

**BY ORDER OF THE COMMANDER
COMBAT FORCES COMMAND**

**COMBAT FORCES COMMAND MANUAL
13-602DCO-S, VOLUME 3**



22 DECEMBER 2025

***Nuclear, Space, Missile, Command and
Control Operations***

***DEFENSIVE CYBERSPACE
OPERATIONS FOR SPACE (DCO-S) –
OPERATING PROCEDURES***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: CFC/S35C

Certified by: CFC/S35C

Pages: 34

This manual implements Air Force Instruction (AFI) 13-602, Volume 3, *Spacecrew Operations*. This publication applies to all United States Space Force (USSF) and United States Air Force (USAF) uniformed members, Department of Defense (DoD) civilian personnel, civilian contractors (as applicable per contract documentation), allied mission partners (as applicable per international agreement) performing Defensive Cyberspace Warfare (DCW) operations duties on a Defensive Cyberspace Operations for Space (DCO-S) Weapon System (WS) in support of USSF or a Combatant Command (CCMD). This manual requires the collection and/or maintenance of information protected by the Privacy Act of 1974 authorized by 10 U.S.C. 9013, Secretary of the Air Force. The applicable System of Record Notice(s) (SORN) F011 AF AFMC B, *Patriot Excalibur (PEX) System Records* is available at:

<https://pclt.defense.gov/DIRECTORATES/Privacy-and-Civil-Liberties-Directorate/Privacy/SORNsIndex/DOD-Component-Notices/Air-Force-Article-List/>.

Ensure all records generated as a result of processes prescribed in this manual adhere to AFI 33-322, *Records Management and Information Governance Program*, and are disposed of in accordance with (IAW) the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Department of the Air Force (DAF) Form 847, *Recommendation for Change of Product*; route DAF Forms 847 from the field through the appropriate functional chain of command. This manual may not be supplemented. The authorities to waive wing, unit, or delta level requirements in this manual are identified with a tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit

requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternatively, to the publication OPR for non-tiered compliance items, IAW [paragraph 1.4](#).

Chapter 1—GENERAL INFORMATION	4
1.1. General.....	4
1.2. Scope.	4
1.3. Waivers.....	4
1.4. Certifying Official.	5
1.5. Governing Guidance.	5
Chapter 2—ROLES AND RESPONSIBILITIES	6
2.1. Overview.....	6
2.2. Delta Commanders (DEL/CC).....	6
2.3. Cyberspace Warfare (CW) Squadron Commanders (SQ/CC).....	6
2.4. Crew Chief.....	7
2.5. Individual Spacecrew.....	7
2.6. Embedded Cyber Intelligence Squadron/Detachment Commander.	8
Chapter 3—MISSION PLAN, BRIEF, EXECUTE, AND DEBRIEF	9
3.1. Mission Plan, Brief, Execute, and Debrief (PBED).....	9
3.2. Mission Planning.	9
3.3. Mission Briefing.	9
3.4. Mission Execution.	10
3.5. Mission Debrief.	11
Chapter 4—SAFETY OF OPERATIONS	13
4.1. Personnel Safety and Crew Rest Requirements.....	13
4.2. Crew Changeover.	13
4.3. Operations Check (Ops Check).	13
4.4. Risk Management.	13
4.5. Go/No-Go Criteria.	14
4.6. Operations Review Board (ORB).	14
Chapter 5—OPERATIONS DOCUMENTATION	16
5.1. General.....	16

5.2.	Technical Orders (TOs).	16
5.3.	Standard Operating Procedures (SOP).....	16
5.4.	Tactics, Techniques, and Procedures (TTP).	18
5.5.	Unit-Developed Checklists.	18
5.6.	Master Station Log (MSL).....	19
5.7.	Initial Operations for New or Upgraded Systems.	20
5.8.	WS Modification.	20
5.9.	Operations Review Board (ORB) Report Process.	20
Chapter 6—CREW COMPOSITION AND CONSTRUCT		22
6.1.	General.....	22
6.2.	Cyber Force Element.	22
6.3.	Mission Planning Cell (MPC).....	23
6.4.	Mission Support Cell (MSC).	25
6.5.	Crew Utilization Procedure.....	27
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		28
Attachment 2—CYBER 9-LINE TEMPLATE		33
Attachment 3—OPERATIONAL RISK MANAGEMENT WORKSHEET EXAMPLE		34

Chapter 1

GENERAL INFORMATION

1.1. General. This manual provides basic guidance for spacecrew operation of the DCO-S WS for USSF DCW crewmembers IAW AFI 13-602, Volume 3, *Spacecrew Operations*. This manual defines minimum requirements for establishing and sustaining DCW crew force readiness and cannot address every situation. Mission success depends upon a unit's readiness and ability to perform Combatant Commander (CCDR) requested capabilities. The intent of this volume is to establish guidance that applies to the day-to-day management of spacecrew operations, to include crew force management. In the context of this document, "DCO-S WS" can describe either a specific WS (e.g. Manticore, Kraken) or a grouping of similar systems into a single category.

1.2. Scope. This manual was developed to define spacecrew operations for DCO-S WSs. It is applicable to all spacecrew members performing DCW on a DCO-S WS in support of USSF or a CCMD. Applicability includes USSF and USAF uniformed members, DoD civilian personnel, civilian contractors (as applicable per contract documentation), Qualification Training (QT) instructors, allied mission partners (as applicable per international agreement), and other selected personnel performing or instructing Combat Mission Ready (CMR) space operations duties on the DCO-S WS.

1.2.1. A DCW spacecrew consists of officers, enlisted, government civilians, and civilian contractors who conduct space operations and are assigned to the DCO-S WS. A detailed depiction of DCW crew positions is identified in this manual.

1.2.2. Throughout this manual, DCW spacecrews will be referred to as spacecrews. **(T-2)**

1.3. Waivers. Units requiring a waiver will submit a new DAF Form 679, *Department of the Air Force Publication Compliance Item Waiver Request/Approval*, and route it to the appropriate level. **(T-2)**

1.3.1. CFC/CC delegated T-2 waiver authority to the CFC Deputy Commander (CD) in the SpOC/CC Memorandum, *Delegations and Withholding of Authorities*, 23 October 2024.

1.3.2. The following organizations will provide coordination in Section II of the DAF 679. **(T-2)**

1.3.2.1. Squadron Commander (SQ/CC)

1.3.2.2. Delta Commander (DEL/CC)

1.3.2.3. CFC Cyber Warfare Division (CFC/S35C)

1.3.2.4. CFC Training and Readiness (CFC/S73)

1.3.3. Place a copy of approved waivers in the individual's training folder in the current records management system, PEX, or its successor programs. PEX can be accessed at <https://test.omni.af.mil/ePex/Login?location=Login%2FHome%2FSelectPexPerson>.

1.3.4. For more detailed guidance, reference Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures* or contact CFC Training Branch (CFC/S735T) for questions on the waiver coordination process.

1.4. Certifying Official. The certifying official is responsible for ensuring a crewmember has demonstrated sufficient proficiency to perform all tasks assigned to the newly appointed position (e.g., crew position, instructor, evaluator).

1.4.1. The certifying official is the final signatory of certifications in PEX (e.g., evaluation AF Form 8, *Certificate of Aircrew Qualification*).

1.4.2. Certifying official responsibilities reside with the SQ/CC. Responsibilities of the certifying official will not be delegated. **(T-2)** For Cyberspace Warfare (CW) Detachments (Dets) that are aligned directly to a DEL, the Det/CC is the certifying official.

1.5. Governing Guidance. SQ/CC and the on-duty Crew Chief will ensure compliance with the operational aspects of this manual and the following instructions specific to DCW: **(T-2)**

1.5.1. CCDR instructions and associated USSF Components directives.

1.5.1.1. The Commander of Space Forces (COMSPACEFOR) standards direct staff and all Tactical Control units on normal, recurring tasks within mission/subject area annexes within their CCMD.

1.5.1.2. COMSPACEFOR standards are effective upon COMSPACEFOR approval until superseded or rescinded. The signature on the COMSPACEFOR standards cover sheet applies to the COMSPACEFOR standards and all annexes.

1.5.2. Operational tasking orders (e.g. Combined Space Tasking Order (CSTO), Cyber Tasking Order (CTO)).

1.5.2.1. Operational tasking orders will take precedence over local Special Instructions (SPINS).

1.5.2.2. In the case of a guidance conflict, operational SPINS will take priority over the component standards. **(T-2)**

1.5.3. Orders from Commander, United States Space Command and Commander, United States Cyber Command that direct presentation of forces and execution of operations in support of CCDR authority.

1.5.3.1. Planning Order (PLANORD). PLANORDs are planning directives that provide essential planning guidance and direct the development, adaptation, or refinement of a plan or order.

1.5.3.2. Deployment Order (DEPOD). DEPODs are directives from the Secretary of Defense, issued by the Chairman of the Joint Chiefs of Staff, authorizing the transfer of forces between CCDRs, Services, and DoD agencies. It outlines the gaining CCDR's authority over the transferred forces.

1.5.3.3. Operations Order (OPORD). OPORDs are directives issued by a CC to subordinate CCs for the purpose of effecting the coordinated execution of an operation.

1.5.3.4. Execution Order (EXORD). EXORDs are directives to implement an approved Concept of Operations. It is authorized by the President and Secretary of Defense and may be issued by the Chairman of the Joint Chiefs of Staff at their direction. CCMDs and subordinate components use EXORDs to initiate and execute military operations.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Overview. The roles and responsibilities listed below are to be executed at all levels within FLDCOMs, DELs, and CW operational units, unless otherwise stated. CCs at every level are responsible for ensuring the personnel under their command are qualified to perform the DCW mission in a contested, degraded, and operationally-limited environment.

2.2. Delta Commanders (DEL/CC). For the purposes of this manual, Delta (DEL) refers to Space Base Deltas (SBD), Space Launch Deltas (SLD), Mission Deltas (MD), or Space Deltas. The DEL/CC will:

2.2.1. Develop and implement a debrief process and ensure incorporation of Weapons and Tactics Programs into unit training and evaluation programs.

2.2.2. Review all new or modified DCO-S systems, publications, procedures, and processes for impacts on operations.

2.2.2.1. Ensure documentation is accurate and approved prior to implementation.

2.2.2.2. Ensure applicable training and evaluation products and materials are accurate and approved prior to implementation.

2.2.3. Submit requested changes to the DEL 6 Chief of Standardization and Evaluation for review and disposition in the recurring Standardization and Evaluation Board (SEB).

2.2.4. Define and refine robust intelligence requirements (i.e., Priority Intelligence Requirements and Essential Elements of Information) in order to meet operational and training needs in the face of a contested, degraded, and operationally-limited environment for space and cyberspace operations. Submit requests for information to embedded Intelligence SQ/Det to ensure crews have current intelligence for operations.

2.2.5. Approve minimum DCW crew reporting standards to meet Space Force Generation (SPAFORGEN) requirements.

2.2.5.1. Coordinate between CFC/S73 and other DEL/CCs to establish reporting requirements for committing DCO-S operators as “Employed-in-Place” (EiP) or available to CCDRs during the Commit phase of SPAFORGEN.

2.2.5.2. Establish minimum Mission Planning Cell (MPC) and Mission Support Cell (MSC) reporting standards as part of the SPAFORGEN cycle.

2.3. Cyberspace Warfare (CW) Squadron Commanders (SQ/CC). This section includes both Force Generation and Institutional Force Squadrons and Detachments. Most operational units employing DCO-S WS to perform DCW are Cyberspace Squadrons (CYS). However, some DCW units are detachments, and in those cases, the Det/CC is responsible for all SQ/CC responsibilities outlined in this manual. SQ/CCs will:

2.3.1. Generate combat ready space warfighters to ensure successful execution of DCW missions to secure and defend aligned DEL(s) mission system(s) Mission Relevant Terrain – Cyber (MRT-C) to assure freedom of maneuver in and access to cyberspace for all friendly forces operating within their assigned battlespace to generate CMR space power.

- 2.3.2. Executes all duties IAW AFI 1-2, *Commander's Responsibilities*.
- 2.3.3. Serves as certifying official for all CMR positions.
- 2.3.4. Serves as the certifying authority for all CMR personnel and those who transition to or from non-current or decertified status.
- 2.3.5. Review all new or modified systems, publications, procedures, and processes for impacts on operations.
- 2.3.6. Ensure operations-related documentation is accurate and approved prior to implementation.
- 2.3.7. Define and refine robust intelligence requirements (i.e., Priority Intelligence Requirements and Essential Elements of Information) in order to meet operational and training needs in the face of a contested, degraded, and operationally-limited environment for space operations. Submit requests for information to DEL Intelligence, Surveillance, and Reconnaissance (ISR) support to ensure crews have current intelligence for operations.
- 2.3.8. Present required number of operators and crews based on unique mission requirements and approved waivers IAW Space Force Guidance Memorandum (SPFGM) 2024-10-01, *Operations Planning and Execution*.
- 2.3.9. Establish unit-specific mission planning guidance addressing Mission Essential Tasks (METs) and ensure an appropriate level of mission planning is being conducted prior to each mission, IAW requirements outlined in the *DEL 6 Mission Planning Guide*. Mission Planning Guides for CFC and DEL 6 are available on SharePoint at: <https://usaf.dps.mil/sites/SpOC-DEL6/home/Staff/WeaponsTactics/Mission%20Planning/Forms/AllItems.aspx?id=%2Fsites%2FSpOC%2DDEL6%2Fhome%2FStaff%2FWeaponsTactics%2FMission%20Planning%2FMission%20Planning%20Guides&viewid=28c6fa22%2D9928%2D473f%2Da807%2Dc27561f9b587&FolderCTID=0x0120000A9BF62C93886B459D69CBF736410994>.

2.4. Crew Chief. The on-duty DCO-S Crew Chief, regardless of rank, is responsible for the operation of the DCO-S system. The Crew Chief will:

- 2.4.1. Ensure operations are planned, briefed, executed, and debriefed IAW the following: Joint Publication (JP) 5-0, *Joint Planning*; Space Doctrine Publication (SDP) 5-0, *Planning*; *DEL 6 Mission Planning Guide*; and SQ standards.
- 2.4.2. Ensure crewmembers are trained and certified IAW CFCMAN 13-602DCO-S, Volume 1, *Defensive Cyberspace Operations for Space (DCO-S) – Training*, and CFCMAN 13-602DCO-S, Volume 2, *Defensive Cyberspace Operations for Space (DCO-S) – Standardization and Evaluation Criteria*, prior to performing DCW duties.

2.5. Individual Spacecrew. Individual Spacecrew members will:

- 2.5.1. Spacecrew cyber operators will use best judgement to conduct operations in a safe and effective manner.
- 2.5.2. Complete training requirements and maintain currencies for assigned crew position.
- 2.5.3. Submit changes IAW local change management process to ensure DCO-S operations procedures are current and accurate.

2.5.4. Only conduct CMR operations in a position for which they are qualified and certified in.

2.5.5. Effectively determine sources of risk and make sound decisions to take appropriate operational and system risks based on a wide range of scenarios, mission constraints, mission restraints, and authorities.

2.6. Embedded Cyber Intelligence Squadron/Detachment Commander. The embedded Cyber Intelligence SQ/Det CC, also known as the Senior Intelligence Officer (SIO), is responsible for the execution of the Intelligence function within the DEL and its subordinate units. The SIO will:

2.6.1. Share actionable Cyber Threat Intelligence to all units performing DCW.

2.6.2. Coordinate with DEL and operational unit leadership to ensure Cyber Intelligence personnel are fully qualified to fill all mobility requirements to include any clearance requirements.

2.6.3. Coordinate with SQ leadership to ensure Cyber Intelligence personnel are fully qualified to fill all mobility requirements to include any clearance requirements.

2.6.4. Coordinate cyber-related intelligence CMR positions with operations SQ leadership and designate to which proficiency level each intelligence position will train.

2.6.5. Provide current, dynamic, and tactically relevant cyber-related intelligence to mission operations personnel and leadership.

2.6.6. Coordinates with MPC and Cyber Force Element to further mission areas and ensure feedback is incorporated into operations.

2.6.7. Perform Intelligence Preparation of the Battlespace for current and future operations, aiding mission planners and CW operators in daily tasks.

2.6.8. Coordinate with operational unit leadership to ensure realistic training and evaluation, and facilitate Tactics, Techniques, and Procedures (TTP) development.

2.6.9. Provide Cyber Warning Intelligence and Attack Sensing and Warning to mission operations.

2.6.10. Maintain intelligence training and intelligence standardization and evaluation programs, including intelligence QT and Combat Training (CT).

2.6.11. As needed, responsible for maintaining the unit Intelligence Oversight program.

2.6.12. Provides daily intelligence briefings during crew changeovers, accepts Mission Reports (MISREPs) at the conclusion of every shift, supports long-term planning efforts, and possesses surge capability to provide dynamic intelligence support during execution of high-interest or high-threat missions.

Chapter 3

MISSION PLAN, BRIEF, EXECUTE, AND DEBRIEF

3.1. Mission Plan, Brief, Execute, and Debrief (PBED). SQs will determine the appropriate mission PBED needs to meet mission requirements. **(T-2)** SQs will plan operations and ensure issues are analyzed to determine root cause as well as document lessons learned and recommended corrective actions. **(T-2)**

3.2. Mission Planning. Mission planning will take place before each operational shift, before high interest missions, before each training and evaluation event, and when directed by SQ/CC or Combat Squadron Commander (CSq/CC). **(T-2)** Mission planning will be IAW JP 5-0, SDP 5-0, *DEL 6 Mission Planning Guide*, and SQ standards. **(T-2)**

3.2.1. Mission Planning Cell (MPC). The CW MPC will coordinate and integrate plans with CSq MPCs, schedule DCW mission planning, and disseminate all mission plans to the DCO-S crew. **(T-2)** The MPC will consist of a dedicated planning team, including a CW team lead and intelligence planning lead, that will be responsible for Higher Headquarters (HHQ) taskings, assist with large force employment, and operational crew taskings. **(T-2)**

3.2.2. MPC members will take into account operational and mission taskings, current system status, communications status, status of supporting systems, space operations plans, intel capability, expected events, situation of supported friendly forces, intelligence on adversary actions and threats, and potential branches and sequels to the anticipated plan. **(T-2)**

3.2.3. Mission planning will be influenced by the following: tasking orders, SPINS, Technical Orders (TOs), published intelligence instructions, spin-up briefs, mission transfers, applicable FLDCOM and/or CCMD guidance, *SpOC Mission Planning Guide*; *DEL 6 Mission Planning Guide*, operational objectives, and debriefing guidance. **(T-2)**

3.3. Mission Briefing. The Crew Chief will brief the plan to all crewmembers to promote safe and effective missions. **(T-2)** All crewmembers must attend tactical mission briefs unless previously coordinated with the CSq/CC or designated representative. **(T-2)** Any questions or concerns that arise by the crew will be addressed prior to mission execution. **(T-2)** The purpose for all mission briefings is to ensure the entire crew is well informed and prepared to execute the mission at hand.

3.3.1. All briefings will include, at a minimum: **(T-2)**

3.3.1.1. Risk Management.

3.3.1.2. Go/No-Go status.

3.3.1.3. Mission priorities and objectives.

3.3.1.4. Rollback, Contingency, and Emergency Plans, to include Abort Criteria.

3.3.1.5. Significant rules (e.g., SPINS, Training rules, Rules of Engagement (ROEs)).

3.3.1.6. WS, assigned terrain, and facility status.

3.3.1.7. Threat Intelligence. Assigned intelligence personnel will provide a situation brief to include current intelligence for each CCMD, red order of battle (if applicable), observed

TTPs, intelligence assumptions, adversary intent, and Most Likely and Most Dangerous Enemy Courses of Action. **(T-2)**

3.3.2. Crewmembers not attending the mission brief will receive, at a minimum, an overview of the mission objectives, their roles and responsibilities, current Crew Information File (CIF) read file, and Emergency Procedures prior to beginning the mission. **(T-2)**

3.3.3. Positional Changeover Brief. For operational needs, the crew will be required to brief an oncoming crewmember. **(T-2)** When required, a positional changeover briefing with the oncoming crewmember will be delivered IAW checklist(s) and applicable directives. **(T-2)**

3.3.4. Alternate Mission Briefs. Alternate missions will be briefed in case the originally planned and briefed mission is cancelled/aborted or the mission was No-Go for some reason (e.g., equipment malfunction). **(T-2)**

3.4. Mission Execution. The DCO-S crew will execute missions to secure and defend the assigned mission systems in alignment with mission area objectives. **(T-2)**

3.4.1. DCO-S crews will perform the following DCW mission activities:

3.4.1.1. Continuous Monitoring (CONMON). Crews will perform persistent defense of space systems by observing system host and network data, receiving and analyzing signature or behavior-based alerts, and determining the legitimacy and impact of any indicators of compromise (IOC) by MCAs within defended mission systems. **(T-3)** CONMON activities are informed by the results of all other mission activities and intelligence reporting that drive actions such as signature updates or creation, or requirement for additional data sources. CONMON activities may result in the generation of Enable Hardening activities or indications and warnings to be investigated during Threat Hunting activities.

3.4.1.2. Threat Hunting (Hunt). Crews will execute intelligence driven, threat-focused hunt operations to expose Malicious Cyber Actors (MCA) and determine MCA scope and purpose within protected USSF mission systems. **(T-2)** Hunt activities involve proactive and iterative searches of defended systems for detection and isolation of threats which may evade existing cybersecurity implementation. Crews will also investigate indications and warnings including those from CONMON activities. **(T-2)**

3.4.1.3. Enable Hardening (Harden). Crews will enable actions to mitigate adversary exploitation where mission systems require technological upgrades or updates to software, hardware, or processes. **(T-2)** Crews will provide the operational CCs and applicable program offices with mission system hardening recommendations to increase system cybersecurity and resilience. **(T-2)** Crews will recommend hardening actions and report on mission system hardening recommendations to mitigate threat-specific risks to supported CCs. **(T-2)** Hardening activities intend to reduce the attack surface, increase resilience, and enhance deterrence through the increased difficulty of system exploitation by MCAs.

3.4.1.4. Continuous Assessment (Assess). Crews will assess the effectiveness of clearing and hardening actions taken by local system administrators to improve overall system security and resilience. **(T-2)** The assessment objective is to replicate threat intrusion actions to ensure vulnerabilities were mitigated, negating attempts by potential MCAs employing similar intrusion and exploitation TTPs.

3.4.1.5. Clear. Crews will target and engage MCAs to eliminate or neutralize threats from a mission system, and include actions on the Department of Defense Information Network (DoDIN) to interdict, contain, disrupt, or degrade MCA activity. **(T-2)** The objective of clearing operations is eradicating identified threats from the mission system.

3.4.2. DCO-S crews will provide the following DCW capabilities:

3.4.2.1. Battlespace Awareness. Crews will conduct organizational activity mapping, network mapping, system mapping, and asset enumeration and characterization to provide a real-time understanding of the terrain and associated risks. **(T-2)**

3.4.2.2. Discover and Counter Infiltration (D&CI). D&CI is the detecting, illuminating, and defeating of known or unknown threats within a defended network or mission system. The crew's employment of COMMON and hunt methodologies and processes will reinforce organic capability to detect, discover and characterize adversarial TTPs which evade routine cybersecurity measures. **(T-2)**

3.4.2.3. Cyber Threat Emulation (CTE). CTE is the process of emulating known adversary TTPs to replicate real-world threats to train and assess crew readiness. The cyber operator's ability to detect, respond to, and recover from the malicious cyber activity will be tested continuously throughout this process. **(T-3)**

3.4.2.4. Threat Mitigation. Crews will provide comprehensive, threat-focused reviews of a DEL's MRT-C. **(T-2)** Using authorized access, crews will assess mission system cybersecurity posture and processes against specific threats to identify cybersecurity vulnerabilities. **(T-2)**

3.4.3. All crewmembers must review and acknowledge any CIF items prior to executing mission duties. **(T-2)** Crewmembers joining an ongoing mission will receive a CIF update prior to executing mission duties. **(T-2)**

3.4.4. Mission Report (MISREP). There is currently no guidance document for DCO-S MISREPs.

3.4.5. All DCW incident reporting will be IAW MD 6 through the 66 CYS Cyberspace Warfare Operations Center (CWOC) Cyber Incident Response Plan and DEL reporting requirements. **(T-2)**

3.5. Mission Debrief. Spacecrews will conduct a debrief after any high interest events, training and evaluation events, any event previously mission planned and executed, any deviations from standards, and when directed by SQ/CC or CSq/CC. **(T-2)**

3.5.1. The debrief will be designed to capture lessons learned, learning points, and lessons observed beginning with mission planning through mission execution. **(T-2)**

3.5.2. SQs will make every effort to include all personnel involved in the mission or event in the debrief. **(T-2)**

3.5.3. Crew Chief and supervisors are responsible for tracking currency for their crewmembers. Spacecrews will track task accomplishment, for currency requirements, during each operations shift as part of the mission debrief and document accomplishment in PEX. **(T-2)**

3.5.4. Lessons Learned will be documented in the CFC approved Lessons Learned Information System. **(T-2)**

3.5.5. Line Instructors will incorporate applicable lessons learned and learning points into training and TTP development to ensure continuous improvement of the mission. **(T-2)**

Chapter 4

SAFETY OF OPERATIONS

4.1. Personnel Safety and Crew Rest Requirements. To ensure mission success and personnel safety, spacecrew members under nominal operations will have the opportunity for eight (8) hours of uninterrupted crew rest prior to assuming an operational shift. **(T-2)** Uninterrupted crew rest is defined as a period of time with no unit taskings. The purpose of crew rest is to provide the member the opportunity to receive an appropriate amount of sleep to ensure they are ready to assume operations.

4.1.1. Crew Rest is defined as a condition that allows an individual the opportunity for eight hours of uninterrupted rest prior to assuming an operational shift. Each crewmember is individually responsible for ensuring they obtain sufficient sleep during crew rest periods.

4.1.2. Nominal Duty Period is 12 hours with the addition of changeover briefings.

4.1.3. The Crew Chief or MPC Chief may extend the Duty Period up to 14 hours to compensate for unplanned mission delays, provided the mission requirements justify the increased risk.

4.1.4. The SQ/CC or CSq/CC may extend the Duty Period up to 16 hours to compensate for unforeseen emergencies (e.g., snowed in, accident, injury).

4.1.5. Extended Duty Periods must be annotated in the Mission Log, at a minimum detailing authorizing agent and crewmembers affected. **(T-2)**

4.1.6. Crew rest is mandatory for any crewmember prior to performing any crew duty on any mission system. **(T-2)**

4.1.7. Only operations crewmembers performing crew duties are entitled to crew rest.

4.1.8. Recommended crew rest for rotation of shifts (e.g. transition from days to mids) is a minimum of 24 hours.

4.1.9. Crewmembers are prohibited from consuming alcohol within an eight (8) hour window before assuming crew duties. **(T-2)**

4.1.10. Crewmembers are prohibited from using or being under the influence of medication that can hinder operational performance during the mission. **(T-2)**

4.2. Crew Changeover. Units will create a changeover checklist, PowerPoint slides, and procedures to ensure standardization between crews and all information is passed as needed. **(T-3)** Crew changeover can be incorporated with the CSq, and changeover brief will occur at the beginning and end of every shift. **(T-2)**

4.3. Operations Check (Ops Check). All oncoming spacecrews will accomplish sufficient Ops Checks to ensure safe and effective mission accomplishment. **(T-2)** Each unit will ensure local procedures are established for performing Ops Checks that meet the minimum requirements as outlined in the CIF. **(T-2)**

4.4. Risk Management. Units will use Operational Risk Management (ORM) worksheets (reference [Attachment 3](#)) to address event risk factors. **(T-3)** ORM worksheets will address mission planning for the event, spacecrew experience, spacecrew personal risk factors, event

complexity, event duration, risk to the Mission Partner network, and DCO-S WS status. **(T-2)** WS status will include an impact assessment on all WS deviations employed without completing the formal WS modification process, as described in AFI 10-601, *Operational Capability Requirements Documentation and Validation*. **(T-2)** The impact assessment must include the deviation's impact to the Mission Partner network, Authority to Operate, and Authority to Connect. **(T-2)** The Crew Chief is responsible for ensuring ORM worksheet completion prior to each event.

4.4.1. Each operator will complete a personal ORM worksheet to identify personal risk factors and provide this worksheet to the Crew Chief prior to the pre-mission brief. **(T-3)**

4.4.2. Crew Chiefs will review all ORM worksheets to validate there are no issues or that all issues are mitigated per Go/No-Go criteria for the crew to execute the tasked mission or perform the duties of their crew's respective position. **(T-3)**

4.5. Go/No-Go Criteria.

4.5.1. The SQ/CC will provide written guidance via CIF in PEX. **(T-2)** Crewmembers will not operate on the DCO-S WS until Go/No-Go procedures have been accomplished and verified. **(T-2)**

4.5.2. Crew Chiefs will conduct Go/No-Go verifications for every shift. **(T-2)**

4.5.3. The Go/No-Go process will at a minimum verify the following:

4.5.3.1. Qualification/certification IAW CFCMAN 13-602DCO-SV1 and CFCMAN 13-602DCO-SV2. **(T-2)**

4.5.3.2. Currency and proficiency. **(T-2)**

4.5.3.3. Compliance and acknowledgement of CIF items. **(T-2)**

4.5.3.4. Completion of Individual risk assessments. **(T-2)**

4.5.3.5. Completion of ORM worksheets (reference [Attachment 3](#)). **(T-3)**

4.5.4. All Crew Chiefs will conduct checks for Go/No-Go criteria covering the succeeding 72 hours and prior to entering pass period (e.g. Crew 1 Chief is expected to enter pass on a Thursday at 1500 and not expected to return for next shift until Monday at 0700). **(T-2)** This will consist of validating Go/No-Go criteria for their crew working in the next sequential scheduled shifts (e.g. Monday through Thursday, 0700-1500), alerting the MPC Chief of members not meeting Go criteria, and briefing the oncoming crew at changeovers. **(T-2)**

4.6. Operations Review Board (ORB). SQs will conduct an ORB to determine the cause of any abnormal system response IAW AFI 13-602V3. **(T-2)**

4.6.1. Abnormal system responses requiring an ORB include but are not limited to adversary action negatively impacting a system, major system degradation, indications of erroneous system response, procedures with significant mission impact, and significant events where the cause cannot be determined by initial assessment or when corrective action is beyond minimal retraining or minor procedural changes. Spacecrew member deviations from real-world operations significant enough to drive mission impacts or result in system degradations may also drive ORBs.

4.6.2. The ORB convening authority is the responsible SQ/CC (in coordination with DEL Standardization and Evaluation (Stan/Eval)) performing combat operations. The SQ/CC will inform their DEL/CC and the DEL 6/CC when convening an ORB. **(T-2)**

4.6.3. If the abnormal system response potentially impacts operations outside the DEL, the convening authority will also provide a memorandum to HQ CFC/CD for Operations, HQ CFC/S73, HQ CFC Current Operations (CFC/S33), HQ CFC/S35C, and HQ CFC Safety Office. **(T-2)**

4.6.4. ORB composition is at the discretion of the convening authority. A safety representative, as defined in AFI 91-202_SPOCSUP, *The US Air Force Mishap Prevention Program*, is a mandatory participant for all ORBs. The safety representative may determine their participation is not required after the initial convening of the ORB.

4.6.5. At the conclusion of an ORB, the SQ/CC will produce an initial report. **(T-2)** Refer to [paragraph 5.9](#) for details on ORB documentation and reporting.

Chapter 5

OPERATIONS DOCUMENTATION

5.1. General. Operational space systems are operated IAW published technical data and operations procedures. TOs, Operating Instructions (OI), Standard Operating Procedures (SOPs), and Tactics, Techniques and Procedures (TTP) will be designed to work in concert with one another to achieve mission success while ensuring safety and proper operation of the DCO-S WS. **(T-2)** TTPs may also supplement steps within procedures with situation-specific recommendations.

5.1.1. TOs and SOPs will capture necessary steps to ensure proper operation of the WS within acceptable safety and system limits. **(T-2)**

5.1.2. TTPs will capture non-prescriptive guidance to identify best practices and recommended actions to employ the WS in a wide range of situations and adversary actions. **(T-2)**

5.1.3. TTPs will not violate TOs or published WS limitations but may recommend the use of specific procedures or combinations of procedures. **(T-2)**

5.1.4. DEL Stan/Eval, Weapons & Tactics, and unit tacticians will develop and implement TOs, SOPs, and TTPs to ensure operational and equipment safety and integrity. **(T-2)**

5.1.5. For procedures affecting more than one DEL, the DEL 6/CC will have the ultimate responsibility of ensuring procedures are sound before operational use by the DCW crew. **(T-2)**

5.2. Technical Orders (TOs). Operational systems will be operated IAW published technical information and operations procedures. **(T-2)** Changes to TOs will be accomplished IAW TO 00-5-1, *AF Technical Order System*. **(T-2)** TOs include all manuals developed or acquired for organic operation, maintenance, inspection, modification or management of centrally acquired and managed USSF systems and end items.

5.2.1. Systems are operated IAW published TOs, where available. TOs will be maintained IAW TO 00-5-1 and other applicable TOs available at <https://etims.cce.af.mil/ETIMS/index>. **(T-2)**

5.2.2. Units may develop operations manuals and local procedures (e.g., SOPs) to supplement TOs as necessary. Locally developed guidance will not conflict with nor violate the TO. **(T-2)** Local procedures will be developed as OIs as specified below. **(T-2)**

5.3. Standard Operating Procedures (SOP). SOPs are a set of step-by-step instructions to ensure safe and effective WS employment.

5.3.1. When contractor-developed procedures are produced and delivered, SQ Stan/Eval will assess any procedural impacts and prepare implementation guidance. **(T-2)**

5.3.2. SQs will validate DCW operations procedures using off-line systems, ranges, or simulators to the maximum extent possible prior to operational use. **(T-2)**

5.3.3. The SQ/CC will determine the appropriate level of validation and training required before a new or changed procedure is implemented for operations. **(T-2)**

5.3.4. SOPs will be identified as permanent or temporary. Rescind TP (e.g., Interim Operations Supplement) once they are no longer required. **(T-2)**

5.3.5. The coordination and implementation process for new or updated procedures will ensure technical accuracy, adherence to established standards, and training requirements. **(T-2)** Changes to procedures are categorized according to the urgency for their implementation. The three categories of changes are emergency, urgent, and routine, as defined in TO 00-5-1 and AFI 13-602V3.

5.3.6. DEL Chief of Stan/Eval will review SOPs at least annually to ensure accuracy, currency and applicability. **(T-2)** Approved procedure changes will count as a review for that procedure. **(T-2)** Senior Line Evaluators will identify updates driving training product changes to the line instructors and operations support. **(T-2)**

5.3.7. All Permanent Procedures and relevant crew aids in the applicable work center or issued to all personnel performing duties in the operations center will be maintained on a system of appropriate classification. **(T-2)**

5.3.8. No new or changed procedures will be used for operations until properly approved, coordinated and trained, as required. **(T-2)**

5.3.9. CIFs, Interim Operations Supplements, and Difference Training (DT) completion will be documented and signed off by crewmembers in PEX. **(T-2)**

5.3.10. Crew Chiefs will use system auditing tools to validate crewmember completion of required documentation signoff. **(T-2)**

5.3.11. Development of SOPs. Units operating systems without formally published technical information will develop SOPs to ensure proper WS employment. **(T-2)** Contractor-developed procedures are produced and delivered according to the specifications in the governing contract. The implementing DEL will review these contractor documents to assess any procedural impacts. **(T-2)**

5.3.11.1. SOPs will be formatted IAW TO 00-5-1 or DAFMAN 90-161, para 4.5. **(T-2)**

5.3.11.2. Instructions are updated as needed to keep pace with changes to the system and operational employment. The coordination and implementation process of new and/or updated procedures ensures technical accuracy and adherence to established standards and training requirements. Any changes to instructions are categorized according to the urgency for their implementation. The three categories of changes are emergency, urgent and routine.

5.3.11.3. Units will review OIs and SOPs at least annually to ensure accuracy, currency, and applicability. **(T-2)** Any changes to OIs or SOPs will first be reviewed by the SQ/CC prior to approval by DEL Chief of Stan/Eval. **(T-2)** This review will be documented and maintained for two years in PEX. **(T-2)**

5.3.11.4. All permanent instructions are maintained in the appropriate work center or issued to all personnel performing duties in the work center. No new or changed instructions will be used for operations until properly approved, coordinated (according to category), and spacecrew is trained as required. **(T-2)**

5.3.11.5. Units will forward a copy of all approved permanent instructions and related training material to the 66 CYS Formal Training Flight (FTF) for incorporation into QT. **(T-2)**

5.3.11.6. Supplemental instructions are used to amplify and/or augment existing permanent procedures or TOs without altering them. Units using supplemental instructions will develop and implement a process for coordination, approval, and periodic review prior to use. **(T-2)**

5.3.11.7. Create and publish CIF to ensure operators are aware.

5.4. Tactics, Techniques, and Procedures (TTP). Operations personnel will incorporate and apply TTP while conducting mission operations to effectively posture and defend the WS and employ it to maximum effectiveness based on current situation, tasking, priorities, limitations, and constraints IAW Air Force Space Command Instruction (AFSPCI) 10-260, *Tactics Development Program*. **(T-2)** DELs will execute the complete Weapons and Tactics model. **(T-2)** This includes Threat Assessments, threat-based exercises and training events, Weapons and Tactics conferences, Tactics Review Boards, a Tactics Improvement Process and operational testing; for the purpose of improving Operations Capability (OPSCAP) in a contested, degraded, and operationally-limited environment.

5.4.1. Spacecrews are expected to develop and improve TTPs in the course of training, exercises, and operations.

5.4.2. When conditions permit, these TTPs will be documented, submitted as Tactical Improvement Proposals IAW DAFMAN 11-260, *Tactics Development Program*, and reviewed by system experts prior to operational use. **(T-2)** The nature of operations may require spacecrews to implement new tactics prior to full coordination or testing to keep a system safe or to accomplish the mission in the face of adversary action or unanticipated scenarios.

5.4.3. Spacecrews who execute untested or undocumented TTPs must always adhere to sound risk management principles, known system limitations, and established ROEs. **(T-2)**

5.4.4. Spacecrew members will maintain vigilance and an appropriate state of readiness to respond to threats and unforeseen events. **(T-2)**

5.4.5. HQ USSF, FLDCOMs, and DELs will execute the complete Weapons and Tactics model as outlined in DAFMAN 11-415, *Weapons and Tactics Programs* and AFSPCI 10-260. **(T-2)** This includes Threat Assessments, Realistic Training Review Boards (RTRBs), threat-based exercises and training events, Weapons and Tactics Conferences, Tactics Review Boards, a Tactics Development Process, and operational testing; all for the purpose of improving combat capability.

5.5. Unit-Developed Checklists.

5.5.1. Locally developed checklists will be used and will, at a minimum, include: **(T-2)**

5.5.1.1. Warnings and Caution messages as required by the unit.

5.5.1.2. Position-specific weapon or mission employment information as required by the unit.

5.5.2. Line Instructor, Line Evaluator, and Tactician will review the locally developed checklists and crew aids prior to SQ/CC approval. **(T-2)**

5.5.3. SQ/CC will approve locally developed checklists and crew aids. **(T-2)**

5.5.4. Line Evaluators will maintain the list of current and authorized checklists, crew aids, and other information as necessary in the CIF library. **(T-2)**

5.5.5. Units will create a changeover checklist IAW [paragraph 4.2](#) of this manual. **(T-2)**

5.5.6. Temporary Procedures (TP).

5.5.6.1. TPs are short-term, non-standard changes to operating procedures (e.g., WS testing). TPs are valid for 45 days and may be extended up to 90 days. TPs will be approved by the DEL Chief of Stan/Eval Branch prior to implementation. **(T-2)** In an emergency, TPs may be approved by the SQ/CC or SQ/DO and then verified by the DEL Chief of Stan/Eval within five business days.

5.5.6.2. TP will be removed following TO publication and/or update. **(T-2)**

5.5.6.3. Create and publish CIF to ensure operators are aware.

5.5.7. Supplemental Procedures. Procedures containing instructions for use in conjunction with data contained in their parent TOs and are not stand-alone publications.

5.5.8. Crew Aids. For details on locally prepared crew aids, reference TO 00-5-1.

5.6. Master Station Log (MSL).

5.6.1. Crew Chiefs will document significant events/crew actions required for the MSL, such as the following minimum requirements: **(T-2)**

5.6.1.1. Any missions or orders.

5.6.1.2. Mission number and type.

5.6.1.3. Incoming crewmembers.

5.6.1.4. Shift change times.

5.6.1.5. Period of Interest/Vulnerability Window.

5.6.1.6. CFC/CC notes and/or communication.

5.6.1.7. CIFs.

5.6.1.8. DCO-S WS status, degradations, or abnormal system response (e.g., network sensor down).

5.6.1.9. Changes or deviations to Mission Materials (e.g., TTP updates, new SOPs).

5.6.1.10. Changes to Crew Duty Periods.

5.6.1.11. Updates or notifications from CFC, Combined Space Operations Center (CSpOC), or National Space Defense Center (NSDC).

5.6.1.12. Significant communications as determined by the Crew Chief.

5.6.2. On-shift Crew Chiefs will review MSL with on-coming Crew Chief during shift-change to ensure turn-over of key events or information. **(T-2)**

5.6.3. Operational units will have a Continuity of Operations plan and Primary, Alternate, Contingency, Emergency plan in place to maintain MSL to account for operations during outage periods. **(T-2)**

5.6.4. MSLs will be electronic, updated by each mission cell on shift, compliant with AFI 33-322 and maintained for a minimum of five years. **(T-2)**

5.7. Initial Operations for New or Upgraded Systems. Prior to system operational test activities and/or initial operations, the responsible SQ/CC will ensure operations, training, standardization, evaluation, and crew force management programs are developed and managed to provide adequate support to the new or upgraded system operations. **(T-2)**

5.7.1. Space Systems Command (SSC) individuals may be used to conduct operations on new or upgraded systems prior to operational use.

5.7.2. SSC individuals will be identified, documented, and trained as specified in Department of the Air Force Guidance Memorandum (DAFGM) 2025-13-01V1, *Ready Spacecrew Program Training* and CFCMAN 13-602DCO-SV1 prior to conducting operations on a live DCO-S WS. **(T-2)**

5.8. WS Modification. Permanent modifications that change the configuration of an asset or software for operational effectiveness, suitability, survivability, safety, service life extension, and/or reduce ownership costs of a fielded WS, subsystem, or item are submitted on AF Form 1067, *Modification Proposal*. For information on this process, refer to Department of the Air Force Instruction (DAFI) 63-101/20-101, *Integrated Life Cycle Management*. Permanent modifications will require an additional amount of developmental testing/operational testing prior to fielding. **(T-2)**

5.9. Operations Review Board (ORB) Report Process. When an ORB has been finalized, the SQ/CC will generate an initial report. **(T-2)**

5.9.1. The following information will be in an official memorandum format: **(T-2)**

5.9.1.1. Date the ORB convened and topic.

5.9.1.2. Personnel participating in the ORB (include rank, name, duty title, telephone number, and email address).

5.9.1.3. If the safety representative determines their involvement is unnecessary, document the name and other required information of the individual making the determination and in parentheses state “determined safety involvement not necessary.”

5.9.1.4. Sequence of events (e.g., time, locations). Use mission crew or duty positions instead of names.

5.9.1.5. Include a brief description of event impact on the primary or secondary mission.

5.9.1.6. Explain the root cause(s) of the incident.

5.9.1.7. Recommendations, Lessons Learned, and Action Items.

5.9.1.8. Include a broad summary of the cause(s) of the incident.

5.9.2. Crew Chiefs will provide status updates on all action items to the ORB convening authority every 30 days after submission of initial report until closed. **(T-2)** Crew Chiefs may combine updates from multiple ORBs into one report when providing status updates.

5.9.3. The ORB team will fully protect against the release of any information pertaining to the ORB and its outcomes. **(T-2)** Treat all information pertaining to ORBs with the same rigor as safety investigations.

5.9.3.1. Information will be considered preliminary until the approval of the ORB report by the appropriate convening authority. **(T-2)**

5.9.3.2. Unless the ORB is convened by a Joint CC, members of the investigative team will not convey preliminary information, conclusions, or assessments outside of the FLDCOM. **(T-2)**

5.9.4. During the ORB process, requests for information will go to the DEL/CC and HQ CFC/S33, HQ CFC/S73, and HQ CFC/S35C. **(T-2)**

5.9.5. If the ORB investigation leads to discovery of reportable criteria, the ORB convening authority will immediately notify the DEL/CC. **(T-2)**

5.9.6. CIFs are intended to inform operators of updates on a temporary basis and will not be used as permanent procedures. **(T-2)** CIFs will be established when a unit deems necessary based on changes in HHQ guidance, updated crew aids, checklists, or any other information certified operators may need to perform the mission effectively. **(T-2)**

Chapter 6

CREW COMPOSITION AND CONSTRUCT

6.1. General. 62 CYS, 64 CYS, 68 CYS, and 69 CYS are the Force Generation Squadrons (FGS) that generate and present personnel and capabilities through CSqs and Combat Detachment (CDets) IAW SPFGM 2025-10-02. All other operational DCW units not generating and presenting forces will align their crew composition and construct to the maximum extent possible and practical. **(T-2)**

6.2. Cyber Force Element. The Cyber Force Element consists of Cyberspace Defense Operator (CDO), Incident Responder (IR), and Crew Chief CMR positions, and will align duty shifts to their CSqs. **(T-2)** The following paragraphs define each crew position by type, but do not quantify each crew position, as that may differ for each operational unit.

6.2.1. Cyberspace Defense Operator (CDO). CDO is the foundational CMR crew position for initial Basic Mission Qualified (BMQ) on the DCO-S WS. CDOs will conduct directed administration, detection, scoping, and strike actions in support of COMMON, Hunt, Harden, Assess, and Clear activities as well as dynamic tasks. CDOs will perform the following key duties, which are not all-inclusive: **(T-2)**

6.2.1.1. Conduct directed PBED.

6.2.1.2. Execute directed detection actions. Analyze extracted network, host, and other forensic artifacts to support endpoint compromise determinations.

6.2.1.3. Execute directed scoping actions. Find endpoints matching targets such as accounts, registry configurations, files, processes, Internet Protocol (IP) addresses, ports, domains, or other correlating data to determine extent of compromises.

6.2.1.4. Execute directed strike actions against targets such as accounts, registry configurations, files, processes, IP addresses, ports, domains, or other system components known to contain compromises.

6.2.2. Incident Responder (IR). IR is a CMR position upgrade. IRs will conduct and direct scoping and strike actions in support of harden, assess, and clear activities. IRs will perform the following key duties, which are not all-inclusive: **(T-2)**

6.2.2.1. Respond to anomalies and adversary activity within assigned space mission area(s) MRT-C by assisting with mitigation, containment, recovery, and/or restoration operations.

6.2.2.2. Integrate and participate with mission area Incident Response Teams.

6.2.2.3. Update and maintain cyber-Incident Response Plans for defended mission systems.

6.2.2.4. Report incidents to CSq/CC, on-duty space ops Crew Chief, and 66 CYS/CWOC.

6.2.2.5. When not responding to an anomaly, event, or incident, perform CDO duties at an advanced level.

6.2.3. Crew Chief. Crew Chief is a CMR position upgrade. Crew Chiefs will perform the following key duties, which are not all-inclusive: **(T-2)**

- 6.2.3.1. Translate tactical objectives into tactical tasks to be completed by the crew each shift.
- 6.2.3.2. Lead the Cyber Force Element and is responsible for crew safety.
- 6.2.3.3. Ensure crewmembers have completed training and evaluation requirements prior to performing operations.
- 6.2.3.4. Oversee taskings, missions, and system operations.
- 6.2.3.5. Responsible for multiple operational reporting criteria directed at joint, service, and FLDCOM level.
- 6.2.3.6. Provide decisive first assessment of detected cyber threats to CSq, 66 CYS/CWOC, and appropriate stakeholders.
- 6.2.3.7. Ensure optimal performance of DCW on mission area systems.
- 6.2.3.8. Report planned and unplanned OPSCAP and other system outage information to the responsible HHQ within established timing standards.
- 6.2.3.9. Report suspicious cyber activity via 9-line IAW [Attachment 2](#).
- 6.2.3.10. Perform data collection, processing, and reporting of operations.
- 6.2.3.11. Disseminate vertical and horizontal reports, communications, direction, and status to HHQ, subordinate units, and supporting organizations to ensure direction is acknowledged and accomplished, feedback is provided, and re-direction is possible.
- 6.2.3.12. Identify, document, and disseminate results of anomalous and malicious cyberspace activity and/or actors within assigned MRT-C to appropriate stakeholders.
- 6.2.3.13. Maintain situational awareness of crew operations.

6.3. Mission Planning Cell (MPC). MPC consists of a MPC Chief, Tactician(s), and Threat Hunter(s). The following paragraphs define each position by type, but do not quantify each position, as that may differ for each operational unit. The MPC will perform the following key duties, which are not all-inclusive: **(T-2)**

- 6.3.1. Ensure the effective implementation of PBED at the tactical level IAW the *SpOC Mission Planning Guide*.
- 6.3.2. Be responsible for optimal application of high-level mission, environment, enemy, effects, capabilities, plan, phasing, contracts, and contingencies (ME3C(PC)2) planning methodology to DCW.
- 6.3.3. Produce mission plans based on operational orders, TACON taskings, current intelligence, current and future operations, lessons learned, and maintenance or sustainment actions affecting operations.
- 6.3.4. Dynamically access, aggregate, collate, and display situational awareness and mission impact information for all components of the mission system.
- 6.3.5. Provide tactical assessment to the strategic vision on how national and joint missions in other domains are supported.
- 6.3.6. MPC Chiefs will perform the following key duties, which are not all-inclusive: **(T-2)**

- 6.3.6.1. Brief mission plans vertically and horizontally as needed for mission execution approval and completion.
- 6.3.6.2. Direct mission plans to DCW Crew Chief and coordinate with other crews and work centers as required. Recommend surges, aborts, response, and recovery actions to the Crew Chief.
- 6.3.6.3. Integrate and collaborate with their CSq MPC to align timing and tempo of DCW tactical objectives to Mission Area operations.
- 6.3.6.4. Coordinate with the 66 CYS/CWOC and other mission partners as appropriate on incident response efforts.
- 6.3.6.5. Coordinate additional authority approval requests as needed for mission completion.
- 6.3.6.6. Centralize assumptions for Requests for Information with their corresponding Intelligence supporting agency.
- 6.3.6.7. Coordinate communication contracts with appropriate agencies to execute mission plans.
- 6.3.6.8. Debrief mission results. Submit MISREPs and other reports IAW established procedures. Identify and communicate operator, WS, sensor, and signatures areas for improvement.
- 6.3.7. Tacticians will perform the following key duties, which are not all-inclusive: **(T-2)**
 - 6.3.7.1. Lead the tactical planning efforts to define mission objectives.
 - 6.3.7.2. Tailor plan development to incorporate adversary threat capabilities and assessments, most likely and most dangerous (ML/MD) Courses of Action (COAs), blue scheme of maneuver, and time-phased actions.
 - 6.3.7.3. Convert tasked operational mission statement, CC's intent, operational objectives, constraints, and restraints into tactical mission objectives and end state required to begin PBED and mission execution.
 - 6.3.7.4. Interpret tasked orders into tactical objectives to support national and joint missions across multiple domains.
 - 6.3.7.5. Be knowledgeable in Red and Blue Teaming to guide the learning process.
 - 6.3.7.6. Conduct technical assessments. Execute threat replication tactical plans to generate adversary-like data and validate friendly TTPs on detection of enemy TTPs.
 - 6.3.7.7. Conduct procedural assessments. Execute threat replication tactical plans to provide assessments of internal communication, coordination, and other SOPs.
 - 6.3.7.8. Report results of TTP assessments to DEL Weapons and Tactics.
 - 6.3.7.9. Design threat replication tactical plans IAW established Pre-Approved Actions, Pre-Coordinated Actions, and ROEs.
- 6.3.8. Threat Hunters will perform the following key duties, which are not all-inclusive: **(T-2)**
 - 6.3.8.1. Create Tactical Objectives to meet Operational Tasks.

6.3.8.2. Prioritize intelligence for design of scoped, hypothesis-based threat hunt mission plans.

6.3.8.3. Interpret constraints and restraints to create branches and contingencies to mission plans.

6.3.8.4. Ensure Cyber Force Elements are briefed on objectives, ROEs, Measures of Effectiveness (MOE), Measures of Performance (MOP), plans, contingencies, and applicable TTPs.

6.3.8.5. Validate mission planning.

6.4. Mission Support Cell (MSC). The MSC consists of MSC Chief, Network Specialist(s), and Host Specialist(s). The following paragraphs define each position by type, but do not quantify each position, as that may differ for each operational unit. The MSC will perform the following key duties, which are not all-inclusive: **(T-2)**

6.4.1. Manage crew schedules for operations.

6.4.2. In coordination with space operations crews and sustainment teams, identify and analyze assigned mission area MRT-C and Key Terrain in Cyberspace (KT-C).

6.4.3. Know and understand the risk to space operations, space mission systems, people, assets, data, and capabilities.

6.4.4. Validate the normal cyberspace activity baseline for assigned space missions.

6.4.5. Conduct analysis of cyber threats and vulnerabilities.

6.4.6. Perform anomaly and threat analytics within assigned mission systems.

6.4.7. Track vulnerabilities and attack vectors across MRT-C to include identifying and assessing the embedded components within the space enterprise.

6.4.8. Fully understand vulnerabilities, potential impacts to operations, and identify mitigating actions and/or configurations.

6.4.9. MSC Chiefs will perform the following key duties, which are not all-inclusive: **(T-2)**

6.4.9.1. Verify terrain mapping and coverage.

6.4.9.2. Develop and maintain a DCW system integration plan and continuous assessment plan.

6.4.9.3. Manage employment of detection signatures and create new detection methods.

6.4.9.4. Update signatures and tune network sensors (e.g., Zeek, Suricata) based on emerging threats, actionable intelligence, and Indicators of Compromise (IOC).

6.4.9.5. Act as the primary integrator with the host installation command post and/or Crisis Action Team to gather pertinent event or crisis information for mission operations execution and/or MPC planning considerations and Combat Unit leadership situational awareness.

6.4.9.6. Conduct Crew Force Management responsibilities.

6.4.10. Host Specialists will perform the following key duties, which are not all-inclusive: **(T-2)**

6.4.10.1. Specialize in advanced vulnerabilities and emerging threats in hardware and software of host systems.

6.4.10.2. Assess the configuration, settings, logging, and activity of a targeted host system to identify security shortfalls, vulnerabilities, or maliciously configured systems.

6.4.10.3. Develop tools utilized for investigations into an incident or counter threat actions, regardless of Operating System.

6.4.10.4. Assess a targeted host system for health and gather information which operators can analyze or use to determine actions.

6.4.10.5. Adjudicate TTPs related to hosts.

6.4.10.6. Guide development of exercises, simulators, and other resources.

6.4.11. Network Specialists will perform the following key duties, which are not all-inclusive: **(T-2)**

6.4.11.1. Specialize in advanced vulnerabilities and threats of network architectures, hardware, technologies, and associated systems.

6.4.11.2. Conduct network reconstruction by analyzing the data collected from packet captures and flow data.

6.4.11.3. Identify misconfigured or malicious activity based on the observable network traffic.

6.4.11.4. Assess the configuration, settings, and activity of a network to identify security shortfalls, vulnerabilities, or maliciously configured network infrastructure.

6.4.11.5. Develop tools utilized for investigations into an incident or counter threat actions on network infrastructure.

6.4.11.6. Guide development of exercises, related simulations, and other resources.

6.4.11.7. Adjudicate TTPs related to network appliances and analysis.

6.5. Crew Utilization Procedure.

6.5.1. Unit CCs will ensure spacecrew members are assigned to authorized positions IAW Unit Manning Documents (UMDs) and that any applicable spacecrew member status is properly documented in Defense Readiness Reporting System – Strategic (DRRS-S) and PEX. **(T-2)**

6.5.2. During SPAFORGEN Prepare and Ready phases, Supervisors may assign spacecrew members to valid tasks and SQ support roles, provided they have assessed relevant factors, including the effect on completing Recurring Training (RT) or CT prior to entering the Commit phase.

6.5.3. Supervisors will limit non-crew duties for Inexperienced (INEXP) spacecrew members in the first year of their initial operational assignment, as referenced in CFCMAN 13-602DCO-SV1 Chapter 10, to those related to unit mission activities. **(T-2)**

6.5.4. Spacecrew members will be CMR qualified IAW the position description they fill as outlined in this manual. **(T-2)**

CHANDLER P. ATWOOD
Brigadier General, USSF
Deputy Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 1-2, *Commander's Responsibilities*, 15 September 2025

AFI 10-601, *Operational Capability Requirements Documentation and Validation*, 27 April 2021

AFI 13-602V3, *Spacecrew Operations*, 6 September 2019

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 91-202_SPOCSUP, *The US Air Force Mishap Prevention Program*, 15 October 2021

AFSPCI 10-260, *Tactics Development Program*, 23 February 2016

CFCMAN 13-602DCO-SV1, *Defensive Cyberspace Operations for Space (DCO-S) – Training*, 22 December 2025

CFCMAN 13-602DCO-SV2, *Defensive Cyberspace Operations for Space (DCO-S) – Standardization and Evaluation Criteria*, 22 December 2025

DAFGM 2025-13-01V1, *Ready Spacecrew Program Training*, 8 August 2025

DAFI 63-101/20-101, *Integrated Life Cycle Management*, 16 February 2024

DAFMAN 11-260, *Tactics Development Program*, 17 March 2023

DAFMAN 11-415, *Weapons and Tactics Programs*, 1 August 2023

DAFMAN 90-161, *Publishing Processes and Procedures*, 18 October 2023

DEL 6 Mission Planning Guide, 1 February 2025

JP 5-0, *Joint Planning*, 1 December 2020

SDP 5-0, *Planning*, December 2021

SPFGM 2025-10-02, *Operations Planning and Execution*, 11 June 2025

SpOC Mission Planning Guide, 4 October 2024

SpOC/CC Memo, *Delegations and Withholding of Authorities*, 23 October 2024

TO 00-5-1, *AF Technical Order System*, 19 November 2024

Prescribed Forms

None

Adopted Forms

AF Form 8, *Certificate of Aircrew Qualification*

AF Form 1067, *Modification Proposal*

DAF Form 679, *Department of the Air Force Publication Compliance Item Waiver Request/Approval*

DAF Form 847, *Recommendation for Change of Product*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFSPCI—Air Force Space Command Instruction

BMQ—Basic Mission Qualified

CC—Commander

CCDR—Combatant Commander

CCDR—Combatant Commander

CCMD—Combatant Command

CD—Deputy Commander

CDet—Combat Detachment

CDO—Cyberspace Defense Operator

CIF—Crew Information File

CMR—Combat Mission Ready

COA—Course of Action

COMSPACEFOR—Commander of Space Forces

COMMON—Continuous Monitoring

CSpOC—Combined Space Operations Center

CSq—Combat Squadron

CSTO—Combined Space Tasking Order

CT—Combat Training

CTE—Cyber Threat Emulation

CTO—Cyber Tasking Order

CYS—Cyberspace Squadron

CW—Cyberspace Warfare

CWOC—Cyberspace Warfare Operations Center

D&CI—Discover and Counter Infiltration

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFGM—Department of the Air Force Guidance Memorandum

DAFMAN—Department of the Air Force Manual

DCO-S—Defensive Cyberspace Operations for Space

DCW—Defensive Cyberspace Warfare
DEL—Delta
DEPOD—Deployment Order
Det—Detachment
DO—Director of Operations
DoD—Department of Defense
DoDIN—Department of Defense Information Network
DRRS-S—Defense Readiness Reporting System - Strategic
DT—Difference Training
EiP—Employed-in-Place
EXORD—Execution Order
FLDCOM—Field Command
FGS—Force Generation Squadron
FTF—Formal Training Flight
GM—Guidance Memorandum
HHQ—Higher Headquarters
HQ—Headquarters
IAW—In Accordance With
IOC—Indicators of Compromise
IP—Internet Protocol
IR—Incident Responder
ISR—Intelligence, Surveillance, and Reconnaissance
JP—Joint Publication
KT-C—Key Terrain in Cyberspace
MCA—Malicious Cyber Actors
MD—Mission Delta
MET—Mission Essential Task
MISREP—Mission Report
MOE—Measures of Effectiveness
MOP—Measures of Performance
MPC—Mission Planning Cell
MRT-C—Mission Relevant Terrain – Cyber

MSC—Mission Support Cell
MSL—Master Station Log
NSDC—National Space Defense Center
OI—Operating Instructions
OPORD—Operations Order
OPR—Office of Primary Responsibility
Ops Check—Operations Check
OPSCAP—Operations Capability
ORB—Operations Review Board
ORM—Operational Risk Management
PBED—Plan, Brief, Execute, Debrief
PEX—Patriot Excalibur
PLANORD—Planning Order
QT—Qualification Training
ROE—Rules of Engagement
RT—Recurring Training
RTRB—Realistic Training Review Board
SBD—Space Base Delta
SDP—Space Doctrine Publication
SEB—Standardization and Evaluation Board
SLD—Space Launch Delta
SOP—Standard Operating Procedure
SPAFORGEN—Space Force Generation
SPFGM—Space Force Guidance Memorandum
SPINS—Special Instructions
SQ—Squadron
SSC—Space Systems Command
Stan/Eval—Standardization and Evaluation
TO—Technical Order
TP—Temporary Procedures
TTP—Tactics, Techniques, and Procedures
UMD—Unit Manning Document

USAF—United States Air Force

USSF—United States Space Force

WS—Weapon System

Office Symbols

CFC/S33—Combat Forces Command Current Operations

CFC/S35C—Combat Forces Command Cyber Warfare Division

CFC/S73—Combat Forces Command Training and Readiness

CFC/S735T—Combat Forces Command Training Branch

Attachment 2

CYBER 9-LINE TEMPLATE

Figure A2.1. Cyber 9-Line Template.

9-Line Request Template	Approved by: Date Approved:
DESCRIPTION: This template provides a structured method for units to report suspicious cyber activity to the Delta 6 Security Operations Center: ussf.schriever.del-6.mbx.soc@mail.smil.mil	
<ul style="list-style-type: none"> • Official 9-Line Report Request <ul style="list-style-type: none"> ○ Line 1-Reporting Unit Information <ul style="list-style-type: none"> ▪ Unit: ▪ Unit Location: ▪ Secure Phone: ▪ Secure E-mail: ○ Line 2-Location of Activity <ul style="list-style-type: none"> ▪ Point of Contact: <ul style="list-style-type: none"> • Secure Phone: • Secure E-mail: ▪ Victim Organization: ▪ Victim Location: ○ Line 3-Technical Details <ul style="list-style-type: none"> ▪ System <ul style="list-style-type: none"> • System Domain (SIPR, NIPR, etc): • System Mission/Role: • IP Address: • MAC Address: • System Name: • Operating System: • Affected Asset(s) on Critical Asset List: ▪ Malware/Suspicious Activity <ul style="list-style-type: none"> • File Name/Suspicious Activity: <ul style="list-style-type: none"> ○ Mission Impact (If Applicable): • Detection Method (AV, HIPS, etc): • Detection Date/Time: ○ Line 4-Description of Activity/Event: ○ Line 5-Incident/Ticket/CAT # (If Applicable): ○ Line 6-Reporting Unit Commander: <ul style="list-style-type: none"> ▪ Name: ▪ Rank: ▪ Office Symbol: ▪ Secure Phone: ▪ Secure E-mail: ○ Line 7-Updates: ○ Line 8-Recommendations: ○ Line 9-Actions Taken: 	

Attachment 3

OPERATIONAL RISK MANAGEMENT WORKSHEET EXAMPLE

Figure A3.1. Operational Risk Management Worksheet Example.

ORM - Personal Checklists

*****Read ORM - ROEs before completing*****

PERSONAL CHECKLIST A HEALTH & STRESS RISK FACTORS	0 Points Each (LOW) Green	1 Point Each (MODERATE) Yellow	2 Points Each (HIGH) Orange
Personal Health Factors (hydration, nutrition, illness/injury, etc.)	Minor	Elevated	Serious
Personal/Family Stress (health, finance, relationship, etc.)	Minor	Elevated	Serious
Work/Career Stress	Minor	Elevated	Serious
Perceived Mission Pressure (external & internal)	Minor	Elevated	Serious
*SCORE:			
* Health and Stress Scoring			
- Total of all factors 7 or more: overall score SEVERE			
- Any factor HIGH: overall score HIGH			
- Total of all four factors 3 or more: overall score HIGH			
- Total of all four factors 1-2: overall score MODERATE			
- Total of all four factors 0: overall score LOW			
PERSONAL CHECKLIST B FATIGUE RISK FACTORS	0 Points Each (LOW) Green	1 Point Each (MODERATE) Yellow	2 Points Each (HIGH) Orange
12+ hr Work/Duty Days Past Week	2	3	4
Combine Prior Sleep (past 72 hrs/3 days)	> 18 hrs	15-18 hrs	< 15 hrs
Sleep in Last 12 hrs	> 6 hrs	4-6 hrs	< 4 hrs
**SCORE:			
** Fatigue Scoring:			
- Total of all factors 5 or more: overall score SEVERE			
- Any factor HIGH: overall score HIGH			
- Total of all factors 4: overall score HIGH			
- Total of all factors 1-3: overall score MODERATE			
- Total of all factors 0: overall score LOW			