 1-4. Events shown in figures are for illustrative purposes only and are not actual T&R events.

XXXX-XXXX-####: Provide interior guard

SUPPORTED MET(S): MCT #.#.#

EVALUATION CODED: YES/NO SUSTAINMENT INTERVAL: 12 months

DESCRIPTION: Text

CONDITION: Text

STANDARD: Text

EVENT COMPONENTS:
1. Event component.
2. Event component.
3. Event component.

REFERENCES:
1. Reference
2. Reference
3. Reference

PREREQUISITE EVENTS:
XXXX-XXXX-#### XXXX-XXXX-####

INTERNAL SUPPORTED:
XXXX-XXXX-#### XXXX-XXXX-####

INTERNAL SUPPORTING:
XXXX-XXXX-#### XXXX-XXXX-####

SUPPORT REQUIREMENTS:

EQUIPMENT: XXX

MISCELLANEOUS: XXX

ADMINISTRATIVE INSTRUCTIONS: XXX

Figure 1-3. Example of a Collective T&R Event

XXXX-XXXX-####: Stand a sentry post

EVALUATION CODED: NO SUSTAINMENT INTERVAL: 12 months

DESCRIPTION: Text

MOS PERFORMING: ####, ####

INITIAL TRAINING SETTING: XXX

CONDITION: Text

STANDARD: Text

PERFORMANCE STEPS:
1. Event component.
2. Event component.
3. Event component.

REFERENCES:
1. Reference
2. Reference
3. Reference

PREREQUISITE EVENTS:
XXXX-XXXX-#### XXXX-XXXX-####

INTERNAL SUPPORTED:
XXXX-XXXX-#### XXXX-XXXX-####

INTERNAL SUPPORTING:
XXXX-XXXX-#### XXXX-XXXX-####

SUPPORT REQUIREMENTS:

EQUIPMENT: XXX

MISCELLANEOUS: XXX

ADMINISTRATIVE INSTRUCTIONS: XXX

Figure 1-4. Example of an Individual Event

1. Event Code. The event code is explained in paragraph 1005.

2. Title. The name of the event. The event title contains one action verb and one object.

3. Evaluation-Coded (E-Coded). Collective events categorize the capabilities that a given unit may be expected to perform. There are some collective events that the Marine Corps has determined that a unit MUST be able to perform, if that unit is to be considered fully ready for operations. These E-Coded events represent the irreducible minimum or the floor of readiness for a unit. These E-Coded events are derived from the training measures of effectiveness (MOE) for the METs for units that must report readiness in DRRS. It would seem intuitive that most E-Coded events would be for battalion sized units and higher since those are the units that report in DRRS. However, if the Marine Corps has determined that the readiness of a subordinate, supporting unit to accomplish a particular collective event is vital to the accomplishment of the supported unit's MET, then that lower echelon collective event is E-Coded.

4. Supported MET(s). List all METs that are supported by the training event in the judgment of the OccFld drafting the T&R manual, even if those events are not listed as MOE in a MET.

5. Sustainment Interval. It is critical to understand the intent of the sustainment interval so training time is not wasted with duplicated training. Sustainment interval is expressed in number of months. Most individual T&R events and many lower level collective events are never out of sustainment because they are either part of a Marine's daily routine, or are frequently executed within the sustainment interval. Sustainment interval is relevant when an individual or collective event is not observed and evaluated within the sustainment period, has atrophied, and therefore retraining and evaluation is required.

6. Billet/MOS. Each individual training event will contain a billet code and/or MOS that designates who is responsible for performing that event and any corresponding formal course required for that billet. Each commander has the flexibility to shift responsibilities based on the organization of his command. These codes are based on recommendations from the collective subject matter expertise that developed this manual and are listed for each event.

7. Grade. The grade field indicates the rank at which Marines are required to complete the event.

8. Description. This field allows T&R developers to include an explanation of event purpose, objectives, goals, and requirements. It is a general description of an action requiring learned skills and knowledge, i.e., engage fixed target with crew-served weapons. This is an optional field for individual events but is required for collective events. This field can be of great value guiding a formal school or OPFOR unit trying to discern the intent behind an event that might not be readily apparent.

9. Condition. Condition refers to the constraints that may affect event performance in a real-world environment. It indicates what is provided (equipment, tools, materials, manuals, aids, etc.), environmental constraints or conditions under which the task is to be performed, and any specific cues or indicators to which the performer must respond. Commanders can modify the conditions of the event to best prepare their Marines to accomplish the assigned mission (e.g. in a desert environment; in a mountain environment; etc.). When resources or safety requirements limit the conditions, this should be stated. The content of the condition should be included in the event on a "by exception" basis. If there exists an assumption regarding the

conditions under which all or most of the events in the manual will be performed, then only those additional or exceptional items required should be listed in the condition. The common conditions under which all the events in a chapter will be executed will be listed as a separate paragraph at the beginning of the chapter.

10. Standard. The performance standard indicates the basis for judging the 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 must be strictly adhered to. The standard for collective events will likely be general, describing the desired end-state or purpose of the event. The standard for individual events will be objective, quantifiable, and readily observable. Standards will more specifically describe to what proficiency level, specified in terms of accuracy, completeness, time required, and sequencing the event is to be accomplished. These guidelines can be summarized in the acronym "ACTS" (Accuracy Completeness Time Sequence). In no cases will "per the reference" or "per/in accordance with commander's intent" be used as a stand-alone standard.

11. Event Components/Performance Steps. Description of the actions that the event is composed of, or a list of subordinate, included T&R event and event descriptions. The event components help the user determine what must be accomplished and the proper sequence of execution of subordinate events. Event components are used for collective events; performance steps are used for individual events.

a. The event components and performance steps will be consciously written so that they may be employed as performance evaluation check lists by the OPFORs. They must be sequenced to demonstrate the building block approach to training.

b. Event components may be events one individual in the unit performs, events that small groups in the unit perform, or events involving the entire unit.

12. Chained Events. Enables unit leaders to effectively identify prerequisite, supporting, and supported events that ultimately support MCTs/METs. Supported events are chained to supporting events to enable the accomplishment of the supported event to standard and therefore are considered "chained". The completion of identified supported events can be utilized to update sustainment interval credit for supporting events, based on the assessment of the commander.

13. 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.

14. Supported Event. An event whose performance is inherently supported by the performance of one or more supporting events. A supported event will be classified as internal supported if it has been developed specifically for the community. A supported event that has been chained to an event from an external community T&R will be classified as external supported.

15. Supporting Event. An event whose performance inherently supports the performance of a supported event. A supporting event will be classified as internal supporting if it has been developed specifically for the community. A supporting event that has been chained to a community event from an external community T&R will be classified as external supporting.

16. Initial Training Setting. All individual events will designate the setting at which the skill is first taught, either formally, Marine on the Job Training (MOJT) within the OPFOR, or via a distance learning product (DL).

17. References. The training references shall be utilized to determine task performance steps. They assist the trainee in satisfying the performance standards, or the trainer in evaluating the effectiveness of task completion. T&R manuals are designed to be a training outline, not to replicate or replace doctrinal publications, reference publications or technical manuals. References are key to developing detailed lesson plans, determining grading criteria, and ensuring standardization of training. For individual events only one authoritative reference is required.

18. Distance Learning Products. Distance learning products include: Individual multimedia instruction, computer-based training, MarineNet, etc. This notation is included when, in the opinion of the T&R manual group charter in consultation with the Marine Air-Ground Task Force T&R Standards Division representative, the event can be taught via one of these media vice attending a formal course of instruction or receiving MOJT.

19. Support Requirements. This is a list of the external and internal support the unit and Marines will need to complete the event. This is a key section in the overall T&R effort, as resources will eventually be tied directly to the training towards METS. Future efforts to attain and allocate resources will be based on the requirements outlined in the T&R manual. The list includes, but is not limited to:

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

The ordnance requirements for one year of training for the events in the T&R will be aggregated into a table contained in an appendix to the T&R. The task analyst and the OccFld representatives will be careful not to "double count" ammunition that might be employed in the performance of collective and individual events that are chained.

20. Suitability of Simulation/Simulators/DL products. The following "Suitability and Sequence" codes listed in figure 1-5 have been developed to communicate characteristics for employing simulations during training. Units of measure have been assigned based on the amount of time it takes a Marine or unit to train to task utilizing a particular simulator. Suitability and sequence codes are captured in the event title in a parenthetical remark, as well as within the simulation field of the T&R event. The simulation field also identifies the type of simulation, units of measure, and any other pertinent information.

Code	Requirement
L	The event can only be trained to standard in a Live environment. Any event assessed as "NO" for Simulatab1e was coded "L."
P	The event must be performed to standard in simulator as a PREREQUISITE to live fire qualification as per current doctrine, policy, or T&R manual.
S/L	Event must be trained to standard in simulation then live unless simulation capacity is not available, then live only training is appropriate.
L/S	Event must be trained to standard in a live environment then simulation unless simulation capacity is not available, then live only training is appropriate.
S	Event can ONLY be conducted to standard and qualification in simulator.

Figure 1-5. Suitability and sequence codes

a. Training simulation capabilities offer an opportunity to build and sustain proficiency while achieving and/or maintaining certain economies. Commanders should take into consideration simulation tools as a matter of course when designing training.

b. Simulation Terms:

(1) Simulation: A model of a system animated discretely or continuously over a period of time. A simulation may be closed-loop (i.e., it executes based in initial inputs without human intervention), or it may be open-loop (i.e., human input to alter the variables in the system during execution is allowed). A simulation is an approximation of how the modeled system will behave over time. Simulations are constructed based on verified and validated mathematical models of actual systems. Simulations can be very simple or complex depending on the degree of fidelity and resolution needed to understand the behavior of a system.

(2) Simulator: A simulator is the physical apparatus employed as the interface for humans to interact with a model or observe its output. A simulator has input controls and outputs in the form of human sensory stimuli (visual, auditory, olfactory, tactile/haptic, and taste). For instance, some of the features of the vehicle cab (the seat, steering wheel, turn signals, accelerator pedal, brakes, and windshield) and projection screen. Both the vehicle cab and projection screen are the interface by which a human being interacts with the simulated environment of a driving a vehicle and observe the outputs of the mathematical models of vehicle dynamics.

(3) Model: A mathematical representation of the behavior (i.e., shows the behavior of projectiles, combat simulations, etc.) of a system at a distinct point in time.

(4) Live: Real people operates real systems to include both live people operating real platforms or systems on a training range and battle staffs from joint, component or service tactical headquarters using real world command and control systems.

(5) Virtual: Real people operating simulated systems. Virtual simulations inject humans-in-the-loop in a central role by exercising motor control skills (e.g., flying an air platform simulator, engaging targets in indoor simulated marksmanship trainer), decision skills, and/or communication skills.

(6) Constructive: Models and simulations that involve simulated people operating simulated systems (i.e., MAGTF Tactical Warfare Simulation). Real people make inputs to such simulations, but are not involved in determining the outcomes.

(7) Live, Virtual and Constructive (LVC) Training Environment: Defined by combining any of the three training domains LVC to create a common operational environment, by which units can interact across LVC domains as though they are physically located in the same operational environment.

(8) Distance Learning: Any instruction and evaluation provided through a variety of DL delivery systems (i.e., MarineNet) where the students and instructors are separated by time and/or location.

c. Figure 1-6 depicts an event title with simulation code and simulation and/or simulators that can be used, as displayed within a T&R event.

XXXX-XXX-XXXX: Call for indirect fire using the grid method (L/S)

SUPPORT REQUIREMENTS:

SIMULATION EVALUATION:

SIMULATED	SUITABILITY	SIMULATOR	UNIT OF MEASURE	HOURS	PM
Yes	L/S	ODS	Marine Hours	12	Y

Figure 1-6. Example of simulation/simulators displayed within a T&R event

21. Miscellaneous

a. This field provides space for any additional information that will assist in the planning and execution of the event. Units and formal learning centers are cautioned not to disregard this information or to consider the information of lesser importance than what is contained in other parts of the T&R event. Miscellaneous fields provide an opportunity for the drafters of the T&R event to communicate vital information that might not fit neatly into any other available field. The list may include, but is not limited to:

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

1007. COMBAT READINESS PERCENTAGE (CRP)

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 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 E-Coded Events. E-Coded events and unit CRP calculation are described in follow-on paragraphs. The CRP achieved through the completion of E-Coded Events is directly relevant to readiness assessment in DRRS.

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. The 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%

3. Combat readiness percentage is a valuable tool to assist commanders in readiness reporting by providing objective data to support and inform their subjective assessment.

1009. CHEMICAL BIOLOGICAL RADIOLOGICAL NUCLEAR TRAINING

1. All personnel assigned to the OPFOR must be trained in chemical, biological, radiological, and nuclear (CBRN) 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 CBRN attacks. Basic operating standards are those that the individual, and collectively the unit, must perform to continue operations in a CBRN environment.

2. In order to develop and maintain the ability to operate in a CBRN environment, CBRN training is an integral part of the training plan and events in this T&R Manual. Units should train under CBRN conditions whenever possible. Per reference (c), all units must be capable of accomplishing their assigned mission in a contaminated environment.

1010. NIGHT TRAINING

1. While it is understood that all personnel and units of the OPFOR are capable of performing their assigned mission in "every clime 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.

1011. RISK MANAGEMENT (RM)

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

2. All leaders and Marines will integrate RM in the planning process and implement hazard controls to reduce risk to acceptable levels. Applying the RM process will reduce mishaps, injuries, and damage they cause, thereby increasing both individual performance and unit readiness. Risk management assists the commander in avoiding unnecessary risk, determining the balance between training realism and unnecessary risks in training, making an informed decision to implement a course of action, identifying feasible and effective control measures, adjusting training plans to fit the level of proficiency and experience of Marines/Sailors, and providing reasonable alternatives for mission accomplishment.

3. Specifically, commanders are required to implement and document deliberate RM in the planning and execution of all training evolutions and activities. Furthermore, the authority to approve or accept risk assessment

code (RAC) 1 or 2 hazards will not be delegated below lieutenant colonel (O5). Further guidance for RM is found in Marine Corps Order 3500.27_.

1012. IMPROVISED EXPLOSIVE TRAINING

1. Improvised explosive device (IED) threat impacts all elements of the MAGTF and all Marines regardless of MOS, location, or operational environment. The ability to effectively operate and survive in environments with an IED threat is critical to force protection, maintaining combat effectiveness, and mission accomplishment.

2. Per Marine Corps policy on organizing, training, and equipping for operations in an IED environment (MCO 3502.9), Marines must be capable of not only accomplishing their assigned mission, but also accomplishing their mission in environments with an IED threat. Counter-improvised explosive device (C-IED) training must be integrated into the unit training plan in order-to ensure personnel assigned to the OPFOR train and maintain proficiency in C-IED tactics, techniques, and procedures.

CYBER T&R MANUAL

CHAPTER 2

MISSION-ESSENTIAL TASKS

CHAPTER 2

MISSION-ESSENTIAL TASKS

2000. CORE MISSION-ESSENTIAL TASKS (MET).. The MET tables list the standardized core METs for various units supported by the CYBERSPACE community.

2001. CYBERSPACE MCTS

MCT 5.4.2.4	Conduct Cyberspace Operations
MCT 5.9	Plan and Direct Cyberspace Operations
MCT 5.9.2	Conduct Offensive Cyberspace Operations (OCO)
MCT 5.9.3	Plan and Direct Offensive Cyberspace Operations (OCO)
MCT 5.9.4	Conduct Defensive Cyberspace Operations (DCO)
MCT 5.9.5	Plan and Direct Defensive Cyberspace Operations (DCO)

CYBER T&R MANUAL

CHAPTER 3

COLLECTIVE EVENTS

CYBER T&R MANUAL

CHAPTER 3

COLLECTIVE EVENTS

3000. PURPOSE. Chapter 3 contains collective training events for the CYBERSPACE community.

3001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-character, 3-field alphanumeric system, i.e. XXXX-XXXX-XXXX. This chapter utilizes the following methodology:

a. Field one. This field represents the community. This chapter contains the following community codes:

Code	Description
CYBR	CYBERSPACE

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
DCO	Defensive cyberspace operations

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
9000	Brigade/Group Level
8000	Regiment Level
7000	Battalion/Squadron Level
6000	Company Level
5000	Platoon Level
4000	Squad/Section Level
3000	Team/Crew Level

3002. INDEX OF COLLECTIVE EVENTS

Event Code	E-Coded	Event
8000 Level Events		
CYBER-MIG-8001	YES	Direct cyberspace operations
CYBER-MIG-8002	YES	Provide command and control for cyberspace operations
7000 Level Events		
CYBER-IDM-7001	NO	Provide command and control for defensive cyberspace operations
CYBER-MFCY-7001	NO	Operate Cyber Tactical Operations Center (C-TOC)
CYBER-OCAC-7001	NO	Conduct offensive cyberspace operations command and control.

6000 Level Events		
CYBER-IDM-6001	NO	Operate CDOC
CYBER-MFCY-6001	YES	Direct cyberspace operations
CYBER-MFCY-6002	NO	Conduct defensive cyberspace operations
CYBER-MFCY-6003	YES	Conduct offensive cyberspace operations
5000 Level Events		
CYBER-MFCY-5001	YES	Direct defensive cyberspace operations
CYBER-MFCY-5002	YES	Direct offensive cyberspace operations
CYBER-MFCY-5003	NO	Conduct defensive cyberspace operations
CYBER-OCE-5001	NO	Conduct offensive cyberspace operations
4000 Level Events		
CYBER-IDM-4001	NO	Conduct defensive cyberspace operations (GS)
CYBER-IDM-4002	YES	Conduct defensive cyberspace operations (DS)
CYBER-MFCY-4001	YES	Conduct defensive cyberspace operations
3000 Level Events		
CYBER-MFCY-3001	NO	Conduct offensive cyberspace operations
CYBER-RRT-3001	YES	Enable offensive cyberspace operations
CYBER-SST-3001	YES	Enable offensive cyberspace operations

3003. 8000-LEVEL EVENTS

CYBER-MIG-8001: Direct cyberspace operations

SUPPORTED MET(S):

MCT 5.4.2.4	MCT 5.9	MCT 5.9.2
MCT 5.9.3	MCT 5.9.4	MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, facilitate, and deconflict offensive/defensive cyberspace operations.

EVENT COMPONENTS:

1. Review available intelligence and assess current situation.
2. Identify and map key terrain in cyberspace.
3. Identify defensive cyberspace support requirements.
4. Identify offensive cyberspace support requirements.
5. Develop staff process to receive, process, prioritize, and submit cyberspace operations support requests.
6. Plan for the integration of cyberspace operations.
7. Monitor and track execution of cyberspace operations.
8. Publish and disseminate cyberspace support matrix.

REFERENCES:

1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS

7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-IDM-7001 CYBER-OCAC-7001

CYBER-MIG-8002: Provide command and control for cyberspace operations

SUPPORTED MET(S):

MCT 5.4.2.4	MCT 5.9	MCT 5.9.2
MCT 5.9.3	MCT 5.9.4	MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Commanders and battle staff monitor Measures of Effectiveness (MOE) and Measures of Performance (MOP) to achieve end state.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Exercise authority and direction over assigned or attached forces in the accomplishment of the mission.

EVENT COMPONENTS:
1. Maintain situation awareness of current cyberspace operation mission.
2. Integrate Intelligence reporting.
3. Integrate with DODIN operations.
4. Direct cyberspace operations tasks.
5. Coordinate with higher and adjacent.
6. Maintain situational awareness of cyberspace operations.
7. Provide cyberspace operations running estimate.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-IDM-7001 CYBER-OCAC-7001

3004. 7000-LEVEL EVENTS

CYBER-IDM-7001: Provide command and control for defensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

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

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: IOT preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Establish a CDOC.
2. Integrate DCO with DODIN operations.
3. Integrate Intelligence reporting
4. Direct DCO tasks.
5. Maintain situation awareness of current DCO mission.
6. Coordinate with higher and adjacent.
7. Provide DCO running estimate.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-IDM-6001 CYBER-MFCY-6002

CYBER-MFCY-7001: Operate Cyber Tactical Operations Center (C-TOC)

SUPPORTED MET(S):

MCT 5.4.2.4	MCT 5.9	MCT 5.9.2
MCT 5.9.3	MCT 5.9.4	MCT 5.9.5

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

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, facilitate, and deconflict OCO within a Joint Force Headquarters Cyber (JFHQ-C).

EVENT COMPONENTS:
1. Establish a C-TOC.
2. Maintain situation awareness of current OCO mission.
3. Integrate intelligence reporting
4. Direct OCO tasks.
5. Coordinate with higher and adjacent.
6. Maintain situational awareness of OCO operations.
7. Provide OCO running estimate.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-MFCY-6001 CYBER-MFCY-6002 CYBER-MFCY-6003

CYBER-OCAC-7001: Conduct offensive cyberspace operations command and control.

SUPPORTED MET(S):
MCT 5.9.2 MCT 5.9.3

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

DESCRIPTION: Commanders and battle staff monitor Measures of Effectiveness (MOE) and Measures of Performance (MOP) to achieve end state.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Establish SCIF.
2. Establish SCI communications.
3. Maintain situation awareness of current cyberspace operation mission.
4. Plan tactical offensive cyberspace operations.
5. Integrate Intelligence reporting.
6. Integrate with MAGTF operations
7. Direct offensive cyberspace operations tasks.
8. Coordinate with higher and adjacent.

9. Maintain situational awareness of cyberspace operations.
10. Provide offensive cyberspace operations running estimate.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

3005. 6000-LEVEL EVENTS

CYBER-IDM-6001: Operate CDOC

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

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

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Establish a CDOC.
2. Coordinate DCO with DODIN operations.
3. Integrate Intelligence reporting.
4. Direct DCO tasks.
5. Maintain situation awareness of current DCO mission.
6. Coordinate with higher and adjacent.
7. Provide DCO running estimate.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-IDM-4001 CYBER-IDM-4002

CYBER-MFCY-6001: Direct cyberspace operations

SUPPORTED MET(S):

MCT 5.4.2.4	MCT 5.9	MCT 5.9.2
MCT 5.9.3	MCT 5.9.4	MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Exercise authority and direction over assigned or attached forces in the accomplishment of the mission.

EVENT COMPONENTS:

1. Review available intelligence and assess current situation.
2. Identify and map key terrain in cyberspace.
3. Identify defensive cyberspace support requirements.
4. Identify offensive cyberspace support requirements.
5. Develop staff process to receive, process, prioritize, and submit cyberspace operations support requests.
6. Plan for the integration of cyberspace operations.
7. Monitor and track execution of cyberspace operations.
8. Publish and disseminate cyberspace support matrix.

REFERENCES:

1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:

CYBER-MFCY-5001	CYBER-MFCY-5002

CYBER-MFCY-6002: Conduct defensive cyberspace operations

SUPPORTED MET(S):

MCT 5.9.4	MCT 5.9.5

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

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Develop a defensive cyberspace operations plan IOT preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Conduct mission planning.
2. Conduct mission protect.
3. Conduct cyber support.
4. Conduct D&CI.
5. Conduct cyber readiness.
6. Conduct CTE.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:

CYBER-MFCY-4001	CYBER-MFCY-5001	CYBER-MFCY-5003

CYBER-MFCY-6003: Conduct offensive cyberspace operations

SUPPORTED MET(S):

MCT 5.9.2	MCT 5.9.3

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Conduct reconnaissance.
2. Conduct mission planning.
3. Conduct mission.
4. Provide MOE and MOP

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS

7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:
CYBER-MFCY-5002 CYBER-OCE-5001

3006. 5000-LEVEL EVENTS

CYBER-MFCY-5001: Direct defensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Review available intelligence and assess current situation.
2. Identify and map key terrain in cyberspace.
3. Identify defensive cyberspace support requirements.
4. Develop staff process to receive, process, prioritize, and submit cyberspace operations support requests.
5. Plan for the integration of defensive cyberspace operations.
6. Monitor and track execution of defensive cyberspace operations.
7. Publish and disseminate defensive cyberspace support matrix.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS: CYBER-MFCY-4001

CYBER-MFCY-5002: Direct offensive cyberspace operations

SUPPORTED MET(S):

MCT 5.9.2 MCT 5.9.3

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Review available intelligence and assess current situation.
2. Identify and map key terrain in cyberspace.
3. Identify offensive cyberspace support requirements.
4. Develop staff process to receive, process, prioritize, and submit cyberspace operations support requests.
5. Plan for the integration of offensive cyberspace operations.
6. Monitor and track execution of offensive cyberspace operations.
7. Publish and disseminate offensive cyberspace support matrix.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS: CYBER-MFCY-3001

CYBER-MFCY-5003: Conduct defensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

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

DESCRIPTION: The Mission Element is a task organized force and may not contain all elements of DCO

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:

1. Conduct mission planning.
2. Conduct mission protect.
3. Conduct cyber support.
4. Conduct D&CI.
5. Conduct cyber readiness.
6. Conduct CTE.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS: CYBER-MFCY-4001

CYBER-OCE-5001: Conduct offensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.2 MCT 5.9.3

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

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Plan OCO.
2. Coordinate OCO targeting.
3. Execute OCO.
4. Assess OCO effects.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

3007. 4000-LEVEL EVENTS

CYBER-IDM-4001: Conduct defensive cyberspace operations (GS)

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

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

DESCRIPTION: DCO-IDM teams are task organized and may not contain all elements of DCO.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Conduct mission planning.
2. Conduct mission protect.
3. Conduct cyber support.
4. Conduct D&CI.
5. Conduct cyber readiness.
6. Conduct limited penetration testing.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CYBER-IDM-4002: Conduct defensive cyberspace operations (DS)

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Conduct mission planning.
2. Conduct mission protect.

3. Conduct cyber support.
4. Conduct D&CI.
5. Conduct cyber readiness.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS: CYBER-RRT-3001

CYBER-MFCY-4001: Conduct defensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.4 MCT 5.9.5

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: The CPT is task organized and may not contain all elements of DCO.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

EVENT COMPONENTS:
1. Conduct mission planning.
2. Conduct mission protect.
3. Conduct cyber support.
4. Conduct D&CI.
5. Conduct cyber readiness.
6. Conduct CTE.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS: CYBER-MFCY-3001

3008. 3000-LEVEL EVENTS

CYBER-MFCY-3001: Conduct offensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.2 MCT 5.9.3

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

DESCRIPTION: Mission element is a task organized force and may not contain all elements of OCO

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Conduct reconnaissance.
2. Conduct mission planning.
3. Conduct mission.
4. Provide MOE and MOP.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CYBER-RRT-3001: Enable offensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.2 MCT 5.9.3

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: The radio reconnaissance teams support advance force, pre-assault, or other operations where the employment of conventional RadBn teams may be inappropriate or unfeasible. RRTs are a SIGINT/EW/OCO team consisting of six Marines capable of conducting spectrum surveys, Tech-SIGINT collection/analysis, digital network exploitation, Intel/EW/CO systems integration, offensive cyberspace operations, and language translation.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: To support MAGTF operations that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:
1. Integrate with supported unit, as required.
2. Establish security.
3. Establish communications.
4. Conduct tactical OCO.
5. Provide MOE/MOP.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:

1711-OCO-2001	1711-OCO-2002	1711-OPS-2001
1711-OPS-2002	1711-OPS-2003	1711-OPS-2004

CYBER-SST-3001: Enable offensive cyberspace operations

SUPPORTED MET(S):
MCT 5.9.2 MCT 5.9.3

EVALUATION-CODED: YES **SUSTAINMENT INTERVAL:** 12 months

DESCRIPTION: Conventional SIGINT/EW/OCO team consisting of six Marines capable of conducting spectrum surveys, Tech-SIGINT collection/analysis, digital network exploitation, Intel/EW/CO systems integration, offensive cyberspace operations, and language translation.

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: To support MAGTF operations that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

EVENT COMPONENTS:

1. Integrate with supported unit, as required.
2. Establish security.
3. Establish communications.
4. Conduct tactical OCO.
5. Provide MOE/MOP.

REFERENCES:

1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CHAINED EVENTS:

PREREQUISITE EVENTS:

1711-OCO-2001	1711-OCO-2001	1711-OCO-2002
1711-OCO-2002	1711-OPS-2001	1711-OPS-2001
1711-OPS-2002	1711-OPS-2003	1711-OPS-2004

CYBER T&R MANUAL

CHAPTER 4

MOS 1702 INDIVIDUAL EVENTS

CHAPTER 4

MOS 1702 INDIVIDUAL EVENTS

4000. PURPOSE. This chapter details the individual events that pertain to Cyberspace Officers. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

4001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1702	Cyberspace Officer

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
CYBR	Cyberspace
DCO	Defensive cyberspace operations
OCO	Offensive cyberspace operations

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
1000	Core Skills
2000	Core Plus Skills

4002. INDEX OF EVENTS

Event Code	Event
1000 Level Events	
1702-CYBR-1001	Determine cyberspace operations requirement
1702-CYBR-1002	Develop cyberspace operations plan
1702-CYBR-1003	Direct cyberspace operations
2000 Level Events	
1702-CYBR-2001	Direct the integration of Cyberspace Operations
1702-DCO-2001	Direct defensive cyberspace operations
1702-OCO-2001	Direct offensive cyberspace operations

4003. EVENTS

1702-CYBR-1001: Determine cyberspace operations requirement

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

MOS PERFORMING: 1702

GRADES: 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Plan, coordinate, and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:
1. Review the mission tasking.
2. Review intelligence and assess situation.
3. Analyze key terrain in cyberspace.
4. Determine offensive/defensive operational requirements.
5. Review DODIN ops situation.
6. Review capabilities TO/TE.
7. Review authorities.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
10. TAO Tradecraft Guidelines
11. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1702-CYBR-1002: Develop cyberspace operations plan

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

MOS PERFORMING: 1702

GRADES: 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, plan, and coordinate offensive/defensive cyberspace operations.

PERFORMANCE STEPS:

1. Analyze higher headquarters plan.
2. Prioritize requirements.
3. Develop concept of operations.
4. Coordinate with higher/adjacent units.
5. Coordinate with national/theater agencies.
6. Assess intelligence gain/loss (IGL).
7. Assess technical gain/loss (TGL).
8. Conduct de-confliction.
9. Supervise production of cyberspace operation products.
10. Determine measure of effectiveness (MOE).
11. Determine measure of performance (MOP).

REFERENCES:

1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
10. TAO Tradecraft Guidelines
11. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1702-CYBR-1003: Direct cyberspace operations

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

MOS PERFORMING: 1702

GRADES: 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, plan, and coordinate offensive/defensive cyberspace operations.

PERFORMANCE STEPS:

1. Review legal considerations.
2. Coordinate with higher/adjacent units.
3. Coordinate with external agencies.
4. Verify measure of effectiveness (MOE).
5. Verify measure of performance (MOP).
6. Direct actions within the cyberspace domain.
7. Ensure compliance with operational risk management requirements for cyberspace operations.
8. Ensure compliance with appropriate authorities and requirements.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1702-CYBR-2001: Direct the integration of Cyberspace Operations

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

MOS PERFORMING: 1702

GRADES: 2NDLT, 1STLT, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, facilitate, and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:
1. Validate cyberspace techniques, tactics, and procedures.
2. Manage coordination with external agencies.
3. Manage coordination with higher/adjacent units.
4. Advise the commander on CO capabilities.
5. Report findings.
6. Coordinate the approval of CO.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS

5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
10. TAO Tradecraft Guidelines
11. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1702-DCO-2001: Direct defensive cyberspace operations

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

MOS PERFORMING: 1702, 1720

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, facilitate, and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Verify key terrain in cyberspace.
3. Direct risk mitigation plan.
4. Direct mission defense plan.
5. Direct asset identification plan.
6. Direct event audit plan.
7. Direct monitoring plan.
8. Direct strategies to prevent and mitigate intrusion.
9. Report mitigation effectiveness.
10. Participate in change management board.
11. Advise commander on escalation criteria and events.
12. Coordinate Effect Request Form (ERF) development, submittal, and execution.
13. Integrate with DODIN operations.
14. Provide recommendations for changes to configuration baseline.
15. Coordinate support for DCO-RA.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations

8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1702-OCO-2001: Direct offensive cyberspace operations

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

MOS PERFORMING: 1702, 1710

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5, CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Organize, facilitate, and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Validate mission analysis.
3. Task organize.
4. Issue warning order.
5. Deconflict operations.
6. Assess MOP.
7. Assess MOE.
8. Validate post-mission analysis.
9. Disseminate mission results.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CYBER T&R MANUAL

CHAPTER 5

MOS 1705 INDIVIDUAL EVENTS

CHAPTER 5

MOS 1705 INDIVIDUAL EVENTS

5000. PURPOSE. This chapter details the individual events that pertain to Cyberspace Limited Duty Officers. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

5001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1705	Cyberspace Limited Duty Officer

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
CYBR	Cyberspace

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
2000	Core Plus Skills

5002. INDEX OF EVENTS

Event Code	Event
2000 Level Events	
1705-CYBR-2001	Perform capabilities development
1705-CYBR-2002	Perform cyberspace capability evaluation

5003. EVENTS

1705-CYBR-2001: Perform capabilities development

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

MOS PERFORMING: 1705

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Design, develop, test, and evaluate tools and capabilities required to conduct cyberspace operations throughout the systems development life cycle.

PERFORMANCE STEPS:

1. Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
2. Manage the building, testing, and modification of capability prototypes.
3. Direct system testing and validation procedures and documentation.
4. Manage the development of capability components.
5. Direct the remediation of technical problems encountered during testing and implementation of new systems.
6. Provide guidelines for integrating systems.
7. Provide input to the Risk Management Framework process activities and related documentation.
8. Manage design and development documentation.
9. Develop mitigation strategies to address cost, schedule, performance, and security risks.
10. Provide support to test and evaluation activities.
11. Trace capability requirements to design components and perform gap analysis.
12. Verify stability, interoperability, portability, and/or scalability of capability.

REFERENCES:

1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
10. TAO Tradecraft Guidelines
11. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1705-CYBR-2002: Perform cyberspace capability evaluation

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

MOS PERFORMING: 1705

GRADES: CAPT, MAJ, LTCOL

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Conduct engineering and technology research to test and evaluate current and potential cyberspace capabilities.

PERFORMANCE STEPS:

1. Research current technology.
2. Identify cyber capabilities strategies for custom hardware and software development.
3. Collaborate with stakeholders to identify and/or develop capabilities.
4. Recommend cyberspace capabilities for use within a system.
5. Troubleshooting prototype designs and process issues.
6. Oversee the identification and/or development of reverse engineering capabilities.

REFERENCES:

1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
10. TAO Tradecraft Guidelines
11. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CYBER T&R MANUAL

CHAPTER 6

MOS 1710 INDIVIDUAL EVENTS

CHAPTER 6

MOS 1710 INDIVIDUAL EVENTS

6000. PURPOSE. This chapter details the individual events that pertain to Cyberspace Warrant Officers. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

6001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1710	Cyberspace Warrant Officer

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
CYBR	Cyberspace

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
2000	Core Plus Skills

6002. INDEX OF EVENTS

Event Code	Event
2000 Level Events	
1710-CYBR-2001	Advise the unit leader on weapons employment

6003. EVENTS

1710-CYBR-2001: Advise the unit leader on weapons employment

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

MOS PERFORMING: 1710

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Facilitate and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:

1. Advise the development and integration of cyberspace concepts, capabilities, tools, and effects.
2. Advise in the weaponeering of cyberspace capabilities.
3. Advise on tactical and operational missions impact to strategic objectives.
4. Advise on planning and execution of cyberspace operations.
5. Manage the conduct cyber threat emulation, on-net operations, and exploitation analysis.
6. Advise on the effects, capabilities, TTPs in cyberspace operations.

REFERENCES:

1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CYBER T&R MANUAL

CHAPTER 7

MOS 1711 INDIVIDUAL EVENTS

CHAPTER 7

MOS 1711 INDIVIDUAL EVENTS

7000. PURPOSE. This chapter details the individual events that pertain to Offensive Cyberspace Marines. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

7001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1711	Offensive Cyberspace Marine

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
OCO	Offensive cyberspace operations
OPS	Operations

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
2000	Core Plus Skills

7002. INDEX OF EVENTS

Event Code	Event
2000 Level Events	
1711-OCO-2001	Conduct exploitation analysis
1711-OCO-2002	Conduct offensive cyberspace operations
1711-OPS-2001	Conduct target research
1711-OPS-2002	Conduct cyber threat emulation
1711-OPS-2003	Conduct malware analysis
1711-OPS-2004	Conduct capability analysis

7003. EVENTS

1711-OCO-2001: Conduct exploitation analysis

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Conduct analysis driven by operational and intelligence products.
3. Apply legal considerations.
4. Apply technical considerations.
5. Identify operational constraints.
6. Identify environmental constraints.
7. Review and assess intelligence Gain/loss.
8. Develop operational plan.
9. Deconflict operations.
10. Execute operations plan.
11. Conduct post-mission analysis.
12. Disseminate mission results.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CHAINED EVENTS:

PREREQUISITE EVENTS:
2611-INTL-2001 2611-INTL-2002

1711-OCO-2002: Conduct offensive cyberspace operations

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Conduct analysis driven by OSINT and intelligence databases.
3. Apply legal considerations.
4. Apply technical considerations.
5. Identify operational constraints.
6. Identify environmental constraints.
7. Deconflict operations.
8. Classified. See USCC CMF T&R Manual version 3.1.
9. Employ equipment.
10. Classified. See USCC CMF T&R Manual version 3.1.
11. Conduct post-mission analysis.
12. Disseminate mission results.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CHAINED EVENTS:

PREREQUISITE EVENTS:
2611-INTL-2004 2611-INTL-2005

1711-OPS-2001: Conduct target research

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Review tasking.
2. Conduct research utilizing available data sources.
3. Integrate data.
4. Conduct traffic analysis.
5. Identify targets.
6. Identify applicable capabilities.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1711-OPS-2002: Conduct cyber threat emulation

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Review tasking.
2. Conduct research on threat actors.
3. Determine desired adversarial TTP.
4. Conduct traffic analysis.
5. Identify targets.
6. Identify applicable capabilities.

7. Execute adversarial TTPs.
8. Report actions.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1711-OPS-2003: Conduct malware analysis

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Obtain malware.
2. Build virtual environment for testing.
3. Determine assembly code level instruction.
4. Establish snapshot of test environment.
5. Running malware in test environment.
6. Take second snapshot of test environment.
7. Determine changes.
8. Report actions.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

1711-OPS-2004: Conduct capability analysis

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

MOS PERFORMING: 1711

GRADES: SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Execute offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Obtain capability.
2. Build virtual environment for testing.
3. Configure target systems.
4. Establish snapshot of test environment.
5. Running capability in test environment.
6. Take second snapshot of test environment.
7. Determine changes.
8. Report actions.

REFERENCES:
1. DoDD 8140.01 Cyberspace Workforce Management
2. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
3. JP 3-12(R) Cyberspace Operations
4. JP 3-13R Cyberspace Operations
5. MCO 3100.4 Cyberspace Operations
6. NWP 3-12 CYBERSPACE OPERATIONS
7. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON
8. TAO Tradecraft Guidelines
9. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CYBER T&R MANUAL

CHAPTER 8

MOS 1720 INDIVIDUAL EVENTS

CYBER T&R MANUAL

CHAPTER 8

MOS 1720 INDIVIDUAL EVENTS

8000. PURPOSE. This chapter details the individual events that pertain to Cyberspace Defensive Warrant Officers. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

8001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1720	Cyberspace Defensive Warrant Officer

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
CYBR	Cyberspace

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
2000	Core Plus Skills

8002. INDEX OF EVENTS

Event Code	Event
2000 Level Events	
1720-CYBR-2001	Advise the unit leader on capabilities employment

8003. EVENTS

1720-CYBR-2001: Advise the unit leader on capabilities employment

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

MOS PERFORMING: 1710, 1720

GRADES: WO-1, CWO-2, CWO-3, CWO-4, CWO-5

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Facilitate and deconflict offensive/defensive cyberspace operations.

PERFORMANCE STEPS:

1. Advise the development and integration of defensive cyberspace concepts, capabilities, and effects.
2. Advise in the weaponeering of defensive cyberspace capabilities.
3. Advise on defensive tactical and operational missions impact to strategic objectives.
4. Advise on planning and execution of defensive cyberspace operations.
5. Advise on the collection, analysis, development of targets, conducting cyberspace surveillance, and crafting exploitation and intrusion countermeasures.
6. Advise on the effects, capabilities, TTPs in cyberspace operations.

REFERENCES:

1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

CYBER T&R MANUAL

CHAPTER 9

MOS 1721 INDIVIDUAL EVENTS

CYBER T&R MANUAL

CHAPTER 9

MOS 1721 INDIVIDUAL EVENTS

9000. PURPOSE. This chapter details the individual events that pertain to Defensive Cyberspace Operators. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

9001. EVENT CODING. Events in this T&R manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1721	Defensive Cyberspace Operators

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
DCO	Defensive Cyberspace Operations

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
1000	Core Skills
2000	Core Plus Skills

9002. INDEX OF EVENTS

Event Code	Event
1000 Level Events	
1721-DCO-1001	Conduct defensive cyberspace operations
1721-DCO-1002	Conduct defensive cyberspace operations analysis
1721-DCO-1003	Conduct program language review
1721-DCO-1004	Conduct forensic analysis
1721-DCO-1005	Conduct system research
2000 Level Events	
1721-DCO-2001	Manage a defensive cyberspace operations element
1721-DCO-2002	Identify potential compromise
1721-DCO-2003	Analyze the system architecture
1721-DCO-2004	Identify anomalous network behavior
1721-DCO-2005	Conduct risk analysis

9003. EVENTS

1721-DCO-1001: Conduct defensive cyberspace operations

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

MOS PERFORMING: 1721

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given authorities, references, certifications, mission tasking, currently-fielded equipment, a target environment, and a spectrum survey

STANDARD: To satisfy mission requirements within a time limit established by the commander.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Conduct analysis driven by operational and intelligence products.
3. Correlate incident data.
4. Perform analysis of log files.
5. Perform cyber defense incident triage.
6. Perform cyber defense trend analysis and reporting.
7. Collect and inspect system images.
8. Perform real-time cyber defense incident handling.
9. Analyze network alerts.
10. Document cyber defense techniques, guidance, and reports.
11. Employ approved defense-in-depth principles and practices.
12. Collect intrusion artifacts.
13. Correlate threat data.
14. Write and publish after action reviews.
15. Perform incident response functions.
16. Ensure proper handling of sensitive incident material.
17. Coordinate with intelligence analysts to correlate threat assessment data.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1721-DCO-1002: Conduct defensive cyberspace operations analysis

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

MOS PERFORMING: 1721

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given authorities, references, certifications, mission tasking, currently-fielded equipment, a target environment, and a spectrum survey.

STANDARD: To satisfy mission requirements within a time limit established by the commander.

PERFORMANCE STEPS:
1. Conduct analysis driven by operational intelligence products.
2. Determine collection methods and exploitation tactics, techniques, and procedures. (TTPs) for physical and mobile/wireless networks.
3. Identify network and security protocols, configurations, and risks.
4. Examine network topologies.
5. Assess computer and network vulnerabilities.
6. Identify and analyze anomalies.
7. Identify malicious intent.
8. Analyze network traffic.
9. Reconstruct a malicious activity.
10. Identify network mapping and operating system (OS) fingerprinting activities.
11. Assist in the construction of signatures.
12. Report suspected anomalous behavior.
13. Assess effectiveness of security controls.
14. Provide operational defense recommendations.
15. Provide input for Disaster Recovery, Contingency, and Continuity of Operations Plans.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling
3. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
4. JP 3-12(R) Cyberspace Operations
5. JP 3-13R Cyberspace Operations
6. MCO 3100.4 Cyberspace Operations
7. NWP 3-12 CYBERSPACE OPERATIONS
8. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1721-DCO-1003: Conduct program language review

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

MOS PERFORMING: 1721

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given an understanding of programming fundamentals, basic logic and memory concepts, and mission tasking.

STANDARD: To assess potential flaws in code.

PERFORMANCE STEPS:
1. Develop logic diagram.
2. Identify different language tiers and types of programing languages.
3. Identify and use program structural components.
4. Identify classes and objects in programming.
5. Analyze, create, and compile programs.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling
3. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
4. JP 3-12(R) Cyberspace Operations
5. JP 3-13R Cyberspace Operations
6. MCO 3100.4 Cyberspace Operations
7. NWP 3-12 CYBERSPACE OPERATIONS
8. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1721-DCO-1004: Conduct forensic analysis

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

MOS PERFORMING: 1721

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given authorities, references, required certifications, mission tasking, currently-fielded equipment, a target environment, malicious software, and forensic malware analysis capabilities.

STANDARD: Identify the objectives of malware authors, determine compromised data during an incident, and develop countermeasures to prevent future incidents utilizing the digital forensics methodology.

PERFORMANCE STEPS:
1. Understand digital forensic fundamentals.
2. Coordinate with partner digital forensic organizations.
3. Perform digital media identification.
4. Conduct digital media imaging.
5. Conduct metadata analysis.
6. Conduct malware analysis.
7. Perform digital forensics.

8. Identify and counter code obfuscation techniques.
9. Complete a forensics investigation.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling
3. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
4. JP 3-12(R) Cyberspace Operations
5. JP 3-13R Cyberspace Operations
6. MCO 3100.4 Cyberspace Operations
7. NWP 3-12 CYBERSPACE OPERATIONS
8. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1721-DCO-1005: Conduct system research

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

MOS PERFORMING: 1721

GRADES: PVT, PFC, LCPL, CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: FORMAL

CONDITION: Given authorities, references, required certifications, mission tasking, currently-fielded equipment, and a target environment.

STANDARD: To satisfy mission requirements within a time limit established by the commander.

PERFORMANCE STEPS:
1. Review tasking.
2. Conduct research utilizing available data sources.
3. Integrate data.
4. Conduct traffic analysis.
5. Identify targets.
6. Identify applicable capabilities.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. DoDD 8140.01 Cyberspace Workforce Management
3. ECSD 001 Computer Security Incident Handling
4. FM 3-12 CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS
5. JP 3-12(R) Cyberspace Operations
6. JP 3-13R Cyberspace Operations
7. MCO 3100.4 Cyberspace Operations
8. NWP 3-12 CYBERSPACE OPERATIONS
9. SECNAVINST 3052.2_ Cyberspace Policy and Administration within the DON

1721-DCO-2001: Manage a defensive cyberspace operations element

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

MOS PERFORMING: 1721

GRADES: SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Supervise mission analysis.
2. Identify support requirements.
3. Conduct tactical planning.
4. Conduct mission assessment.
5. Conduct risk management framework analysis.
6. Coordinate with higher, adjacent, and supported agencies.
7. Supervise team execution.
8. Document team execution.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

1721-DCO-2002: Identify potential compromise

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

MOS PERFORMING: 1721

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Conduct operational analysis.

2. Deploy sensors.
3. Correlate enumerated host and network data.
4. Determine initial entry.
5. Identify privileged escalation.
6. Identify data mining.
7. Identify removal of evidence.
8. Conduct vulnerability and configuration analysis.
9. Generate report of findings.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

1721-DCO-2003: Analyze the system architecture

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

MOS PERFORMING: 1721

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Conduct analysis driven by operational and intelligence products.
2. Conduct interviews of stakeholders.
3. Build dependency model.
4. Conduct vulnerability analysis.
5. Conduct configuration analysis.
6. Identify undocumented/rogue systems.
7. Conduct forensics analysis.
8. Conduct Active Directory analysis.
9. Conduct network architecture analysis.
10. Coordinate actions with DODIN operations.
11. Conduct compliance review.
12. Generate report of findings.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

1721-DCO-2004: Identify anomalous network behavior

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

MOS PERFORMING: 1721

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Conduct analysis driven by operational and intelligence products.
2. Evaluate baseline network behavior.
3. Conduct network intrusion analysis.
4. Conduct network architecture analysis.
5. Conduct wireless architecture analysis.
6. Conduct VTC architecture analysis.
7. Generate report of findings.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

1721-DCO-2005: Conduct risk analysis

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

MOS PERFORMING: 1721

GRADES: CPL, SGT, SSGT, GYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Conduct analysis driven by operational and intelligence products.
2. Conduct vulnerability analysis.

3. Conduct configuration analysis.
4. Conduct network architecture analysis.
5. Conduct intrusion detection analysis.
6. Evaluate cyber defense controls.
7. Conduct system analysis.
8. Generate report of findings.

REFERENCES:

1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

CYBER T&R MANUAL

CHAPTER 10

MOS 1799 INDIVIDUAL EVENTS

CYBER T&R MANUAL

CHAPTER 10

MOS 1799 INDIVIDUAL EVENTS

10000. PURPOSE. This chapter details the individual events that pertain to Cyberspace Operations Chief. Each individual event provides an event title, along with the conditions events will be performed under, and the standard to which the event must be performed to be successful.

10001. EVENT CODING. Events in this T&R Manual are depicted with an up to 12-digit, 3-field alphanumeric system (i.e., XXXX-XXXX-XXXX). This chapter utilizes the following methodology:

a. Field one. This field represents the MOS. This chapter contains the following MOS codes:

Code	Description
1799	Cyberspace Operations Chief

b. Field two. This field represents the functional/duty area. This chapter contains the following functional/duty areas:

Code	Description
CYBR	Cyberspace
DCO	Defensive cyberspace operations
OCO	Offensive cyberspace operations

c. Field three. This field provides the level at which the event is accomplished and numerical sequencing of events. This chapter contains the following event levels:

Code	Description
2000	Core Plus Skills

10002. INDEX OF EVENTS

Event Code	Event
2000 Level Events	
1799-CYBR-2001	Integrate cyberspace operations
1799-DCO-2002	Supervise defensive cyberspace operations
1799-OCO-2001	Supervise offensive cyberspace operations

10003. EVENTS

1799-CYBR-2001: Integrate cyberspace operations

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

MOS PERFORMING: 1799

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Enable the ability to exercise authority and direction over assigned or attached forces in the accomplishment of the mission.

PERFORMANCE STEPS:
1. Review operations plan.
2. Advise execution of cyberspace techniques, tactics, and procedures.
3. Coordinate with external agencies.
4. Coordinate with higher/adjacent units.
5. Provide recommendations to development of intelligence requirements.
6. Generate intelligence requests for information.
7. Advise on CO capabilities.
8. Report findings.
9. Coordinate the approval of CO.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling
3. TAO Tradecraft Guidelines
4. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

---

1799-DCO-2002: Supervise defensive cyberspace operations

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

MOS PERFORMING: 1799

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Enable the ability to preserve the ability to utilize friendly cyberspace capabilities, protect data, networks, net-centric capabilities, and other designated systems.

PERFORMANCE STEPS:
1. Review mission tasking
2. Verify key terrain in cyberspace.

3. Validate risk mitigation plan.
4. Validate mission defense plan.
5. Validate asset identification plan.
6. Validate event audit plan.
7. Validate monitoring plan.
8. Validate strategies to prevent and mitigate intrusion.
9. Report mitigation effectiveness.
10. Participate in change management board.
11. Advise commander on escalation criteria and events.
12. Coordinate Effect Request Form (ERF) development, submittal, and execution.
13. Integrate with DODIN operations.
14. Coordinate intelligence oversight.
15. Coordinate cyberspace surveillance and reconnaissance oversight.
16. Provide recommendations for changes to configuration baseline.
17. Validate post-mission analysis.
18. Disseminate mission results.

REFERENCES:
1. CJCSM 6510.01_ Computer Network Defense (CND) Volume I (Incident Handling Program)
2. ECSD 001 Computer Security Incident Handling

1799-OCO-2001: Supervise offensive cyberspace operations

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

MOS PERFORMING: 1799

GRADES: MSGT, MGYSGT

INITIAL TRAINING SETTING: MOJT

CONDITION: In a designated environment given references, all necessary authorities, network accesses, and commanders(s) guidance. Using software, hardware, and personnel as necessary.

STANDARD: Enable the execution of offensive cyberspace actions that create various direct denial effects (i.e., degrade, disruption, or destruction) and manipulation.

PERFORMANCE STEPS:
1. Review mission tasking.
2. Validate mission analysis.
3. Task organize.
4. Execute warning order.
5. Coordinate intelligence oversight.
6. Coordinate cyberspace surveillance and reconnaissance oversight.
7. De-conflict operations.
8. Supervise use of available data sources.
9. Assess MOP.
10. Assess MOE.
11. Validate post-mission analysis.

12. Disseminate mission results.

REFERENCES:

1. TAO Tradecraft Guidelines
2. Title 10 USC-Cyberspace Mission Profile and Operational Plan Approval Process

CYBER T&R MANUAL

APPENDIX A

ACRONYMS

AAV - amphibious assault vehicle
ACP - automated commissioning package
ACT - accuracy completeness time sequence
ACTS - Assignment, Classification, and Travel Systems
AIRS - Automated Inspection Reporting System
AO - area of operations
APTS - advanced presentation and training skills
AR - Active Reserve
ASTB-E - Aviation Selection Test Battery Series-E
AT4C - advanced tool for coaching
BIC - billet information code
CAPT - Captain
CAR - commander's attainment report
CBRN - chemical, biological, radiological, and nuclear
CBT - computer-based training
CG - commanding general
CMC - Commandant of the Marine Corps
CMR - consolidated memorandum receipt
CO - commanding officer
COA - course of action
CONPLAN - contingency plan
CONUS - continental United States
COT - consecutive overseas tours
CPL - Corporal
CRP - combat readiness percentage; command recruiting program
CSR - consolidated strength report
CWO - chief warrant officer
DEP - delayed entry program
DL - distance learning
DOD - Department of Defense
DoDFMR - Department of Defense Financial Management Regulation
DON - Department of the Navy
DRRS - Defense Readiness Reporting System
EAD - extended active duty
ECFC - enlisted career force controls
ECS - effective communication skills
EFMP - Exceptional Family Member Program
ENLPROM - enlisted promotions
EPM - enlistment processing manual
1STLT - First Lieutenant
FAI - functional area inspection
FLC - formal learning center
FMF - fleet Marine force
FY - fiscal year
GOV - government owned vehicle
GSA - Government Services Administration
GYSGT - Gunnery Sergeant
HOTAS - hands-on throttle and stick
HQMC - Headquarters, Marine Corps
IAW - in accordance with

IGMC - Inspector General of the Marine Corps
IIADT - incremental initial active duty training
IMI - individual multimedia instruction
IPOCT - in place consecutive overseas tours
IRAM - Individual Records Administration Manual
IRR - Individual Ready Reserve
IRT - Itinerant Recruiting Trip
JPIC - Joint Package Inspection Checklist
LATMOV - lateral move
LCPL - Lance Corporal
LDO - limited duty officer; line of duty
LOI - letter of instruction
LSL - lump sum leave
MAJ - Major
MARADMIN - Marine Administrative Message
MARCORPROMMAN - Marine Corps Promotion Manual
MARCORSEPMAN - Marine Corps Separation and Retirement Manual
MARFORRES - Marine Corps Forces Reserve
MASP - military academic skills program
MC2 - Marine Corps Communication and Consulting
MC3 - Marine Corps Communication, Coaching, and Counseling
MC4 - Marine Corps Communication, Consulting, Coaching, and Counseling
MCC - monitored command code
MCEOB - Marine Corps Enlisted Opportunities Book
MCI - Marine Corps Institute
MCMEDS - Marine Corps Medical Entitlements Data System
MCMP - Marine Corps mentoring program
MCO - Marine Corps order
MCOOB - Marine Corps Officer Opportunity Book
MCP3 - Marine Corps Performance, Programming and Philosophy
MCPS - Marine Corps Presentation Skills
MCRAMM - Marine Corps Reserve Administrative Management Manual
MCRC - Marine Corps Recruiting Command
MCRD - Marine Corps Recruit Depot
MCRISS - Marine Corps Recruiting Information Support System
MCRISS-OSS - Marine Corps Recruiting Information Support System-Officer Selection Station
MCRISS-PSRS - Marine Corps Recruiting Information Support System-Prior Service Recruiting Station
MCRISS-PSRSS - Marine Corps Recruiting Information Support System-Prior Service Recruiting Substation
MCRISS-RS - Marine Corps Recruiting Information Support System-Recruiting Station
MCROB - Marine Corps Reserve Opportunity Book
MCT - Marine Corps Task
MCTFSPRIM - Marine Corps Total Force Reporting Instructions Manual
MCTIMS - Marine Corps Training Information Management System
MCTL - Marine Corps Task List
MECEP - Marine Corps Enlisted Commissioning Education Program
MEPCOM - Military Entrance Processing Command
MEPS - Military Entrance Processing Station
MET - mission essential task
METL - mission essential task list
MGIB-R - Montgomery GI Bill-Reserve
MGYSGT - Master Gunnery Sergeant
MIRS - USMEPCOM Integrated Resource System
MISSO - Manpower Information Systems Support Officer

MOJT - Marine on-the-job training
MOL - Marine online
MOS - military occupational specialty
MSC - major subordinate command
MSGT - Master Sergeant
MUD - Merkel Unit Designator
NAMI - Naval Aerial Medical Institute
NAVMC - Navy Marine Corps
NIDT - Non-Instrumented Drug Test
NMCI - Navy Marine Corps Communication Information
NWA - new working applicant
OCHF - Operations Chief
OCM - Officer Commissioning Manual
OCONUS - outside the continental United States
OIC - officer in charge
OPFOR - operating forces; opposing force; opposition force
OPLAN - operational plan
OPNAV - Office of the Chief of Naval Operations
OPNAVINST Chief of Naval Operations instruction
OPS - operations
OPSO - operations officer
ORM - operational risk management
OSO - officer selection officer
OSS - officer selection station
OST - officer selection team
PAC - prospect applicant card
PADD - projected active duty date
PAR - Performance and Review
PFC - Private First Class
PSEP - prior service enlistment program
PSF - public speaking forum
PSR - prior service recruiter
PSRS - prior service recruiting station
PSRSS - prior service recruiting substation
PTAD - permissive temporary additional duty
PVT - Private
QC - quality control
QCIS - quality control SITREP
QSN - quota serial number
RAV - Retention Assist Visit
RECLP - Reserve Enlisted Commissioning Program
RELM - Reenlistment Extension Lateral Move
RI - Recruiter Instructor
ROEP - Reserve Option Enlistment Program
RS - Recruiting Station
RSCE - Recruiting Station Command Element
RSS - Recruiting Substation
RTF - recruiter training file
RUC - reporting unit code
S&R - Schedule and Results
SAT - Systems Approach to Training
SAV - staff assist visit
SDA - special duty assignment
SECNAVINST - Secretary of the Navy instruction
SGT - Sergeant
SGTMAJ - Sergeant Major
SITREP situation report

SMB - SNCOIC Management Book
SMCR - select Marine Corps reserve
SME - subject matter expert
SMOS - supplementary MOS
SNCO - staff noncommissioned officer
SNCOIC - staff noncommissioned officer in charge
SOP - standing operating procedure
SOS - statement of service
SOU - statement of understanding
SRB - selective reenlistment bonus
SRI - Systematic Recruiting Inspection
SRIP - Selected Reserve Incentive Program
SSGT - Staff Sergeant
T&R - training and readiness
T/O - table of organization
TECOM - Training and Education Command
TIP - training input plan
TMS - Training Management System
UMIS - Unit Manpower Information Sheet
UTM - unit training management
WO - Warrant Officer
XO - executive officer

CYBER 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 Publication 1-02, DOD Dictionary of Military and Associated Terms.

A

After Action Review. 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.

Assessment. An informal judgment of the unit's proficiency and resources made by a commander or trainer to gain insight into the unit's overall condition. It serves as the basis for the midrange plan. Commanders make frequent use of these determinations during the course of the combat readiness cycle in order to adjust, prioritize or modify training events and plans.

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. 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.

Collective Event. A clearly defined, discrete, and measurable activity, action, or event (i.e., task) that requires organized team or unit performance and leads to accomplishment of a mission or function. A collective task is derived from unit missions or higher-level collective tasks. Task accomplishment requires performance of procedures composed of supporting collective or individual tasks. A collective task describes the exact performance a group must perform in the field under actual operational conditions. The term "collective" does not necessarily infer that a unit accomplishes the event. A unit, such as a squad or platoon conducting an attack; may accomplish a collective event or, it may be accomplished by an individual to accomplish a unit mission, such as a battalion supply officer completing a reconciliation of the battalion's CMR. Thus, many collective events will have titles that are the same as individual events; however, the standard and condition will be different because the scope of the collective event is broader.

Collective Training Standards (CTS). Criteria that specify mission and functional area unit proficiency standards for combat, combat support, and combat service support units. They include tasks, conditions, standards, evaluator instruction, and key indicators. CTS are found within collective training events in T&R Manuals.

Combat Readiness Cycle. The combat readiness cycle depicts the relationships within the building block approach to training. The combat readiness cycle progresses from T&R Manual individual core skills training, to the accomplishment of collective training events, and finally, to a unit's participation in a contingency or actual combat. The combat readiness cycle demonstrates the relationship of core capabilities to unit combat readiness. Individual core skills training and the training of collective events lead to unit proficiency and the ability to accomplish the unit's stated mission.

Combat Readiness Percentage (CRP). The CRP is a quantitative numerical value used in calculating collective training readiness based on the E-Coded events that support the unit METL. CRP is a concise measure of unit training accomplishments. This numerical value is only a snapshot of training readiness at a specific time. As training is conducted, unit CRP will continuously change.

Condition. The condition describes the training situation or environment under which the training event or task will take place. Expands on the information in the title by identifying when, where and why the event or task will occur and what materials, personnel, equipment, environmental provisions, and safety constraints must be present to perform the event or task in a real-world environment. Commanders can modify the conditions of the event to best prepare their Marines to accomplish the assigned mission (e.g. in a desert environment; in a mountain environment; etc.).

Core Competency. Core competency is the comprehensive measure of a unit's ability to accomplish its assigned MET. It serves as the foundation of the T&R Program. Core competencies are those unit core capabilities and individual core skills that support the commander's METL and T/O mission statement. Individual competency is exhibited through demonstration of proficiency in specified core tasks and core plus tasks. Unit proficiency is measured through collective tasks.

Core Capabilities. Core capabilities are the essential functions a unit must be capable of performing during extended contingency/combat operations. Core unit capabilities are based upon mission essential tasks derived from operational plans; doctrine and established tactics; techniques and procedures.

Core Plus Capabilities. Core plus capabilities are advanced capabilities that are environment, mission, or theater specific. Core plus capabilities may entail high-risk, high-cost training for missions that are less likely to be assigned in combat.

Core Plus Skills. Core plus skills are those advanced skills that are environment, mission, rank, or billet specific. 2000-Level training is designed to make Marines proficient in core skills in a specific billet or at a specified rank at the Combat Ready level. 3000-8000-Level training produces combat leaders and fully qualified section members at the Combat Qualified level. Marines trained at the Combat Qualified level are those the

commanding officer feels are capable of accomplishing unit-level missions and of directing the actions of subordinates. Many core plus tasks are learned via MOJT, while others form the base for curriculum in career level MOS courses taught by the formal school.

D

Defense Readiness Reporting System (DRRS). A comprehensive readiness reporting system that evaluates readiness on the basis of the actual missions and capabilities assigned to the forces. It is a capabilities-based, adaptive, near real-time reporting system for the entire Department of Defense.

Deferred Event. A T&R event that a commanding officer may postpone when in his or her judgment, a lack of logistic support, ammo, ranges, or other training assets requires a temporary exemption. CRP cannot be accrued for deferred "E-Coded" events.

Delinquent Event. An event becomes delinquent when a unit exceeds the sustainment interval for that particular event. The individual or unit must update the delinquent event by first performing all prerequisite events. When the unit commander deems that performing all prerequisite is unattainable, then the delinquent event will be re-demonstrated under the supervision of the appropriate evaluation authority.

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.

Evaluation. Evaluation is a continuous process that occurs at all echelons, during every phase of training and can be both formal and informal. Evaluations ensure that Marines and units are capable of conducting their combat mission. Evaluation results are used to reallocate resources, reprioritize the training plan, and plan for future training.

Event (Training). 1) An event is a significant training occurrence that is identified, expanded and used as a building block and potential milestone for a unit's training. An event may include formal evaluations. 2) An event within the T&R Program can be an individual training evolution, a collective training evolution or both. Through T&R events, the unit commander ensures that individual Marines and the unit progress from a combat capable status to a Fully Combat Qualified (FCQ) status.

Event Component. The major procedures (i.e., actions) that must occur to perform a Collective Event to standard.

Exercise Commander (EC). The Commanding General, Marine Expeditionary Force or his appointee will fill this role, unless authority is delegated to the respective commander of the Division, Wing, or FSSG. Responsibilities and functions of the EC include: 1) designate unit(s) to be evaluated, 2) may designate an exercise director, 3) prescribe exercise objectives and T&R events to be evaluated, 4) coordinate with commands or agencies external to the Marine Corps and adjacent Marine Corps commands, when required.

Exercise Director (ED). Designated by the EC to prepare, conduct, and report all evaluation results. Responsibilities and functions of the ED include: 1) Publish a letter of instruction (LOI) that: delineates the T&R events to be evaluated, establishes timeframe of the exercise, lists responsibilities of various elements participating in the exercise, establishes safety requirements/guidelines, and lists coordinating instructions. 2) Designate the TEC and TECG to operate as the central control agency for the exercise. 3) Assign evaluators, to include the senior evaluator, and ensure that those evaluators are properly trained. 4) Develop the general exercise scenario taking into account any objectives/events prescribed by the EC. 5) Arrange for all resources to include: training areas, airspace, aggressor forces, and other required support.

M

Marine Corps Ground Training and Readiness (T&R) Program. The T&R Program is the Marine Corps' primary tool for planning and conducting training, for planning and conducting training evaluation, and for assessing training readiness. The program will provide the commander with standardized programs of instruction for units within the ground combat, combat support, and combat service support communities. It consolidates the ITS, CTS, METL and other individual and unit training management tools. T&R is a program of standards that systematizes commonly accepted skills, is open to innovative change, and above all, tailors the training effort to the unit's mission. Further, T&R serves as a training guide and provides commanders an immediate assessment of unit combat readiness by assigning a CRP to key training events. In short, the T&R Program is a building block approach to training that maximizes flexibility and produces the best-trained Marines possible.

Mission Essential Task(s) MET(s). A MET is a collective task in which an organization must be proficient in order to accomplish an appropriate portion of its wartime mission(s). MET listings are the foundation for the T&R Manual; all events in the T&R Manual support a MET.

Mission Essential Task List (METL). Descriptive training document that provides units a clear, war fighting focused description of collective actions necessary to achieve wartime mission proficiency. The service-level METL, that which is used as the foundation of the T&R Manual, is developed using Marine Corps doctrine, operational plans, T/Os, UJTL, UNTL, and MCTL. For community based T&R Manuals, an occupational field METL is developed to focus the community's collective training standards. Commanders develop their unit METL from the service-level METL, operational plans, contingency plans, and SOPs.

O

Operational Readiness (DOD, 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

Prerequisite Event. Prerequisites are the academic training and/or T&R events that must be completed prior to attempting the event.

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).

Simulation Training. Simulators provide the additional capability to develop and hone core and core plus skills. Accordingly, the development of simulator training events for appropriate T&R syllabi can help maintain valuable combat resources while reducing training time and cost. Therefore, in cases where simulator fidelity and capabilities are such that simulator training closely matches that of actual training events, T&R Manual developers may include the option of using simulators to accomplish the training. CRP credit will be earned for E-Coded simulator events based on assessment of relative training event performance.

Standard. A standard is a statement that establishes criteria for how well a task or learning objective must be performed. The standard specifies how well, completely, or accurately a process must be performed or product produced. For higher-level collective events, it describes why the event is being done and the desired end-state of the event. Standards become more specific for lower-level events and outline the accuracy, time limits, sequencing, quality, product, process, restrictions, etc., that indicate the minimum acceptable level of performance required of the event. At a minimum, both collective and individual training standards consist of a task, the condition under which the task is to be performed, and the evaluation criteria that will be used to verify that the task has been performed to a satisfactory level.

Sustainment Training. Periodic retraining or demonstration of an event required maintaining the minimum acceptable level of proficiency or capability required to accomplish a training objective. Sustainment training goes beyond the entry-level and is designed to maintain or further develop proficiency in a given set of skills.

Systems Approach to Training (SAT). An orderly process for analyzing, designing, developing, implementing, and evaluating a unit's training program to ensure the unit, and the Marines of that unit acquire the knowledge and skills essential for the successful conduct of the unit's wartime missions.

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.

Technical Exercise Controller (TEC). The TEC is appointed by the ED, and usually comes from his staff or a subordinate command. The TEC is the senior evaluator within the TECG and should be of equal or higher grade than the commander(s) of the unit(s) being evaluated. The TEC is responsible for ensuring that the evaluation is conducted following the instructions contained in this order and MCO 1553.3A. Specific T&R Manuals are used as the source for evaluation criteria.

Tactical Exercise Control Group (TECG). A TECG is formed to provide subject matter experts in the functional areas being evaluated. The benefit of establishing a permanent TECG is to have resident, dedicated evaluation authority experience, and knowledgeable in evaluation technique. The responsibilities and functions of the TECG include: 1) developing a detailed exercise scenario to include the objectives and events prescribed by the EC/ED in the exercise LOI; 2) conducting detailed evaluator training prior to the exercise; 3) coordinating and controlling role players and aggressors; 4) compiling the evaluation data submitted by the evaluators and submitting required results to the ED; 5) preparing and conducting a detailed exercise debrief for the evaluated unit(s).

Training Plan. Training document that outlines the general plan for the conduct of individual and collective training in an organization for specified periods of time.

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.

Unit Evaluation. All units in the Marine Corps must be evaluated, either formally or informally, to ensure they are capable of conducting their combat mission. Informal evaluations should take place during all training events. The timing of formal evaluations is critical and should, when appropriate, be directly related to the units' operational deployment cycle. Formal evaluations should take place after the unit has been staffed with the majority of its personnel, has had sufficient time to train to individual and collective standards, and early enough in the training cycle so there is sufficient time to correctly identified weaknesses prior to deployment. All combat units and units' task organized for combat require formal evaluations prior to operational deployments.

Unit Training Management (UTM). Unit training management is the use of the SAT and Marine Corps training principles in a manner that maximizes training results and focuses the training priorities of the unit on its wartime mission. UTM governs the major peacetime training activity of the Marine Corps and applies to all echelons of the Total Force.

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.