T&R MANUAL ANNEX A

SERVICE-CYBER PROTECTION TEAMS (S-CPT) TRAINING & EVALUATION OUTLINE (T&EO) WORKSHEET

VERSION 4.0

3 MARCH 2025

United States Cyber Command (USCYBERCOM)

Controlled by: USCYBERCOM
Controlled by: J72
CUI Categories: OPSEC
Limited Dissem. Control: FEDCON
POC: USCYBERCOM/J72 USCC_J721@cybercom.ic.gov

1. (U) S-CPT T&EO Worksheet Guidance

1.1 (U) Functions

1.1.1 (CUI) Conduct intelligence-driven hunt operations on specified terrain; counter and clear adversary activity from specified terrain in coordination with the supported commander and mission partners; enable hardening of specified terrain in cyberspace from threat-specific unauthorized activities by reducing the attack surface of a system to increase the difficulty of system access and exploitation; assess the effectiveness of response actions, as well as current and future risk to specified terrain in cyberspace.

1.2 (U) Mission Statement

1.2.1 (U) Conduct Defensive Cyberspace Operations (DCO) Internal Defensive Measure missions to defend specified terrain, remove identified adversary tools, and/or presence on a defended network. Prepare local defenders to deploy advanced DCO Tactics, Techniques, and Procedures (TTP) that ensure the supported mission owner's freedom of action within friendly cyberspace while denying adversaries the same.

1.3 (U) Purpose

1.3.1 (U) This worksheet is used to evaluate S-CPTs during exercises or real-world operations. It includes the core tasks and associated subtasks that comprise the S-CPT Mission Essential Tasks (MET). The trainer or evaluator will enhance the subtasks with any Measures of Performance (MoP)/Measures of Effectiveness (MoE) to satisfy internal training or evaluation requirements.

1.4 (U) Supported METS

1.4.1 (U) ST 5.5.7 Direct Cyberspace Operations

1.4.2 (U) OP 2.3.5.2 Integrate Operational Intelligence

1.4.3 (U) ST 2.3 Manage Collected Information

1.4.4 (U) OP 5.6.5.3 Conduct Defensive Cyberspace Operations

1.5 (U) Task, Conditions, and Standards

1.5.1 (U) Task: In accordance with stated mission, execute operational orders and enduring guidelines.

1.5.2 (U) Conditions: In a training environment simulating operational conditions or real-world operations, given all necessary authorities, network access, and commander's guidance, the team will complete all core tasks associated with the mission. During an evaluation, teams must accomplish all assigned core tasks. All T&EO core tasks do not need to be completed in any specific order or in a single training event.

1.5.3 (U) Standards: Core tasks will be accomplished in accordance with team or higher headquarters standards, identified prior to initiation of training or evaluation.

1.6 (U) Evaluation Standards

1.6.1 (U) The evaluation standard is a tool for commanders to assess team performance against required tasks and subtasks. Commanders can use the evaluation to determine if a team can perform successfully in an operational environment. Commanders will use the T&EO and other factors determined by the operational chain of command to report the team's readiness status at red, yellow, or green. The final decision authority is the Joint Force Headquarters-Cyber (JFHQ-C), JFHQ-Department of Defense Information Network (DoDIN), or Cyber National Mission Force (CNMF) Commander. These evaluation standards (criteria, scale, terms, etc.) are to be used during the evaluation of Cyber Mission Force (CMF) teams during exercises or operations. Only operational tasks will be assessed during 3000-Level events/exercises.

1.6.2 (U) The evaluation standard to be used to assess Subtasks = Yes or No (Y/N) / Hours / Days / Operations (Ops):

1.6.2.1 (U) Yes: The Subtask is assessed as "Yes" if it is completed to standard as defined by the guidelines issued by the Higher Headquarters and determined by the evaluator.

1.6.2.2 (U) No: The Subtask is assessed as "No" if it is not completed to standard as defined by the guidelines issued by the Higher Headquarters and determined by the evaluator.

1.6.2.3 (U) Hours / Days / Operations (<=) is assessed as less than or equal to the number of hours, days, or operations determined by the evaluator to complete that task.

1.6.2.4 (U) Hours / Days / Operations (>=) is assessed as greater than or equal to the number of hours, days, or operations determined by the evaluator to complete that task.

1.6.2.5 (U) Final Report: The final evaluation report will indicate what subtasks were completed using the Go/No-Go assessment and a total in the core task block indicating how many subtasks were passed out of the total number of subtasks (i.e. Core task 2- 15/18).

1.7 (U) Team Information

1.7.1 (U) Team: _____ Date: _____

1.7.2 (U) Trainer/Evaluator Name: _____

2. (U) Supported METs

(U) The information in this section is S//REL USA, FVEY (when filled in).
Entered data must be S//REL USA, FVEY or below – PORTION MARK ALL DATA.

2.1 (U) ST 5.5.7 Direct Cyberspace Operations

Core Task 1: To receive and process orders		**Scoring Metrics** __/6			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Hours**	**Operator <=**	**Criterion 24**
Subtask 1: Conduct the Joint Planning Process using HHQ guidance to develop a tactical plan	LE, OPSO, PLNR	Critical			
Subtask 2: Identify supporting, supported, and adjacent units	TL, LE, ASO, PLNR	NC			
Subtask 3: Determine objective, scope, and end state	TL, LE, PLNR	Critical			
Subtask 4: Identify specified and implied tasks		NC			
Subtask 5: Identify end of mission / exit criteria		NC			
Subtask 6: Identify limitations, constraints, and restraints	LE, SE	NC			

Core Task 2: Conduct mission planning and analysis		Scoring Metrics /5			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Coordinate with customer and stakeholders to conduct pre-mission planning	LE, SE	Critical			
Subtask 2: Obtain network and host baseline documentation		NC			
Subtask 3: Identify the Mission Relevant Terrain and Key Terrain in cyberspace to develop prioritized specified terrain		NC			
Subtask 4: Identify the data collection requirements	PLNR, Master HA, Master NA	NC			
Subtask 5: Determine if split based operations are needed	LE, SE	NC			

Core Task 3: Direct execution of simultaneous Defensive Cyberspace Operations		Scoring Metrics /1			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Ops**	**Operator >=**	**Criterion 2**
Subtask 1: Coordinate and synchronize internal forces to meet mission objectives	TL, OPSO	Critical			

Core Task 4: Conduct mission reporting IAW OPCON governance		Scoring Metrics /2			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Develop and submit Daily SITREP	TL, LE, OPSO	NC			
Subtask 2: Develop and submit general reports requirements to meet mission objectives and commander's intent		NC			

2.2 (U) OP 2.3.5.2 Integrate Operational Intelligence

Core Task 1: To provide intelligence support to Defensive Cyberspace Operations planning		Scoring Metrics /4			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Days**	**Operator <=**	**Criterion 7**
Subtask 1: Identify intelligence required in support of mission	ME	NC			
Subtask 2: Submit intelligence need requests	ASA	NC			
Subtask 3: Provide intelligence-driven adversary attack chains pertinent to the terrain		NC			

Subtask 4: Identify the cyber-related risks to the supported mission	LE, SE	NC			

Core Task 2: To provide intelligence support to Defensive Cyberspace Operations in progress		**Scoring Metrics** __/3			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Disseminate real-time intelligence updates	ASA	Critical			
Subtask 2: Provide intelligence input into mission reporting, as needed		NC			
Subtask 3: Coordinate with external entities, as needed, to satisfy intelligence needs or requirements		NC			

Core Task 3: To provide intelligence support to critical information requests or requirements		**Scoring Metrics** __/1			
No Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Hours**	**Operator <=**	**Criterion 6**
N/A	ASA	NC			

2.3 (U) ST 2.3 Manage Collected Information

Core Task 1: Execute data handling and retention		**Scoring Metrics** __/1			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Handles and retains data IAW legal and agreed-upon guidance	ME, SE	NC			

Core Task 2: Develop analytic scheme of maneuver		**Scoring Metrics** __/2			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Determine adversary TTPs pertinent to the terrain based on the provided intelligence-driven attack chains	LE, SE	NC			
Subtask 2: Identify methods to detect adversary presence on the terrain	ME, SE	NC			

Core Task 3: Plan, coordinate, and execute data collection for, storage, analysis, and transfer to meet mission requirements		**Scoring Metrics** __/4			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Conducts in-band and/or out-of-band data ingestion as needed		NC			

Subtask 2: Determine data transfer requirements	HA, NA, DE, NT	NC			
Subtask 3: Create a sensor placement plan	SE, ME	NC			
Subtask 4: Configure the kit to the collection requirements	ME, DE, NT	NC			

96

97 ## 2.4 (U) OP 5.6.5.3 Conduct Defensive Cyberspace Operations

Core Task 1: To identify, characterize, and validate the area of operations		**Scoring Metrics** __/5			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Days**	**Operator <=**	**Criterion 7**
Subtask 1: Validate data input, data throughput, or access to ensure coverage of the operational environment	ME, DE, NT	Critical			
Subtask 2: Characterize and enumerate the area of operations to identify the operational environment	ME	NC			
Subtask 3: Validate specified cyber terrain against baseline	LE	NC			
Subtask 4: Validate security posture of MRT-C against expected documentation	ME	NC			
Subtask 5: Evaluate the security posture of the cyberspace terrain	ME, NT	NC			

98

Core Task 2: Find, fix, and track adversary presence on defended terrain		**Scoring Metrics** __/4			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Conduct actions to identify adversary presence within the terrain	HA, NA	Critical			
Subtask 2: Conduct forensic analysis of malware activity and associated artifacts	ME	Critical			
Subtask 3: Execute triage-level investigation management to document environment and actions	ME, LE	Critical			
Subtask 4: Identify scope of adversary access to determine extent of intrusion	HA, NA	NC			

99

Core Task 3: Perform triage-level malware analysis to enable defensive actions		**Scoring Metrics** __/2			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Identify, obtain, initial-triage, and malware samples	HA	NC			

Subtask 2: Incorporate findings of malware sample and prepare for additional processing	LE, HA, ASO	Applicable- Critical or Not Applicable - NC			

100

Core Task 4: To coordinate with mission/terrain owner for implementation of critical defensive measures to safeguard key and/or critical terrain		**Scoring Metrics** __/1			
No Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Hours**	**Operator =**	**Criterion 6**
N/A	TL, LE, OPSO	NC			

101

Core Task 5: Execute or coordinate target and engage actions against adversary intrusions		**Scoring Metrics** __/3			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: When ordered, eradicate detected malicious activity to remove adversarial presence	HA, NA, NT	Critical			
Subtask 2: Remove adversary access from the network, as required and directed	HA, NA	Critical			
Subtask 3: Provide mission partner clear recommendations for all identified indicators of compromised or TTPs	ME, NT	NC			

102

Core Task 6: Assess adversary risk to defended terrain		**Scoring Metrics** __/3			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Emulate threats to determine if technical and procedural cyberspace defenses are effective, as needed	HA, NA, ASO	NC			
Subtask 2: Emulate threats to determine if technical and procedural implemented mitigations are effective		NC			
Subtask 3: Identify the cyber-related risks to supported mission	LE, ASA	NC			

103

Core Task 7: Assess effectiveness of clearing actions		**Scoring Metrics** __/2			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Validate if technical and procedural actions are effective	HA, NA, NT	NC			
Subtask 2: Conduct defensive monitoring of the specified terrain to validate post-mitigation actions as required and directed	ME	NC			

Core Task 8: Enable hardening of defended terrain		Scoring Metrics __/2			
Subtasks	**Work Role(s)**	**Critical or Non-critical**	**Scale Y/N**	**Operator =**	**Criterion Y**
Subtask 1: Analyze attack surface of the specified terrain to enable hardening actions	HA, NA	Critical			
Subtask 2: Recommend security best practices on specified terrain to enable hardening actions	ME	NC			

3. (U) Assessment Scoring Metrics

(U) The chart below is UNCLASSIFIED.

(U) Core Task Score: _____ / _ x 100 = _____ % * Go = unit successfully completes 70% or greater of Performance Measures	Go: _____ No/Go: _____
(U) Critical Subtask Score: _____ / _ x 100 = _____ % * Go = unit successfully completes 100% of Critical Subtasks	Go: _____ No/Go: _____
(U) Non-critical Subtask Score: _____ / _ x 100 = _____ % * Go = unit successfully completes 70% of Non-critical Subtasks	Go: _____ No/Go: _____
(U) MET Composite Score: _____ / _ x 100 = _____ % * Go = unit successfully completes 70% or more METs	Go: _____ No/Go: _____

4. (U) Glossary of References and Supporting Information

4.1 (U) CPT Mission Essential Tasks (MET)

(U) The chart below is UNCLASSIFIED.

MET	Performance Measures	Scale	Operator	Criterion
ST 5.5.7 Direct Cyberspace Operations	To receive and process orders	Hours	<=	24
	Conduct mission planning and analysis	Y/N	=	Y
	Direct execution of simultaneous Defensive Cyberspace Operations	Operations	>=	2
	Conduct mission reporting IAW OPCON governance	Y/N	=	Y
OP 2.3.5.2 Integrate Operational Intelligence	To provide intelligence support to Defensive Cyberspace Operations planning	Days	<=	5
	To provide intelligence support to Defensive Cyberspace Operations in progress	Hours	<=	24
	To provide intelligence support to critical information requests or requirements	Hours	<=	6
ST 2.3 Manage Collected Information	Execute data handling and retention	Y/N	=	Y
	Develop analytic scheme of maneuver	Y/N	=	Y
	Plan, coordinate, and execute data collection for, storage, analysis, and transfer to meet mission requirements	Y/N	=	Y
OP 5.6.5.3 Conduct	To identify, characterize, and validate the area of operations	Days	<=	7

Defensive Cyberspace Operations	Find, fix, and track adversary presence on defended terrain	Y/N	=	Y
	To coordinate with mission/terrain owner for implementation of critical defensive measures to safeguard key and/or critical terrain	Hours	<=	6
	Execute or coordinate target and engage actions against adversary intrusions	Y/N	=	Y
	Assess adversary risk to defended terrain	Y/N	=	Y
	Assess effectiveness of clearing actions	Y/N	=	Y
	Enable hardening of defended terrain	Y/N	=	Y

4.2 (U) Acronyms

*All acronyms below are UNCLASSIFIED.

ASA	All Source Analyst
ASO	Analytic Support Officer
CMF	Combat Mission Force
CNMF	Cyber National Mission Force
DCO	Defensive Cyberspace Operations
DE	Data Engineer
DoDIN	Department of Defense Information Network
HA	Host Analyst
HHQ	Higher Headquarters
IAW	In Accordance With
JFHQ-C	Joint Force Headquarters-Cyber
LE	Leadership Element
ME	Mission Element
MET	Mission Essential Task
MoE	Measures of Effectiveness
MoP	Measures of Performance
MRT-C	Mission Relevant Terrain in Cyberspace
NA	Network Analyst
NC	Non-Critical
NT	Network Technician
OPCON	Operational Control
Ops	Operations
OPSO	Operations Officer
PLNR	Planner
S-CPT	Service-Cyber Protection Teams
SE	Support Element
SITREP	Situation Report
T&EO	Training & Evaluation Outline
TL	Team Lead
TTP	Tactics, Techniques, and Procedures
USCYBERCOM	United States Cyber Command


UNITED STATES CYBER COMMAND